

Standardy ochrony danych osobowych przekazywanych między Unią Europejską a Stanami Zjednoczonymi w związku ze zwalczaniem terroryzmu i przestępczości

ABSTRACT: The article presents the development of cooperation between the European Union and the United States of America in relation to the protection of personal data transferred for the purpose of combating terrorism and other crimes. It discusses issues referring to the existing US and European Union obligations with respect to the legal protection of personal data. It analyzes the main legal solutions in this area, namely the “Privacy Shield” program, the PNR agreement, the Financial Messaging Data Agreement and the so-called Data Protection “Umbrella Agreement”.

KEYWORDS: personal data, PNR data, Financial Messaging Data, “Privacy Shield”, EU-US “Umbrella Agreement”

Wprowadzenie

Intensywna współpraca służb policyjnych i organów wymiaru sprawiedliwości państw członkowskich Unii Europejskiej (UE) i Stanów Zjednoczonych w zakresie przekazywania danych osobowych w celu zwalczania terroryzmu i przestępczości nastąpiła

po 11 września 2001 r. i przez obie strony została uznana za niezwykle pożądaną¹. Jednak wiele problemów pojawiło się w związku z nierówną ochroną prawną danych osobowych w państwach UE i w Stanach Zjednoczonych. Wskazywano, iż ochrona gwarantowana w Europie przez poszczególne państwa, z dużym udziałem UE, która poprzez swoje akty prawne wpływa na prawo krajowe państw członków tej organizacji, jest na wyższym poziomie niż ta istniejąca w Stanach Zjednoczonych. Dla państw europejskich odpowiednia ochrona danych osobowych polega na istnieniu szczegółowych regulacji prawnych w tym zakresie, natomiast w Stanach Zjednoczonych prawo do prywatności, które zawiera tzw. prywatność informacyjna, czyli w rozumieniu europejskim prawo do ochrony danych osobowych, było od początków jego funkcjonowania w przestrzeni prawnej traktowane jako „prawo o charakterze negatywnym”, czyli „wolność od”. Państwo amerykańskie nie podejmowało wobec tego tak szczegółowych działań jak kraje europejskie. Stany Zjednoczone podczas jednego z etapów prac nad budową transatlantyckich rozwiązań odnoszących się do ochrony danych osobowych przyznały, iż preferują podejście sektorowe, które polega na połączeniu ustawodawstwa, regulacji i samoregulacji².

Zasadniczy akt prawny w tym zakresie w Stanach Zjednoczonych, *Federal Privacy Act* z 1974 r.³, odnosi się jedynie do urzędów państwowych na poziomie federalnym, nie zabezpieczając jednostki przed naruszeniami ze strony podmiotów prywatnych. Co więcej, chroni on jedynie prawo do danych osobowych obywateli amerykańskich. Jednym z głównych zarzutów w odniesieniu do Stanów Zjednoczonych był także brak instytucji o podobnych kompetencjach jak Generalny Inspektor Danych Osobowych, która funkcjonuje w UE oraz w jej poszczególnych państwach członkowskich, czuwając nad realizacją przepisów prawnych w zakresie ochrony danych osobowych. Konieczność niwelowania wskazanych wyżej rozbieżności była przedmiotem prac w ramach trwającej wiele lat współpracy transatlantyckiej, która doprowadziła do przyjęcia poszczególnych instrumentów prawnych w zakresie ochrony danych osobowych dotyczących danych pasażerów czy informacji finansowych, a także do wypracowania określonego „sposobu

¹ *Komisja Europejska jest gotowa do rozpoczęcia rozmów ze Stanami Zjednoczonymi w sprawie umowy o ochronie danych osobowych przy zwalczaniu terroryzmu lub przestępczości*, komunikat prasowy Komisji Europejskiej, IP/10/1661, Bruksela, 3 XII 2010, http://europa.eu/rapid/press-release_IP-10-1661_pl.htm, 19 X 2018.

² *Decyzja Komisji z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani” oraz przez odnoszące się do nich najczęściej zadawane pytania*, wydane przez Departament Handlu USA (notyfikowana jako dokument nr C(2000) 2441), „Dziennik Urzędowy Wspólnot Europejskich” [dalej jako: Dz.Urz. WE] 2000, nr L 215.

³ *Privacy Act (1974)*, 5 U.S.C. § 552a, <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a>, 19 X 2018.

postępowania” poprzez uruchomienie programów „bezpiecznej przystani” z 2000 r. (ang. *Safe Harbour*)⁴, a następnie „tarczy prywatności” z 2016 r. (ang. *Privacy Shield*)⁵. Ostatnim elementem tej współpracy jest tzw. „porozumienie parasolowe”⁶, które nie stanowi podstawy do wymiany danych osobowych pomiędzy UE a Stanami Zjednoczonymi, ma natomiast gwarantować ochronę informacji przekazywanych zgodnie z już obowiązującym w tym zakresie prawem.

Celem tego artykułu jest przedstawienie i analiza rozwiązań prawnych ustanawiających standardy ochrony danych osobowych w kontekście ich przekazywania z UE do Stanów Zjednoczonych w związku ze zwalczaniem terroryzmu i przestępczości. W artykule podjęto także próbę oceny, czy istniejące standardy gwarantują bezpieczeństwo danych osobowych przekazywanych w ramach wymiany transatlantyckiej. Kwestie te stanowią w ostatnich latach przedmiot intensywnej współpracy pomiędzy UE a USA, stąd omawiana w artykule tematyka jest niezwykle aktualna. Prace nad budową transatlantyckiego systemu ochrony danych osobowych nie zostały zakończone. Wydaje się, że proces ten będzie kontynuowany w następnych latach, a kwestie związane z przestępczością i terroryzmem będą zasadniczym elementem tego systemu.

Artykuł składa się ze wstępu, dwóch części merytorycznych i podsumowania. We wstępie zarysowano m.in. zagadnienie badawcze, perspektywę teoretyczną, z punktu widzenia której prowadzona jest analiza naukowa. W części pierwszej wskazano podstawy prawne przekazywania danych osobowych z państw członkowskich UE do USA. W części drugiej przedstawiono postanowienia „umowy parasolowej”. Rozdział zamyka podsumowanie, w którym zawarto wnioski końcowe, a także przedstawiono wątpliwości i zarzuty wobec przyjętych rozwiązań prawnych, które pojawiły się w pierwszych latach ich funkcjonowania. W artykule zastosowano metodę analizy tekstów prawnych, w szczególności skupiono się na analizie postanowień prawa UE w zakresie ochrony danych osobowych w związku ze zwalczaniem terroryzmu i prze-

⁴ Zasady ochrony prywatności w ramach „bezpiecznej przystani” zostały określone w załączniku nr 1 do *Decyzji Komisji z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony...*

⁵ *Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 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 (notyfikowana jako dokument nr C(2016) 4176)*, „Dziennik Urzędowy Unii Europejskiej” [dalej jako: Dz.Urz. UE] 2016, nr L 207, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016D1250>, 19 X 2018.

⁶ *Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych*, Dz.Urz. UE 2016, nr L 336, [http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:22016A1210\(01\)](http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:22016A1210(01)), 14 I 2018.

stępczości. Przeanalizowano także komunikaty organów UE zawierające stanowisko tychże podmiotów w odniesieniu do omawianych kwestii.

Podstawy prawne przekazywania danych osobowych z państw członkowskich UE do USA

Pierwsze z przyjętych rozwiązań w zakresie ochrony danych osobowych w ramach współpracy UE–USA stanowiło, jak już wspomniano wyżej, swoistego rodzaju „kodeks postępowania”, a nie zbiór przepisów prawnych⁷. Nie odnosiło się ono bezpośrednio do organów państwowych Stanów Zjednoczonych, a jedynie do amerykańskich podmiotów prywatnych, które w drodze samocertyfikacji zobowiązywały się do przestrzegania zasad bezpieczeństwa w odniesieniu do danych osobowych przekazywanych z państw członkowskich UE. Wykaz podmiotów gospodarczych był prowadzony przez Departament Handlu Stanów Zjednoczonych. Kontrolę ze strony państwa zapewniała Federalna Komisja Handlu: do systemu mogły przystąpić jedynie te przedsiębiorstwa, które podlegały nadzorowi tego organu. Zasady „bezpiecznej przystani” miały się odnosić jedynie do podmiotów o charakterze prywatnym, jednak w kontekście sprawy Maximilian Schrems p. Komisarzowi ds. Ochrony Danych rozstrzygniętej przez Trybunał Sprawiedliwości UE w 2015 r. okazało się, iż dane osobowe przekazywane tym podmiotom z państw członkowskich UE mogły być przetwarzane, a w szczególności trafiać do organów publicznych w Stanach Zjednoczonych. W świetle faktów ujawnionych przez Edwarda Snowdena⁸ i szerokich uprawnień służb specjalnych Stanów Zjednoczonych trudno było podtrzymać twierdzenie, iż dane osobowe Europejczyków nie są przedmiotem przetwarzania w Stanach Zjednoczonych, tym bardziej że podmioty gospodarcze, dobrowolnie przystępując do programu „bezpiecznej przystani”, mogły odstąpić od stosowania zawartych tam postanowień, jeśli wymagało tego bezpieczeństwo narodowe, interes publiczny czy prawo krajowe Stanów Zjednoczonych⁹. Decyzja Komisji Europejskiej z dnia 26 lipca 2000 r. wprowadzająca zasady „bezpiecz-

⁷ *Podręcznik europejskiego prawa o ochronie danych*, Agencja Praw Podstawowych, Rada Europy, Urząd Publikacji Unii Europejskiej, Luksemburg 2014, s. 143.

⁸ Edward Snowden to były pracownik CIA, który w 2013 r. ujawnił na łamach prasy informacje o programie masowej inwigilacji. W ramach tego programu Agencja Bezpieczeństwa Narodowego USA podsłuchiwała obywateli USA i innych krajów. Zob. G. Greenwald, *NASA collecting phone records of millions of Verizon customers daily*, „The Guardian”, 6 VI 2013, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>, 20 X 2018.

⁹ *Wyrok w sprawie Maximilian Schrems p. Komisarzowi ds. Ochrony Danych*, C-362/14, http://curia.europa.eu/juris/document/document_print.jsf?jsessionid=9ea7d0f130d6e501ab59ba32452f8cfbe5

nej przystani”, wskutek wyroku Trybunału Sprawiedliwości we wspomnianej wyżej sprawie Maximiliana Schremsa została unieważniona. Trybunał Sprawiedliwości UE wyraźnie stwierdził, iż prawa podstawowe jednostki nie są chronione przed ingerencją ze strony amerykańskich organów władzy publicznej. Dane osobowe przekazywane do Stanów Zjednoczonych mogły być przetwarzane niezgodnie z celem ich transferu, a jednostka nie miała środków prawnych, które umożliwiłyby jej dostęp do tych danych, ich zmianę czy usunięcie¹⁰.

Po intensywnych pracach podjętych przez UE i Stany Zjednoczone w latach 2015-2016 w odniesieniu do transatlantyckiego przepływu danych osobowych i stosownych gwarancji w tym zakresie został wdrożony nowy program o nazwie „tarcza prywatności”, który miał zastąpić zasady „bezpiecznej przystani”¹¹. W zamierzeniu twórców tego programu ma on zapewnić lepszą ochronę danych osobowych Europejczyków i równocześnie stanowić jasne zasady dla przedsiębiorców amerykańskich w nim uczestniczących. Program opiera się, podobnie jak zasady „bezpiecznej przystani”, na samocertyfikacji podmiotów gospodarczych, a nadzór nad jego funkcjonowaniem sprawuje Departament Handlu Stanów Zjednoczonych. Przystępujące do programu podmioty amerykańskie zobowiązują się do przestrzegania m.in. następujących zasad ochrony danych osobowych: powiadomienia, integralności danych i celowości, wyboru, bezpieczeństwa oraz dostępu. Ponadto powinny one w ramach zasady ochrony prawnej, egzekwowania praw oraz odpowiedzialności, zapewnić środki ochrony prawnej, w tym skuteczne środki odwoławcze, dla obywateli państw członkowskich UE, jeśli przetwarzały ich dane osobowe w sposób sprzeczny z zasadami zawartymi w „tarczy prywatności”.

Kolejnym zabezpieczeniem adekwatnego poziomu ochrony jest regulacja, na mocy której uczestnicy „tarczy prywatności” zobowiązują się do corocznej certyfikacji oraz sprawdzenia, czy stosowana przez nią polityka prywatności jest zgodna ze wspomnianymi wyżej zasadami. Jeśli chodzi o zarzuty wysuwane w związku z działalnością służb wywiadowczych Stanów Zjednoczonych, pojawia się pytanie, czy tym razem bezpieczeństwo tych danych zostało zagwarantowane. Stany Zjednoczone zapewniły, że dostęp organów publicznych do danych osobowych, związany m.in. z kwestiami bezpieczeństwa narodowego, jest ograniczony i będzie podlegał zabezpieczeniom oraz mechanizmom nadzoru. Obywatele państw członkowskich UE będą mogli po raz pierwszy skorzystać z mechanizmów ochrony prawnej w tej dziedzinie. Wyraźnie

e8ea9e4ce4.e34KaxiLc3eQc40LaxqMbN4PahiPe0?doclang=PL&text=&pageIndex=0&part=1&mode=DOC&docid=169195&ccc=first&cid=5967, 14 I 2018.

¹⁰ *Ibidem*.

¹¹ *Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r...*

wykluczona została „bezkrytyczna masowa inwigilacja danych osobowych” przekazywanych w ramach programu „tarcza prywatności”¹². Stany Zjednoczone wskazały ponadto, iż Urząd Dyrektora Krajowych Służb Wywiadowczych zapewnił, że „masowe gromadzenie danych może być wykorzystywane wyłącznie w określonych warunkach i wymaga tak ścisłego ukierunkowania, jak to możliwe”¹³.

W „tarczy prywatności” szczegółowo określono zabezpieczenia odnoszące się do wykorzystania danych osobowych w wyjątkowych okolicznościach. Wskazano, iż Europejczycy mają możliwość skorzystania ze środków odwoławczych wobec amerykańskich służb wywiadowczych. Realizację tego prawa ma zapewnić urząd rzecznika w Departamencie Stanu¹⁴. Skargę można wnieść także bezpośrednio do amerykańskiego podmiotu gospodarczego przystępującego do programu, do niezależnego organu ds. rozstrzygania sporów wyznaczonego przez ten podmiot oraz do krajowych organów ochrony danych lub Federalnej Komisji Handlu. Jednostka może także zwrócić się z prośbą o rozstrzygnięcie do arbitrażowego panelu ds. tarczy prywatności, który będzie uprawniony do przyznania „godziwego zadośćuczynienia danej osobie fizycznej”. Właściwej realizacji programu „tarcza prywatności” służyć ma także mechanizm corocznego przeglądu jej funkcjonowania dokonywany przez Komisję Europejską i Departament Handlu Stanów Zjednoczonych. W ramach tych przeglądów krajowe służby wywiadowcze Stanów Zjednoczonych są zobowiązane do współpracy z podmiotami dokonującymi tego przeglądu.

Kolejnym, tym razem klasycznym instrumentem prawnomiędzynarodowym zastosowanym odnośnie do transatlantyckiego przepływu danych osobowych są tzw. umowy PNR (skrót pochodzi od angielskiego terminu *Passenger Name Records*). Są to umowy dotyczące danych gromadzonych przez przewoźników podczas procesu rezerwacyjnego w związku z przelotem pasażera. Należą do nich: imię, nazwisko, adres, telefon, data podróży, trasa podróży, dane kart kredytowych, numery miejsc pasażerów, informacja o biurze podróży i płatnościach, a także informacje odnoszące się do bagażu. Prawo wewnętrzne Stanów Zjednoczonych ustanawia obowiązek linii lotniczych udostępniania wskazanych wyżej danych Departamentowi Bezpieczeństwa Wewnętrznego. Obowiązkiem tym są objęte linie lotnicze obsługujące loty z terytorium Stanów Zjednoczonych i do Stanów Zjednoczonych. Informacje o pasażerach mają być udostępnione przed odlotem samolotu. Przekazanie danych PNR może skutkować

¹² Komisja Europejska uruchamia Tarczę Prywatności UE–USA: lepsza ochrona transatlantyckiego przepływu danych, komunikat prasowy Komisji Europejskiej, Bruksela, 12 VII 2016, http://europa.eu/rapid/press-release_IP-16-2461_pl.htm, 13 I 2018.

¹³ *Ibidem*.

¹⁴ *Ibidem*.

identyfikacją osób, które mogą stanowić potencjalne zagrożenie dla bezpieczeństwa kraju i w związku z tym mogą być przedmiotem zainteresowania organów ścigania. Dane te mogą być także przydatne do oceny ryzyka zagrożenia bezpieczeństwa kraju. Mogą one także służyć do powiązania danych odnoszących się do kart kredytowych z osobami, które np. są podejrzewane o popełnienie określonych przestępstw.

Pierwszym rozwiązaniem w ramach współpracy UE–USA w tym zakresie był tzw. pakiet PNR¹⁵, który regulował przetwarzanie i przekazywanie danych osobowych przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych oraz kwestię odpowiedniej ochrony tych danych. Niemniej standardy amerykańskie, jeśli chodzi o zabezpieczenie przekazywanych z państw członkowskich UE danych osobowych, nie gwarantowały odpowiedniej ochrony, co wielokrotnie podkreślały organizacje pozarządowe oraz Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Europejskie przepisy w zakresie PNR zakładały bowiem możliwość przesyłania danych osobowych pasażerów, ale tylko w ramach zbliżonych systemów prawnych¹⁶. W uzasadnionych przypadkach można było odstąpić od tych zasad, jeśli w określonej sprawie prowadzone było śledztwo, w którym zebrano dowody świadczące o działalności przestępczej lub terrorystycznej danej osoby. Stany Zjednoczone po ataku z 11 września 2001 r. podjęły działania zmierzające do budowy baz danych gromadzonych w sposób systematyczny, w których znajdowałyby się informacje PNR przesyłane z Europy¹⁷. Jednocześnie w amerykańskim systemie prawnym zabrakło postanowień, które stanowiłyby zabezpieczenie dla danych osobowych, a także woli politycznej do uregulowania tych kwestii. Sytuacja ta doprowadziła do zbadania zgodności postanowień przyjętych w pakiecie PNR z prawem UE przez Trybunał Sprawiedliwości WE. W wyroku z dnia 14 maja

¹⁵ Decyzja Rady z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Cel i Ochrony Granic, 2004/496/WE, Dz.Urz. UE 2004, nr L 183, <http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32004D0496>, 14 I 2018; Decyzja Komisji z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych, 2004/535/WE, Dz.Urz. UE 2004, nr L 235, <http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32004D0535>, 14 I 2018.

¹⁶ Wówczas jeszcze powoływano się na: Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. WE 1995, nr L 281, <http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:31995L0046&from=PL>, 3 III 2017.

¹⁷ Zob. szerzej: W. Ostant, *Współpraca Stanów Zjednoczonych i Unii Europejskiej – razem mimo różnic (lata 2001–2010)*, „Przegląd Strategiczny” 2011, nr 2, s. 269 i n.

2006 r. w połączonych sprawach C-317/04 Parlament Europejski p. Radzie Unii Europejskiej oraz C-318/04 Parlament Europejski p. Komisji Wspólnot Europejskich zawieszono możliwość stosowania pakietu PNR oraz zobowiązano Radę Europejską do rewizji postanowień umowy UE–USA dotyczącej przekazywania danych osobowych pasażerów do dnia 30 września 2006 r.¹⁸ Podejmowane wysiłki, odnoszące się do przyjęcia odpowiadających obu stronom standardów ochrony danych osobowych, zaowocowały podpisaniem kolejnej umowy pomiędzy UE a USA w sprawie wykorzystywania danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych w 2012 r.¹⁹ W art. 4 przedmiotowej umowy Stany Zjednoczone zobowiązały się do gromadzenia, wykorzystywania i przetwarzania danych PNR do celów zapobiegania szczególnie wymienionym przestępstwom terrorystycznym oraz przestępstwom z nimi powiązanym, a także przestępstwom o charakterze międzynarodowym podlegającym karze pozbawienia wolności na czas nie krótszy niż trzy lata. Wykorzystywanie danych osobowych może być także dokonywane w celu wykrywania i ścigania wymienionych wyżej przestępstw oraz prowadzenia dochodzeń lub śledztw w ich sprawie²⁰.

Rozdział II tej umowy szeroko określa zabezpieczenia, które zostały zastosowane w przypadku wykorzystywania danych PNR. Znalazły się tam postanowienia odnoszące się do: bezpieczeństwa danych, danych szczególnie chronionych, zautomatyzowanych decyzji indywidualnych, przechowywania danych, niedyskryminacji, przejrzystości, dostępu do danych dla osób fizycznych, możliwości poprawienia i sprostowania danych oraz środków odwoławczych dostępnych dla osób fizycznych²¹. Nadzór nad wykorzystywaniem danych PNR zgodnie z zabezpieczeniami dotyczącymi prywatności przewidzianymi w umowie wykonywać mają departamentalni urzędnicy ds. prywatności, m.in. główny urzędnik ds. prywatności w Departamencie Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS). Niezależny przegląd i nadzór mają prowadzić także: Biuro Inspektora Generalnego DHS, Biuro Kontroli Rządu oraz Kongres Stanów Zjednoczonych²². Zgodnie z art. 26 umowy pozostaje ona w mocy

¹⁸ *Wyrok Trybunału (wielka izba) z dnia 30 maja 2006 r. Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04)*, <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-317/04#>, 14 I 2018.

¹⁹ *Zob. Decyzja Rady z dnia 26 kwietnia 2012 r. w sprawie zawarcia Umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (2012/472/UE)*, Dz.Urz. UE 2012, nr L 215. Do tekstu decyzji został dołączony tekst umowy.

²⁰ *Ibidem*, art. 4.

²¹ *Ibidem*, art. 5-13.

²² *Ibidem*, art. 14.

przez okres siedmiu lat od dnia wejścia w życie, czyli będzie obowiązywała do 2019 r. Postanowienie to przewiduje także możliwość automatycznego przedłużenia tej umowy na następne siedmioletnie okresy w razie braku odmiennej woli obu stron umowy.

Kolejnym instrumentem prawnym o charakterze umowy międzynarodowej jest porozumienie o przetwarzaniu i przekazywaniu z UE do Stanów Zjednoczonych danych z komunikatów finansowych do celów programu śledzenia środków finansowych należących do terrorystów (znane także jako umowa SWIFT) z 2010 r.²³ Umowa ta miała na celu rozstrzygnięcie sporów istniejących pomiędzy stronami z powodu żądań Departamentu Skarbu USA, kierowanych do amerykańskiego oddziału Stowarzyszenia Międzynarodowej Transmisji Danych Finansowych (SWIFT) w odniesieniu do ujawnienia danych finansowych w związku z dochodzeniami dotyczącymi terroryzmu²⁴. Działania Stowarzyszenia umożliwiają przekazywanie informacji finansowych na całym świecie, dzięki którym dokonywane są międzynarodowe przekazy płatnicze. Przechowuje ono takie informacje przez 124 dni, także w centrum operacyjnym, które ma siedzibę na terytorium USA, tworząc tzw. kopie lustrzane (ang. *mirroring*)²⁵. Gromadzone są takie dane osobowe, jak nazwiska zleceniodawcy i odbiorcy płatności. W związku z atakiem z 11 września 2001 r. Departament Skarbu Stanów Zjednoczonych w ramach realizowanego programu śledzenia środków finansowych należących do terrorystów (ang. *Terrorist Finance Tracking Program – TFPT*) wezwał SWIFT do udostępnienia informacji przechowywanych w USA. SWIFT, z pewnymi ograniczeniami, zastosował się do wezwań organów amerykańskich. Informacja ta została podana do wiadomości publicznej w 2006 r.²⁶ Zgodnie ze wspomnianą wyżej umową SWIFT dane z komunikatów finansowych dotyczących transferów finansowych oraz powiązane z nimi dane przechowywane na terytorium UE przez dostawców międzynarodowych usług w zakresie komunikatów finansowych, dotyczących płatności, będą udostępniane Departamentowi Skarbu Stanów Zjednoczonych. Dane mają być przekazywane w celu zapobiegania terroryzmowi lub jego finansowaniu, prowadzenia dochodzeń, wykrywania lub ścigania tego typu przestępstw²⁷. Umowa stanowi ponadto,

²³ Opublikowane w: Dz.Urz. UE 2010, nr L 195, [http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22010A0727\(01\)&from=PL](http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22010A0727(01)&from=PL), 14 I 2018.

²⁴ Zob. *Opinia Grupy Roboczej Art. 29 z dnia 22 listopada 2006 r. w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT)*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_pl.pdf, 14 I 2018.

²⁵ *Ibidem.*

²⁶ *Ibidem.*

²⁷ Zob. art. 1 lit. a) *Umowy między UE a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów*

że dane otrzymane w ramach programu TFTP będą mogły być wykorzystane przez organy ścigania, bezpieczeństwa publicznego lub zwalczania terroryzmu z państw członkowskich, a także agencje unijne: Europol lub Eurojust, do celów zapobiegania terroryzmowi lub jego finansowaniu, prowadzenia odnośnych dochodzeń, wykrywania lub ścigania tych zjawisk²⁸.

Artykuł 2 umowy szczegółowo określa działania wchodzące w zakres pojęcia „czyny związane z terroryzmem lub finansowaniem terroryzmu”. Uregulowano także kwestię gwarancji dostarczanych danych, które mają być stosowane bez dyskryminacji, biorąc pod uwagę w szczególności miejsce zamieszkania i narodowość osoby, której dane są przekazywane²⁹. Strona amerykańska zobowiązuje się także, iż w ramach programu TFTP nie będzie dokonywane automatyczne profilowanie lub komputerowe filtrowanie danych. Odpowiednie postanowienia zapewniają także bezpieczeństwo i integralność danych³⁰ oraz konieczne i proporcjonalne ich przetwarzanie³¹. Umowa reguluje także kwestie zatrzymywania i usuwania danych. USA mają obowiązek, po dokonaniu corocznego przeglądu, trwale usunąć wszystkie nieopbrane dane, które nie są już konieczne dla zwalczania terroryzmu³². Przesłanki tzw. dalszego przekazywania danych oraz podmioty, którym mogą być one przekazywane, zostały ściśle określone w omawianej umowie. Ponadto dalsze przekazywanie danych powinno być odpowiednio rejestrowane³³. Przestrzeganie umowy podlega monitoringowi i nadzorowi ze strony niezależnych organów, w tym osób wyznaczonych przez Komisję Europejską³⁴. Do kompetencji takich organów należy prawo do blokowania każdego lub wszystkich wyszukiwań, które są niezgodne z gwarancjami dotyczącymi przetwarzania dostarczonych danych osobowych, uregulowanych w art. 5 umowy. UE i USA dokonują także wspólnego przeglądu realizacji postanowień umowy. Jednostka, której przekazywane dane dotyczą, otrzymuje na mocy umowy prawo dostępu do danych, prawo do zmiany, usunięcia lub ich zablokowania, jeśli są one nieprawidłowe lub ich przetwarzanie jest sprzeczne z postanowieniami umowy³⁵. Okres obowiązywania umowy SWIFT został

Programu śledzenia środków finansowych należących do terrorystów, Dz.Urz. UE 2010, nr L 195, [http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22010A0727\(01\)&from=PL](http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22010A0727(01)&from=PL), 14 I 2018.

²⁸ *Ibidem*, art. 1 lit. b).

²⁹ *Ibidem*, art. 5 ust. 1.

³⁰ *Ibidem*, art. 5 ust. 4.

³¹ *Ibidem*, art. 5 ust. 5.

³² *Ibidem*, art. 6 ust. 1.

³³ *Ibidem*, art. 7.

³⁴ *Ibidem*, art. 12.

³⁵ *Ibidem*, art. 15 i art. 16.

określony na 5 lat, czyli pierwotnie do 2015 r., z możliwością automatycznego przedłużenia na kolejne okresy jednoroczne w przypadku braku sprzeciwu obu stron umowy.

Postanowienia „umowy parasolowej”

W 2010 r. UE i Stany Zjednoczone rozpoczęły współpracę nad umową, która miała zapewniać ochronę danych osobowych przy współpracy w dziedzinie zwalczania terroryzmu i przestępczości³⁶. Umowa miała zagwarantować wysoki poziom ochrony przekazywanym w ramach współpracy transatlantyckiej informacjom, odnoszącym się m.in. do danych PNR czy danych z komunikatów finansowych. Celem twórców umowy było poszerzenie praw obywateli poprzez umożliwienie im dostępu do danych, prawo do ich usunięcia lub sprostowania w przypadku, gdy przetwarzanie ma związek z zapobieganiem, wykrywaniem, ściganiem oraz prowadzeniem postępowań sądowych odnoszących się do przestępczości karnej, w tym terrorystycznej³⁷. Do podpisania „umowy parasolowej” pomiędzy UE a USA doszło w 2016 r., a kilka miesięcy później zatwierdził ją Parlament Europejski³⁸. Umowa ma także na celu wzmocnienie współpracy pomiędzy amerykańskimi organami ścigania a odpowiadającymi im jednostkami w państwach członkowskich UE. Jest ona także jednym z kluczowych działań podejmowanych przez UE i USA w celu przywrócenia zaufania w kontekście przesyłania danych pomiędzy tymi podmiotami³⁹. Współpraca w ramach partnerstwa transatlantyckiego w tym zakresie uległa osłabieniu w związku z doniesieniami „o szeroko zakrojonych programach gromadzenia danych przez amerykańskie służby wywiadowcze, które wzbudziły poważne obawy zarówno na szczeblu UE, jak i na szczeblu państw członkowskich dotyczące wpływu tego rodzaju przetwarzania danych osobowych na

³⁶ *Komisja Europejska jest gotowa do rozpoczęcia rozmów ze Stanami Zjednoczonymi w sprawie umowy o ochronie danych osobowych przy zwalczaniu terroryzmu lub przestępczości*, komunikat prasowy Komisji Europejskiej, IP/10/1661, Bruksela, 3 XII 2010, http://europa.eu/rapid/press-release_IP-10-1661_pl.htm, 14 I 2018.

³⁷ *Ibidem*.

³⁸ *Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych*, Dz.Urz. UE 2016, nr L 336, [http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:22016A1210\(01\)](http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:22016A1210(01)), 14 I 2018.

³⁹ *Zob. Komunikat Komisji do Parlamentu Europejskiego i Rady: Transatlantyckie przepływy danych: odbudowa zaufania dzięki ustanowieniu silniejszych gwarancji*, COM(2016)117 final, Bruksela, 29 II 2016, <http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52016DC0117>, 14 I 2018.

szeroką skalę przez amerykańskie organy publiczne i przez przedsiębiorstwa prywatne w Stanach Zjednoczonych na prawa podstawowe Europejczyków⁴⁰.

Wspomniana wyżej „umowa parasolowa” reguluje przekazywanie informacji osobowych między właściwymi organami obu stron⁴¹. Stanowi ona uzupełnienie przepisów już przyjętych w zakresie ochrony danych osobowych na mocy porozumień pomiędzy UE a USA lub pomiędzy USA a poszczególnymi państwami członkowskimi UE, które stanowią upoważnienie do działań podejmowanych w celu egzekucji prawa. Ponadto, jak stanowi umowa, stworzone wspólne ramy ochrony danych osobowych będą miały zastosowanie także do umów przyszłych. Umowa odnosi się do danych osobowych przekazanych odrębną podstawą prawną w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych, w tym terroryzmu⁴². Dotyczy wszystkich danych, w tym imion, nazwisk, danych adresowych czy danych z rejestrów karnych. Dalsze przekazywanie danych osobowych do kraju trzeciego lub organizacji międzynarodowej jest uwarunkowane otrzymaniem zgody właściwego organu publicznego państwa, które pierwotnie przekazało przedmiotowe informacje⁴³. Dane osobowe powinny być przechowywane z zachowaniem zasad prawidłowości, odpowiedniości, terminowości i kompletności. W tym celu odpowiednie organy państwowe powinny ustanowić właściwe procedury⁴⁴.

Umowa wprowadza także zasadę „bezpieczeństwa informacji”, która oznacza zabezpieczenie danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą, nieuprawnionym ujawnieniem, modyfikacją, dostępem lub innego rodzaju ich przetwarzaniem. Okres zatrzymywania informacji zgodnie z umową ma być nie dłuższy, niż jest to konieczne i stosowne ze względu na cel przekazania. Okresy zatrzymania są publikowane lub udostępniane publicznie w inny sposób⁴⁵. Umowa wyróżnia także szczególne kategorie informacji osobowych, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub inne, przynależność do związków zawodowych oraz informacji osobowych, dotyczących stanu zdrowia i życia seksualnego. Przetwarzanie tych informacji odbywa się wyłącznie przy zagwarantowaniu właściwych zabezpieczeń przewidzianych prawem⁴⁶.

⁴⁰ *Ibidem*.

⁴¹ *Ibidem*, art. 3.

⁴² *Ibidem*, art. 6 w związku z art. 1.

⁴³ *Ibidem*, art. 7.

⁴⁴ *Ibidem*, art. 8.

⁴⁵ *Ibidem*, art. 12.

⁴⁶ *Ibidem*, art. 13. Zob. także zdanie 2 tego artykułu: „Takie odpowiednie zabezpieczenia mogą obejmować: ograniczenie celów, dla których informacje mogą być przetwarzane, takie jak zezwolenie na przetwarzanie jedynie w indywidualnie rozpatrywanych przypadkach; maskowanie, usuwanie lub

Decyzje zautomatyzowane wywołujące niekorzystne skutki dla osoby fizycznej nie mogą być podejmowane bez udziału człowieka, chyba że w prawie krajowym istnieją zabezpieczenia, które dają możliwość interwencji człowieka⁴⁷. Każda osoba fizyczna ma także prawo do ubiegania się o dostęp do swoich informacji osobowych i jego uzyskanie. Umowa ustanawia możliwość ograniczenia tego prawa m.in. ze względu na prawa i wolności innych osób, bezpieczeństwo publiczne i narodowe, prawidłowy tok czynności w postępowaniach urzędowych, sądowych lub przygotowawczych⁴⁸. Każda osoba ma także prawo do zmiany lub sprostowania swoich informacji osobowych, które może polegać na uzupełnieniu, usunięciu, zablokowaniu lub zastosowaniu innych środków lub metod celem eliminowania nieprawidłowości lub niewłaściwego przetwarzania. W przypadku odrzucenia wniosku danej osoby fizycznej o dostęp do jej danych osobowych lub wniosku o sprostowanie ich nieprawidłowości może ona skorzystać z administracyjnych środków zaskarżenia, które wnosi się do odpowiednich organów, zgodnie z właściwym prawem krajowym⁴⁹. Po wyczerpaniu drogi administracyjnej osoba fizyczna ma prawo do zastosowania sądowych środków zaskarżenia w przypadku odmowy dostępu do jej danych osobowych, odmowy wprowadzenia do nich zmian oraz niezgodnego z prawem świadomego lub celowego ujawnienia danych. W tym ostatnim przypadku osoba fizyczna powinna mieć prawo uzyskania odszkodowania za poniesioną szkodę⁵⁰. Nadzór nad wykonywaniem umowy z ramienia UE sprawują organy do spraw ochrony danych UE i państw członkowskich. Stany Zjednoczone mogą sprawować nadzór przez inspektorów generalnych, głównych urzędników do spraw ochrony prywatności, urzędy rządowe, komisje nadzoru prywatności i swobód obywatelskich, a także inne odpowiednie organy wykonawcze i ustawodawcze rozpatrujące odwołania w sprawach dotyczących prywatności i swobód obywatelskich⁵¹. Strony zobowiązują się także do dokonywania okresowych przeglądów strategii i procedur służących wdrażaniu omawianej umowy oraz ich skuteczności. Umowa została zawarta na czas nieokreślony.

blokowanie tych informacji po osiągnięciu celu, dla którego były one przetwarzane; ograniczenie liczby osób upoważnionych do dostępu do tych informacji; wymóg odbycia specjalistycznych szkoleń przez pracowników, którzy mają dostęp do tych informacji; wymóg zatwierdzenia przez organ nadzoru w celu uzyskania dostępu do tych informacji; lub inne środki ochronne. Zabezpieczenia te należycie uwzględniają charakter informacji, szczególnie wrażliwość tych informacji oraz cel, w jakim są one przetwarzane”.

⁴⁷ *Ibidem*, art. 15.

⁴⁸ *Ibidem*, art. 16.

⁴⁹ *Ibidem*, art. 18.

⁵⁰ *Ibidem*, art. 19.

⁵¹ *Ibidem*, art. 21.

Podsumowanie

Podczas trwającej wiele lat współpracy transatlantyckiej w zakresie tworzenia standardów przekazywania danych osobowych pomiędzy UE a Stanami Zjednoczonymi przyjęto wiele postanowień prawnych, dzięki którym ochrona praw Europejczyków w tym zakresie miała stać się realna. Współpracy tej nie ułatwiły działania władz amerykańskich, które ujawnił Edward Snowden. Mimo wielu wątpliwości w UE w odniesieniu do amerykańskiego partnera postanowiono odbudować zaufanie w tych relacjach dzięki stworzeniu silniejszych gwarancji ochrony przekazywanych danych. Stosunkowo nowym instrumentem jest „tarcza prywatności”, która bezpośrednio nie odnosi się do działań organów publicznych, ale mogą one, powołując się na bezpieczeństwo publiczne, uzyskiwać dane od podmiotów gospodarczych zaangażowanych w ten program. Krytycy „tarczy prywatności” wskazują, iż jej założenia niewiele różnią się od unieważnionych przez Trybunał Sprawiedliwości UE w sprawie Maximilian Schrems p. Komisarzowi ds. Ochrony Danych zasad „bezpiecznej przystani”, które nie zawierały regulacji zabezpieczających jednostkę przed naruszeniem jej danych osobowych ze strony organów publicznych. „Tarczy prywatności” stawia się te same zarzuty co zasadom „bezpiecznej przystani”: brak efektywnych mechanizmów kontroli oraz szerokie wyjątki w zakresie bezpieczeństwa narodowego⁵². Wskazuje się, iż przyjęte postanowienia nie spełniają wymogów niezbędności i proporcjonalności. Uprawnienia służb amerykańskich postrzegane są jako zbyt szerokie, co prowadzi do gromadzenia danych na masową skalę i ich wykorzystywania⁵³. W połowie września 2017 r. został dokonany pierwszy wspólny roczny przegląd, podczas którego dokonano oceny funkcjonowania „tarczy prywatności”⁵⁴. Jeżeli chodzi o zalecenia dalszej poprawy jej funkcjonowania, w odniesieniu do działań służb specjalnych zgłoszono postulat przeglądu sekcji 702 ustawy o kontroli wywiadu (ang. *Foreign Intelligence Surveillance Act*) i wprowadzenia tamże zapisu o środkach ochrony osób spoza USA, tak jak przewiduje to dyrektywa polityczna prezydenta nr 28 (PD-28)⁵⁵. W odniesieniu do

⁵² *Uwagi dotyczące projektu komunikatu Transatlantic Data Flows: Restoring Trust through Strong Safeguards*, Fundacja Panoptikon, Warszawa, 15 IV 2016, https://panoptikon.org/sites/default/files/panoptikon_komunikat_transatlantic_data_flows_15.04.2016.pdf, 14 I 2018.

⁵³ *Ibidem*.

⁵⁴ *Report from the Commission and the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield*, COM(2017) 611 final, Brussels, 18 X 2017, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619, 14 I 2018.

⁵⁵ *Presidential Policy Directive, Signals Intelligence Activities, Policy Directive PD 28*, The White House, Office of the Press Secretary, 17 I 2014, <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>, 14 I 2018.

„porozumienia parasolowego” formułuje się zarzuty o ogólnikowości jego postanowień i wobec tego braku możliwości stwarzania realnych zabezpieczeń w zakresie ochrony danych osobowych. Odnosi się je zwłaszcza do kwestii związanych z profilowaniem i korzystaniem z danych wrażliwych. Wskazuje się, iż brak w „porozumieniu parasolowym” regulacji, które dawałyby jednostce egzekwowlalne prawo do informacji o tym, czy organy państwowe przetwarzają konkretne dane osobowe⁵⁶. W jakim stopniu te zarzuty są uzasadnione i czy stworzone zabezpieczenia rzeczywiście będą działać, pokaże zapewne praktyka następnych lat. Wydaje się, iż takie założenie jest uprawnione w związku z faktem, że te najbardziej kontrowersyjne rozwiązania, takie jak „tarcza prywatności” czy „umowa parasolowa”, są stosunkowo nowe i funkcjonują od niedawna.

Bibliografia

Dokumenty

- Decyzja Komisji z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych, 2004/535/WE*, „Dziennik Urzędowy Unii Europejskiej” 2004, nr L 235, <http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32004D0535>, 14 I 2018.
- Decyzja Komisji z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani” oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (notyfikowana jako dokument nr C(2000) 2441)*, „Dziennik Urzędowy Wspólnot Europejskich” 2000, nr L 215.
- Decyzja Rady z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznych Stanów Zjednoczonych, Biura Cel i Ochrony Granic, 2004/496/WE*, „Dziennik Urzędowy Unii Europejskiej” 2004, nr L 183, <http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32004D0496>, 14 I 2018.
- Decyzja Rady z dnia 26 kwietnia 2012 r. w sprawie zawarcia Umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznych Stanów Zjednoczonych (2012/472/UE)*, „Dziennik Urzędowy Unii Europejskiej” 2012, nr L 215.
- Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 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 (notyfikowana jako dokument nr C(2016) 4176)*, „Dziennik Urzędowy Unii Europejskiej” 2016, nr L 207, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016D1250>, 19 X 2018.

⁵⁶ *Ochrona danych w walce z przestępczością – nowe podejście czy pozorne ruchy?*, Fundacja Panoptykon, 24 IX 2015, <https://panoptykon.org/wiadomosc/ochrona-danych-w-walce-z-przestepczoscia-nowe-podejscie-czy-pozorne-ruchy>, 14 I 2018.

- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*, „Dziennik Urzędowy Wspólnot Europejskich” 1995, nr L 281, <http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:31995L0046&from=PL>, 3 III 2017.
- Komisja Europejska jest gotowa do rozpoczęcia rozmów ze Stanami Zjednoczonymi w sprawie umowy o ochronie danych osobowych przy zwalczaniu terroryzmu lub przestępczości*, komunikat prasowy Komisji Europejskiej, IP/10/1661, Bruksela, 3 XII 2010, http://europa.eu/rapid/press-release_IP-10-1661_pl.htm, 19 X 2018.
- Komisja Europejska uruchamia Tarczę Prywatności UE–USA: lepsza ochrona transatlantyckiego przepływu danych*, komunikat prasowy Komisji Europejskiej, IP/16/2461, Bruksela, 12 VII 2016, http://europa.eu/rapid/press-release_IP-16-2461_pl.htm, 13 I 2018.
- Komunikat Komisji do Parlamentu Europejskiego i Rady: Transatlantyckie przepływy danych: odbudowa zaufania dzięki ustanowieniu silniejszych gwarancji*, COM(2016)117 final, Bruksela, 29 II 2016, <http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52016DC0117>, 14 I 2018.
- Opinia Grupy Roboczej Art. 29 z dnia 22 listopada 2006 r. w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT)*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_pl.pdf, 14 I 2018.
- Podręcznik europejskiego prawa o ochronie danych*, Agencja Praw Podstawowych, Rada Europy, Urząd Publikacji Unii Europejskiej, Luksemburg 2014.
- Presidential Policy Directive, Signals Intelligence Activities, Policy Directive PD 28*, The White House, Office of the Press Secretary, 17 I 2014, <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>, 14 I 2018.
- Privacy Act (1974)*, <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a>, 19 X 2018.
- Report from the Commission and the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield*, COM(2017) 611 final, Brussels, 18 X 2017, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619, 14 I 2018.
- Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych*, „Dziennik Urzędowy Unii Europejskiej” 2016, nr L 336, [http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:22016A1210\(01\)](http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:22016A1210(01)), 14 I 2018.
- Umowa między UE a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów Programu śledzenia środków finansowych należących do terrorystów*, „Dziennik Urzędowy Unii Europejskiej” 2010, nr L 195, [http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22010A0727\(01\)&from=PL](http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22010A0727(01)&from=PL), 14 I 2018.
- Wyrok w sprawie Maximilian Schrems p. Komisarzowi ds. Ochrony Danych, C-362/14*, http://curia.europa.eu/juris/document/document_print.jsf?jsessionid=9ea7d0f130d6e501ab59ba32452f8cfbe5e8ea9e4ce4.e34KaxiLc3eQc40LaxqMbN4PahiPe0?doclang=PL&text=&pageIndex=0&part=1&mode=DOC&docid=169195&occ=first&cid=5967, 14 I 2018.

Wyrok Trybunału (wielka izba) z dnia 30 maja 2006 r. Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04), <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-317/04#>, 14 I 2018.

Artykuły w czasopismach naukowych

Ostant W., *Współpraca Stanów Zjednoczonych i Unii Europejskiej – razem mimo różnic (lata 2001-2010)*, „Przegląd Strategiczny” 2011, nr 2.

Źródła internetowe

Greenwald G., *NASA collecting phone records of millions of Verizon customers daily*, „The Guardian”, 6 VI 2013, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>, 20 X 2018.

Ochrona danych w walce z przestępczością – nowe podejście czy pozorne ruchy?, Fundacja Panoptrykon, Warszawa, 24 IX 2015, <https://panoptrykon.org/wiadomosc/ochrona-danych-w-walce-z-przestepczoscia-nowe-podejscie-czy-pozorne-ruchy>, 14 I 2018.

Uwagi dotyczące projektu komunikatu Transatlantic Data Flows: Restoring Trust through Strong Safeguards, Fundacja Panoptrykon, Warszawa, 15 IV 2016, https://panoptrykon.org/sites/default/files/panoptrykon_komunikat_transatlantic_data_flows_15.04.2016.pdf, 14 I 2018.

