



KOMISJA
EUROPEJSKA

Bruksela, dnia 27.11.2013 r.
COM(2013) 846 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

**Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami
Zjednoczonymi**

1. WPROWADZENIE: ZMIENIAJĄCE SIĘ WARUNKI PRZETWARZANIA DANYCH MIĘDZY UE A STANAMI ZJEDNOCZONYMI

Unia Europejska i Stany Zjednoczone są partnerami strategicznymi, a partnerstwo to ma zasadnicze znaczenie dla promowania ich wspólnych wartości, bezpieczeństwa i wspólnego przywództwa w sprawach globalnych.

Zaufanie do partnerstwa zostało jednak nadwątlone i konieczne jest jego przywrócenie. Unia Europejska, jej państwa członkowskie i obywatele wyrazili głębokie zaniepokojenie doniesieniami o szeroko zakrojonych programach gromadzenia danych przez amerykańskie służby wywiadowcze, w szczególności jeżeli chodzi o ochronę danych osobowych¹. Niedopuszczalne jest masowe nadzorowanie prywatnej komunikacji obywateli, przedsiębiorstw i czołowych polityków.

Przekazywanie danych osobowych jest ważnym i niezbędnym elementem stosunków transatlantyckich. Stanowi ono nieodłączną część transatlantyckiej wymiany handlowej, w szczególności jeżeli chodzi o nowe rozwijające się przedsiębiorstwa cyfrowe prowadzące działalność w takich dziedzinach, jak media społecznościowe lub chmura obliczeniowa, z czym wiąże się duża ilość danych przekazywanych z Unii Europejskiej do Stanów Zjednoczonych. Ponadto przekazywanie danych osobowych stanowi istotny element współpracy UE-USA w obszarze egzekwowania prawa oraz współpracy państw członkowskich ze Stanami Zjednoczonymi w dziedzinie bezpieczeństwa narodowego. Aby ułatwić przepływ danych, zapewniając jednocześnie wysoki poziom ochrony danych zgodnie z wymogami prawa UE, Stany Zjednoczone i Unia Europejska zawarły szereg umów i porozumień.

Wymiana danych do celów komercyjnych została uregulowana w decyzji 2000/520/WE² (zwanej dalej decyzją w sprawie ochrony prywatności w ramach „Bezpiecznej przystani”). Decyzja ta stanowi podstawę prawną transferów danych osobowych z UE do przedsiębiorstw mających siedzibę w Stanach Zjednoczonych, które zobowiązały się do przestrzegania zasad bezpiecznego transferu danych osobowych.

Wymiana danych osobowych między Unią Europejską i Stanami Zjednoczonymi do celów egzekwowania prawa, aby zapobiegać terroryzmowi i innym formom poważnej przestępczości oraz aby zwalczać te zjawiska, opiera się na wielu umowach zawartych na szczeblu UE. Są to: Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej³, Umowa o wykorzystywaniu i przekazywaniu danych dotyczących przelotu pasażera (PNR)⁴, Umowa o przetwarzaniu i przekazywaniu danych z komunikatów finansowych do celów Programu śledzenia środków finansowych należących

¹ Do celów niniejszego komunikatu odniesienia do obywateli Unii obejmują również osoby spoza UE, których dane dotyczą, i które są objęte zakresem stosowania przepisów Unii Europejskiej o ochronie danych.

² Decyzja Komisji 2000/520/WE z dnia 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” oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA, Dz.U. L 215 z 25.8.2000, s. 7.

³ Decyzja Rady 2009/820/WPZiB z dnia 23 października 2009 r. w sprawie zawarcia w imieniu Unii Europejskiej Umowy o ekstradycji między Unią Europejską a Stanami Zjednoczonymi Ameryki oraz Umowy o wzajemnej pomocy prawnej między Unią Europejską a Stanami Zjednoczonymi Ameryki, Dz.U. L 291 z 7.11.2009, s. 40.

⁴ Decyzja Rady 2012/472/UE 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, Dz.U. L 215 z 11.8.2012, s. 4.

do terrorystów⁵ oraz umowa o współpracy między Europolem a Stanami Zjednoczonymi. Umowy te regulują ważne kwestie w zakresie bezpieczeństwa i odpowiadają wspólnym dla Unii Europejskiej i Stanów Zjednoczonych interesom bezpieczeństwa, a jednocześnie gwarantują wysoki poziom ochrony danych osobowych. Ponadto Unia Europejska i Stany Zjednoczone prowadzą obecnie negocjacje w sprawie umowy ramowej o ochronie danych w obszarze współpracy policyjnej i wymiarów sprawiedliwości (tzw. „umowa ramowa”)⁶. Celem jest zapewnienie wysokiego poziomu ochrony danych obywateli, których dane są przedmiotem wymiany, a tym samym dalsze zacieśnianie współpracy między Unią Europejską i Stanami Zjednoczonymi w zwalczaniu przestępczości i terroryzmu na podstawie wspólnych wartości i zatwierdzonych gwarancji.

Instrumenty te działają w środowisku, w którym przepływy danych osobowych zyskują coraz większe znaczenie.

Z jednej strony rozwój gospodarki cyfrowej doprowadził do gwałtownego wzrostu ilości, jakości, różnorodności i charakteru działań związanych z przetwarzaniem danych. Obywatele w coraz większym stopniu wykorzystują w codziennym życiu usługi łączności elektronicznej. Dane osobowe stały się bardzo cennym aktywem: szacowana wartość danych obywateli Unii wyniosła 315 mld EUR w 2011 r. i niewykluczone, że do 2020 r. wzrośnie do niemal 1 bln rocznie⁷. Rynek analizy dużych zbiorów danych rozwija się w tempie 40 % rocznie w skali ogólnoswiatowej⁸. Również innowacje technologiczne, np. związane z chmurą obliczeniową, umożliwiają szersze spojrzenie na pojęcie międzynarodowego przekazywania danych, w miarę jak przepływy danych transgranicznych stają się codzienną rzeczywistością⁹.

W wyniku wzrostu wykorzystania usług łączności elektronicznej i przetwarzania danych, w tym chmury obliczeniowej, znacznie rozszerzył się również zakres i znaczenie transatlantyckich transferów danych. Jeszcze bardziej istotne stały się takie kwestie, jak kluczowa pozycja przedsiębiorstw amerykańskich w gospodarce cyfrowej¹⁰, *routing* transatlantycki dużej części łączności elektronicznej oraz wielkość elektronicznych przepływów danych między Unią Europejską i Stanami Zjednoczonymi.

Z drugiej strony nowoczesne metody przetwarzania danych osobowych pociągają za sobą nowe i istotne kwestie. Dotyczy to zarówno nowych środków przetwarzania danych konsumentów na dużą skalę przez przedsiębiorstwa prywatne do celów komercyjnych, jak i zwiększonych możliwości szeroko zakrojonego nadzoru nad danymi komunikacyjnymi przez służby wywiadowcze.

Szeroko zakrojone programy gromadzenia danych przez amerykańskie służby wywiadowcze, takie jak PRISM, wpływają na prawa podstawowe Europejczyków, a zwłaszcza prawo do prywatności i ochrony danych osobowych. Programy te wskazują również na związek między

⁵ Decyzja Rady z dnia 13 lipca 2010 r. w sprawie zawarcia Umowy między Unią Europejską 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, Dz.U. L 195 z 27.7.2010, s. 3.

⁶ W dniu 3 grudnia 2010 r. Rada przyjęła decyzję upoważniającą Komisję do negocjowania umowy. Zob. IP/10/1661 z dnia 3 grudnia 2010 r.

⁷ Zob. Boston Consulting Group, „The Value of our Digital Identity”, listopad 2012 r.

⁸ Zob. McKinsey, „Big data: The next frontier for innovation, competition, and productivity”, 2011.

⁹ Komunikat pt.: Wykorzystanie potencjału chmury obliczeniowej w Europie, COM(2012) 529 final.

¹⁰ Przykładowo łączna liczba użytkowników o niepowtarzalnej identyfikacji korzystających z Microsoft Hotmail, Google Gmail i Yahoo! Mail z państw europejskich w czerwcu 2012 wyniosła ponad 227 mln, co znacznie przewyższa wyniki wszystkich innych dostawców. Łączna liczba użytkowników o niepowtarzalnej identyfikacji z Unii mających dostęp do aplikacji Facebook i Facebook Mobile w marcu 2012 r. wyniosła 196,5 mln, czyniąc Facebook największą siecią społecznościową w Europie. Google jest wiodącą wyszukiwarką internetową, z której korzysta 90,2 % użytkowników internetu na całym świecie. Z amerykańskiej mobilnej usługi przesyłania wiadomości What's App w czerwcu 2013 r. skorzystało 91 % użytkowników iPhone'a w Niemczech.

nadzorem rządowym a przetwarzaniem danych przez przedsiębiorstwa prywatne, w szczególności przez amerykańskie przedsiębiorstwa internetowe. W rezultacie mogą one oddziaływać na gospodarkę. Jeżeli obywatele są zaniepokojeni szeroko zakrojonym przetwarzaniem ich danych osobowych przez przedsiębiorstwa prywatne lub monitorowaniem ich danych przez służby wywiadowcze, gdy korzystają oni z usług internetowych, może to wpłynąć na ich zaufanie do gospodarki cyfrowej i ewentualnie negatywnie odbić się na wzroście gospodarczym.

W wyniku tych zmian przepływ danych między Unią Europejską a Stanami Zjednoczonymi napotyka nowe wyzwania. Niniejszy komunikat stanowi odpowiedź na te wyzwania. Przeanalizowano w nim przyszłe działania na podstawie ustaleń zawartych w sprawozdaniu współprzewodniczących z ramienia UE w grupie roboczej *ad hoc* UE-USA i w komunikacie w sprawie zasad bezpiecznego transferu danych osobowych.

Celem komunikatu jest zaproponowanie skutecznego sposobu przywrócenia zaufania i zacieśnienia współpracy między Unią Europejską a Stanami Zjednoczonymi we wspomnianych dziedzinach oraz wzmocnienia szerszych stosunków transatlantyckich.

Niniejszy komunikat opiera się na założeniu, że normy ochrony danych osobowych powinny być rozpatrywane we właściwym kontekście, nie wpływając na inne wymiary stosunków UE-USA, w tym na prowadzone obecnie negocjacje w zakresie transatlantyckiego partnerstwa handlowego i inwestycyjnego. Z tego powodu normy ochrony danych nie będą negocjowane w ramach transatlantyckiego partnerstwa handlowego i inwestycyjnego, które zapewni pełne poszanowanie zasad ochrony danych.

Należy pamiętać, że o ile UE może podjąć działania w obszarze kompetencji UE, w szczególności w celu zapewnienia stosowania prawa UE¹¹, o tyle bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego¹².

2. WPLYW NA INSTRUMENTY TRANSFERU DANYCH

Po pierwsze, jeżeli chodzi o dane przekazywane do celów komercyjnych, program „Bezpieczna przystań” okazał się istotnym narzędziem wykorzystywanym do transferów danych między Unią Europejską a Stanami Zjednoczonymi. Jego znaczenie komercyjne wzrosło, w miarę jak przepływ danych osobowych stawał się coraz bardziej znaczący w transatlantyckich stosunkach handlowych. W ciągu ostatnich 13 lat program „Bezpieczna przystań” ewoluował, a obecnie obejmuje on ponad 3 000 przedsiębiorstw, z których ponad połowa wzięła w nim udział w ciągu ostatnich pięciu lat. Wzrosły jednak obawy co do poziomu ochrony danych osobowych obywateli UE przekazywanych do Stanów Zjednoczonych w ramach tego programu. Ze względu na dobrowolny i deklaracyjny charakter systemu wzrosło zainteresowanie jego przejrzystością i kwestią egzekwowania prawa. Chociaż większość przedsiębiorstw amerykańskich stosuje zasady programu „Bezpieczna przystań”, niektóre przedsiębiorstwa, które złożyły oświadczenie o zgodności, tych zasad nie stosują. Nieprzestrzeganie zasad bezpiecznego transferu danych osobowych przez niektóre przedsiębiorstwa, które złożyły oświadczenie o zgodności, daje im przewagę konkurencyjną w stosunku do przedsiębiorstw europejskich funkcjonujących na tych samych rynkach.

Ponadto, podczas gdy w ramach programu „Bezpieczna przystań” ograniczenia zasad ochrony danych są dozwolone w stosownych przypadkach ze względu na bezpieczeństwo narodowe¹³,

¹¹ Zob. wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-300/11, ZZ przeciwko Secretary of State for the Home Department.

¹² Art. 4 ust. 2 Traktatu UE.

powstaje pytanie, czy szeroko zakrojone gromadzenie i przetwarzanie danych osobowych w ramach amerykańskich programów nadzoru jest konieczne i proporcjonalne, aby spełnić oczekiwania w zakresie bezpieczeństwa narodowego. Jak wynika z ustaleń grupy roboczej *ad hoc* UE-USA, w ramach tych programów obywatele Unii nie mogą korzystać z tych samych praw i gwarancji procesowych co obywatele Stanów Zjednoczonych.

Zasięg tych programów nadzoru w połączeniu z nierównym traktowaniem obywateli UE podaje w wątpliwość poziom ochrony zapewniony przez ustalenia w ramach programu „Bezpieczna przystań”. Amerykańskie organy mają dostęp do danych osobowych obywateli Unii przesłanych do Stanów Zjednoczonych w ramach programu „Bezpieczna przystań” i mogą je przetwarzać w sposób niezgodny z powodami, dla których dane te zostały pierwotnie zgromadzone w UE, i niezgodny z celem, dla którego zostały one przekazane Stanom Zjednoczonym. Większość amerykańskich przedsiębiorstw internetowych, których przedmiotowe programy prawdopodobnie dotyczą w bardziej bezpośredni sposób, posiadają poświadczenia zgodności w ramach programu „Bezpieczna przystań”.

Po drugie, jeżeli chodzi o wymianę danych do celów egzekwowania prawa, istniejące umowy (umowa w sprawie danych dotyczących przelotu pasażera, umowa w sprawie Programu śledzenia środków finansowych należących do terrorystów – TFTP) okazały się bardzo cennymi narzędziami do rozwiązywania wspólnych zagrożeń z zakresu bezpieczeństwa związanych z poważną przestępczością międzynarodową i terroryzmem, jednocześnie ustanawiając gwarancje, które zapewniają wysoki poziom ochrony danych¹⁴. Gwarancje te obejmują swoim zasięgiem obywateli Unii, zaś umowy przewidują mechanizmy służące do przeprowadzania przeglądu ich wdrażania i rozwiązywania problematycznych kwestii z tym związanych. Na mocy umowy w sprawie programu TFTP ustanowiono również system nadzoru, w ramach którego niezależne organy nadzorcze UE sprawdzają, w jaki sposób dane objęte umową są wyszukiwane przez Stany Zjednoczone.

W kontekście obaw wyrażonych w UE w odniesieniu do amerykańskich programów nadzoru Komisja Europejska wykorzystała te mechanizmy w celu sprawdzenia, w jakim stopniu umowy te są stosowane. W przypadku umowy w sprawie danych dotyczących przelotu pasażera przeprowadzono wspólny przegląd z udziałem unijnych i amerykańskich ekspertów w zakresie ochrony danych, podczas którego przeanalizowano sposób, w jaki zrealizowano umowę¹⁵. W wyniku przeglądu nie uzyskano żadnych wskazówek dotyczących rozszerzenia amerykańskich programów nadzoru na dane pasażerów objęte umową w sprawie danych dotyczących przelotu pasażera ani dowodów na to, że programy miały wpływ na wspomniane dane. W przypadku umowy w sprawie programu TFTP Komisja rozpoczęła formalne konsultacje po przedstawieniu zarzutów amerykańskim służbom wywiadowczym, które posiadały bezpośredni dostęp do danych osobowych w UE wbrew postanowieniom umowy. W wyniku tych konsultacji nie ujawniono jakichkolwiek elementów potwierdzających naruszenie umowy w sprawie programu TFTP, a Stany Zjednoczone muszą przedstawić pisemne zapewnienie, że nie doszło do żadnego bezpośredniego gromadzenia danych, które byłoby sprzeczne z postanowieniami umowy.

¹³ Zob. np. decyzja w sprawie ochrony prywatności w ramach „Bezpiecznej przystani”, załącznik I.

¹⁴ Zob. wspólne sprawozdanie Komisji i Departamentu Skarbu Stanów Zjednoczonych dotyczące wartości danych dostarczonych w ramach programu TFTP na podstawie art. 6 ust. 6 Umowy między Unią Europejską 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.

¹⁵ Zob. sprawozdanie Komisji „Wspólny przegląd z wdrożenia Umowy zawartej między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych”.

Gromadzenie i przetwarzanie danych osobowych na szeroką skalę w ramach amerykańskich programów nadzoru wiąże się jednak z koniecznością prowadzenia dalszego dokładnego monitorowania wykonania umowy w sprawie danych dotyczących przelotu pasażera i umowy w sprawie programu TFTP w przyszłości. W związku z tym Unia Europejska i Stany Zjednoczone uzgodniły, że wiosną 2014 r. przeprowadzą kolejny wspólny przegląd umowy w sprawie programu TFTP. Celem tego przeglądu i kolejnych przeglądów będzie zapewnienie większej przejrzystości w zakresie funkcjonowania systemu nadzoru i sposobu ochrony danych obywateli UE. Równolegle podjęte zostaną kroki w celu zagwarantowania, że w ramach systemu nadzoru w dalszym ciągu będzie się dokładnie analizować sposób przetwarzania danych przekazanych Stanom Zjednoczonym na podstawie umowy, ze szczególnym uwzględnieniem sposobu udostępniania takich danych poszczególnym organom USA.

Po trzecie, wzrost ilości przetwarzanych danych osobowych świadczy o znaczeniu gwarancji prawnych i administracyjnych, które mają zastosowanie. Grupa robocza *ad hoc* UE-USA miała na celu m.in. ustalenie, jakie stosuje się gwarancje, aby zminimalizować wpływ przetwarzania na prawa podstawowe obywateli Unii. Gwarancje są również niezbędne w celu ochrony przedsiębiorstw. Niektóre amerykańskie przepisy, takie jak ustawa „Patriot Act”, zezwalają amerykańskim organom na bezpośrednie wzywanie przedsiębiorstw do udostępnienia im danych przechowywanych w Unii Europejskiej. Przedsiębiorstwa europejskie i amerykańskie mające swoje siedziby w Unii Europejskiej mogą zatem ewentualnie mieć obowiązek przekazywania danych do Stanów Zjednoczonych z naruszeniem przepisów UE i państw członkowskich, a w rezultacie mają do czynienia z kolizyjnymi zobowiązaniami prawnymi. Niepewność prawa wynikająca z takich bezpośrednich wezwań może wstrzymać rozwój nowych usług cyfrowych, takich jak chmura obliczeniowa, które mogą zapewnić skuteczne i tańsze rozwiązania osobom fizycznym i przedsiębiorstwom.

3. ZAPEWNIENIE SKUTECZNOŚCI OCHRONY DANYCH

Transfer danych osobowych między Unią Europejską i Stanami Zjednoczonymi stanowi niezbędny element transatlantyckich stosunków handlowych. Wymiana informacji odgrywa również istotną rolę we współpracy Unii Europejskiej i Stanów Zjednoczonych w zakresie bezpieczeństwa, szczególnie jeżeli chodzi o osiągnięcie wspólnego celu, jakim jest zapobieganie poważnej przestępczości i terroryzmowi oraz ich zwalczanie. Ostatnie doniesienia o programach gromadzenia danych przez amerykańskie służby wywiadowcze podważyły jednak zaufanie, na którym opiera się ta współpraca. W szczególności dotyczy to zaufania do sposobu, w jaki dane osobowe są przetwarzane. Aby odbudować zaufanie do transferów danych na korzyść gospodarki cyfrowej, bezpieczeństwa zarówno w Unii Europejskiej, jak i w Stanach Zjednoczonych oraz szerszych stosunków transatlantyckich, należy podjąć następujące kroki.

3.1. Reforma systemu ochrony danych w UE

Reforma systemu ochrony danych zaproponowana przez Komisję w styczniu 2012 r.¹⁶ stanowi kluczowe działanie w zakresie ochrony danych osobowych. Szczególne znaczenie ma pięć elementów zawartych w przedłożonym pakiecie ochrony danych.

¹⁶ COM(2012) 10 final: Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu danych, Bruksela, dnia 25.1.2012 r. i COM(2012) 11 final: wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych).

Po pierwsze, jeżeli chodzi o zakres terytorialny, z przedłożonego rozporządzenia jasno wynika, że przedsiębiorstwa niemające swojej siedziby w Unii będą musiały stosować się do unijnych przepisów w zakresie ochrony danych, aby móc oferować swoje towary i usługi konsumentom Unii lub monitorować ich zachowanie. Innymi słowy, prawo podstawowe do ochrony danych będzie przestrzegane niezależnie od położenia geograficznego przedsiębiorstwa lub jednostki, w której dokonuje się przetwarzania¹⁷.

Po drugie, w odniesieniu do transferów międzynarodowych w przedłożonym rozporządzeniu ustanowiono warunki, na jakich możliwe jest przekazywanie danych poza UE. Transfery danych dozwolone są jedynie wtedy, gdy spełnione są wspomniane warunki gwarantujące wysoki poziom ochrony praw poszczególnych osób¹⁸.

Po trzecie, jeżeli chodzi o egzekwowanie prawa, zaproponowane przepisy przewidują proporcjonalne i odstrasżające sankcje (do 2 % rocznych obrotów przedsiębiorstwa na całym świecie), mające zapewnić przestrzeganie prawa UE przez przedsiębiorstwa¹⁹. Dzięki istnieniu wiarygodnych sankcji wzrośnie motywacja przedsiębiorstw do przestrzegania prawa UE.

Po czwarte, przedłożone rozporządzenie zawiera jasne przepisy dotyczące obowiązków i zobowiązań przetwarzających takich jak dostawcy usług w chmurze, w tym w zakresie bezpieczeństwa²⁰. Jak wynika z doniesień o programach gromadzenia danych przez amerykańskie służby wywiadowcze jest to bardzo istotne ze względu na fakt, że programy te obejmują swoim zasięgiem dane przechowywane w chmurze obliczeniowej. Ponadto przedsiębiorstwa zapewniające powierzchnię służącą do przechowywania w chmurze obliczeniowej, które zostaną wezwane do przekazania danych osobowych władzom zagranicznym, nie będą w stanie uniknąć odpowiedzialności, powołując się na swój status przetwarzającego, a nie administratora danych.

Po piąte, dzięki pakietowi zostaną ustanowione kompleksowe zasady ochrony danych osobowych przetwarzanych w sektorze egzekwowania prawa.

Oczekuje się, że pakiet zostanie zatwierdzony w odpowiednich ramach czasowych w 2014 r.²¹.

¹⁷ Komisja odnotowuje, że Parlament Europejski potwierdził i wzmocnił tę ważną zasadę zapisaną w art. 3 rozporządzenia, którego dotyczy wniosek, podczas głosowania w dniu 21 października 2013 r. w sprawie sprawozdań dotyczących reformy systemu ochrony danych sporządzonych przez posłów do Parlamentu Europejskiego Jan-Philippa Albrechta i Dimitriosą Droutsasa z Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE).

¹⁸ Komisja odnotowuje, że podczas głosowania w dniu 21 października 2013 r. Komisja LIBE Parlamentu Europejskiego zaproponowała włączenie do przyszłego rozporządzenia przepisu, na mocy którego wezwanie władz zagranicznych do udostępnienia danych osobowych zgromadzonych w UE wymagałoby uzyskania wcześniejszej zgody krajowego organu ds. ochrony danych, jeżeli takie wezwanie zostałoby wydane poza traktatem o wzajemnej pomocy prawnej lub inną umową międzynarodową.

¹⁹ Komisja odnotowuje, że podczas głosowania w dniu 21 października 2013 r. Komisja LIBE zaproponowała wzmocnienie wniosku Komisji poprzez zapewnienie zwiększenia grzywnien nawet do 5 % rocznego obrotu przedsiębiorstwa na całym świecie.

²⁰ Komisja odnotowuje, że podczas głosowania w dniu 21 października 2013 r. Komisja LIBE zatwierdziła wzmocnienie obowiązków i zobowiązań przetwarzających, w szczególności w odniesieniu do art. 26 rozporządzenia, którego dotyczy wniosek.

²¹ Rada Europejska w konkluzjach z października 2013 r. stwierdza że: „Ważne jest budowanie zaufania obywateli i przedsiębiorstw do gospodarki cyfrowej. Terminowe przyjęcie solidnych unijnych ogólnych ram ochrony danych i dyrektywy w sprawie bezpieczeństwa cybernetycznego ma kluczowe znaczenie dla ukończenia tworzenia jednolitego rynku cyfrowego do 2015 r.”.

3.2. Zwiększenie bezpieczeństwa w ramach programu „Bezpieczna przystań”

Program „Bezpieczna przystań” stanowi ważny element stosunków handlowych między Unią Europejską a Stanami Zjednoczonymi – utrzymywanych przez przedsiębiorstwa po obu stronach Atlantyku.

W sprawozdaniu w sprawie funkcjonowania programu „Bezpieczna przystań” Komisja wskazała szereg uchybień w tym programie. W wyniku braku przejrzystości i nieegzekwowania prawa niektórzy członkowie programu „Bezpieczna przystań”, którzy poświadczyli zgodność, w praktyce nie stosują się do jego zasad. Ma to negatywny wpływ na prawa podstawowe obywateli Unii. Ponadto stawia to przedsiębiorstwa europejskie w niekorzystnej sytuacji w porównaniu z konkurencyjnymi przedsiębiorstwami amerykańskimi, które działają w ramach programu, ale w praktyce nie stosują się do jego zasad. Tego rodzaju niedoskonałość ma również wpływ na większość przedsiębiorstw amerykańskich, które prawidłowo stosują ten program. Program „Bezpieczna przystań” działa również jako kanał do przekazywania danych osobowych obywateli Unii z Unii Europejskiej do Stanów Zjednoczonych za pośrednictwem przedsiębiorstw zobowiązanych do przekazania danych amerykańskim służbom wywiadowczym w ramach amerykańskich programów gromadzenia danych. Jeżeli uchybienia te nie zostaną naprawione, przedmiotowy program będzie stwarzać niekorzystne warunki konkurencji dla przedsiębiorstw w UE i wpływać negatywnie na prawo podstawowe do ochrony danych obywateli Unii.

Odpowiadając na ostatnie doniesienia w sprawie nadzoru, europejskie organy ochrony danych podkreśliły braki programu „Bezpieczna przystań”. W art. 3 decyzji w sprawie ochrony prywatności w ramach „Bezpiecznej przystani” organy te są upoważnione do zawieszenia w określonych sytuacjach przepływów danych do przedsiębiorstw, które poświadczyli zgodność²². Niemieccy komisarze ds. ochrony danych postanowili nie wydawać nowych zezwoleń na transfer danych do państw trzecich (np. w celu korzystania z niektórych usług w chmurze). Komisarze zbadają również, czy należy zawiesić transfery danych w ramach programu „Bezpieczna przystań”²³. Istnieje ryzyko, że takie działania podejmowane na szczeblu krajowym stworzyłyby różnice w zasięgu, co oznacza, że program „Bezpieczna przystań” przestałby być kluczowym mechanizmem służącym do transferu danych osobowych między Unią Europejską i Stanami Zjednoczonymi.

Komisja jest upoważniona na mocy dyrektywy 95/46/WE do zawieszenia lub uchylecia decyzji w sprawie ochrony prywatności w ramach „Bezpiecznej przystani”, jeżeli program nie zapewnia już odpowiedniego poziomu ochrony. Ponadto na mocy art. 3 decyzji w sprawie ochrony prywatności w ramach „Bezpiecznej przystani” Komisja może uchylić lub zawiesić decyzję bądź ograniczyć jej zakres, natomiast na mocy art. 4 może dostosować tę decyzję w dowolnym czasie w świetle doświadczenia uzyskanego podczas wprowadzania jej w życie.

W związku z tym można rozważyć szereg wariantów strategicznych, m.in.:

- utrzymanie *statusu quo*;
- udoskonalenie programu „Bezpieczna przystań” i wykonanie szczegółowego przeglądu jego funkcjonowania;

²² W szczególności zgodnie z art. 3 decyzji w sprawie ochrony prywatności w ramach „Bezpiecznej przystani” takie zawieszenie ma miejsce, w przypadku gdy istnieje duże prawdopodobieństwo, że zasady są łamane; istnieje uzasadnione domniemanie, że w ramach mechanizmu realizacji prawa o którym mowa nie podejmuje się lub nie podejmuje się właściwych kroków w odpowiednim czasie w celu załatwienia spornej sprawy; dalszy przekaz tworzyłby bezpośrednie ryzyko wystąpienia poważnej szkody dla osób, których dane dotyczą; a właściwe władze państwa członkowskiego dołożyły należytych starań w tych okolicznościach w celu powiadomienia danej organizacji i umożliwienia udzielenia odpowiedzi.

²³ Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, komunikat prasowy z dnia 24 lipca 2013 r.

- zawieszenie lub uchylenie decyzji w sprawie ochrony prywatności w ramach „Bezpiecznej przystani”.

Z uwagi na zidentyfikowane uchybienia nie można kontynuować wdrażania decyzji w sprawie ochrony prywatności w ramach „Bezpiecznej przystani” w obecnej formie. Uchylenie decyzji wpłynęłoby jednak negatywnie na interesy przedsiębiorstw członkowskich w Unii Europejskiej i Stanach Zjednoczonych. Komisja uważa, że program „Bezpieczna przystań” należy raczej udoskonalić.

Ulepszenia powinny dotyczyć zarówno braków strukturalnych związanych z przejrzystością i egzekwowaniem prawa, jak i konkretnych zasad bezpiecznego transferu danych osobowych i funkcjonowania klauzuli bezpieczeństwa narodowego.

W szczególności, aby program „Bezpieczna przystań” działał zgodnie z przeznaczeniem, amerykańskie władze powinny w bardziej skuteczny i systematyczny sposób monitorować i nadzorować przedsiębiorstwa, które poświadczyły zgodność, pod względem przestrzegania zasad bezpiecznego transferu danych osobowych. Udoskonalenia wymaga przejrzystość polityki prywatności przedsiębiorstw, które poświadczyły zgodność. Obywatelom Unii należy również zapewnić dostępność i przystępność mechanizmów rozstrzygania sporów.

Komisja będzie współpracować z amerykańskimi władzami w trybie pilnym w celu omówienia zidentyfikowanych braków. Środki zaradcze należy określić przed latem 2014 r. i jak najszybciej je wdrożyć. Na tej podstawie Komisja przeprowadzi pełny bilans funkcjonowania programu „Bezpieczna przystań”. Ten szeroko zakrojony proces przeglądu powinien objąć otwarte konsultacje i debatę w Parlamencie Europejskim i Radzie oraz dyskusje z amerykańskimi władzami.

Istotne jest również, aby klauzulę bezpieczeństwa narodowego, przewidzianą decyzją w sprawie ochrony prywatności w ramach „Bezpiecznej przystani”, wykorzystywano jedynie w zakresie, który jest bezwzględnie konieczny i proporcjonalny.

3.3. Wzmocnienie gwarancji ochrony danych w ramach współpracy w zakresie egzekwowania prawa

Unia Europejska i Stany Zjednoczone prowadzą obecnie negocjacje w sprawie umowy ramowej o ochronie danych, tj. transferów i przetwarzania danych osobowych w kontekście współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Zawarcie takiej umowy zapewniającej wysoki poziom ochrony danych osobowych będzie mieć znaczący wpływ na umocnienie zaufania po obu stronach Atlantyku. Dzięki pogłębieniu ochrony praw obywateli Unii w zakresie danych nastąpiłoby wzmocnienie współpracy transatlantyckiej mającej na celu zapobieganie przestępczości i terroryzmowi oraz ich zwalczanie.

Zgodnie z celem decyzji upoważniającej Komisję do negocjowania umowy ramowej celem negocjacji powinno być zapewnienie wysokiego poziomu ochrony zgodnie z dorobkiem UE w zakresie ochrony danych. Powinno to znaleźć odzwierciedlenie w zatwierdzonych przepisach i gwarancjach dotyczących m.in. zasady celowości czy warunków i okresu przechowywania danych. W kontekście negocjacji Komisja powinna również uzyskać zobowiązania dotyczące możliwych do wyegzekwowania praw, w tym sądowych mechanizmów odwoławczych dla obywateli Unii niemających prawa pobytu w Stanach Zjednoczonych²⁴. Bliska współpraca między Unią Europejską i Stanami Zjednoczonymi

²⁴

Zob. odpowiedni fragment wspólnego oświadczenia prasowego opublikowanego po posiedzeniu ministerialnym UE-USA dotyczącym wymiaru sprawiedliwości i spraw wewnętrznych, które odbyło się w dniu 18 listopada 2013 r. w Waszyngtonie: „Jesteśmy zatem zobowiązani do poczynienia szybkich postępów w negocjacjach dotyczących istotnej i kompleksowej umowy ramowej o ochronie danych w dziedzinie egzekwowania prawa, ponieważ jest to sprawa niecierpiąca zwłoki. Umowa posłuży jako podstawa do ułatwienia transferów danych w kontekście współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych poprzez zapewnienie wysokiego poziomu ochrony

poświęcona wspólnym wyzwaniom z zakresu bezpieczeństwa powinna znaleźć odzwierciedlenie w wysiłkach podejmowanych w celu zagwarantowania, że obywatele korzystają z tych samych praw, gdy te same dane są przetwarzane do tych samych celów po obu stronach Atlantyku. Ważne jest również zapewnienie wąskiej definicji odstępstw dla celów z zakresu bezpieczeństwa narodowego. W tej dziedzinie należy uzgodnić gwarancje i ograniczenia.

Wspomniane negocjacje są okazją do wyjaśnienia, że dane osobowe będące w posiadaniu przedsiębiorstw prywatnych i znajdujące się w UE nie będą w sposób bezpośredni udostępniane ani przekazywane amerykańskim organom ścigania poza formalnymi kanałami współpracy, takimi jak umowa o wzajemnej pomocy prawnej lub sektorowe umowy zawarte między Unią Europejską i Stanami Zjednoczonymi zezwalające na tego typu transfery. Dostęp za pomocą innych środków powinien być zabroniony, chyba że ma miejsce w ściśle określonych i wyjątkowych sytuacjach, które mogą zostać poddane kontroli sądowej. Stany Zjednoczone powinny podjąć zobowiązania w tym zakresie²⁵.

Umowa ramowa zatwierdzona zgodnie z powyższymi zasadami powinna ustanowić ogólne ramy, aby zapewnić wysoki poziom ochrony danych osobowych podczas ich transferu do Stanów Zjednoczonych do celów zapobiegania przestępczości i terroryzmowi lub ich zwalczania. W umowach sektorowych należy w stosownych przypadkach, ze względu na charakter danego transferu danych, ustanowić dodatkowe przepisy i gwarancje, bazując na przykładzie umów zawartych między Unią Europejską i Stanami Zjednoczonymi, tj. umowy w sprawie danych dotyczących przelotu pasażera i umowy w sprawie programu TFTP, w których określono ściśle warunki transferu danych i gwarancji w odniesieniu do obywateli Unii.

3.4. Rozwiązywanie problemów Unii związanych z trwającym procesem reform w Stanach Zjednoczonych

Prezydent Stanów Zjednoczonych Barack Obama ogłosił przegląd działań krajowych organów bezpieczeństwa w Stanach Zjednoczonych, w tym mających zastosowanie ram prawnych. Wspomniany bieżący proces stwarza wyjątkową okazję do rozwiania obaw UE, jakie powstały w wyniku ostatnich doniesień o programach gromadzenia danych przez amerykańskie służby wywiadowcze. Najważniejsze zmiany dotyczyłyby rozszerzenia gwarancji przysługujących obywatelom i osobom mającym prawo pobytu w Stanach Zjednoczonych na obywateli Unii niemających prawa pobytu w Stanach Zjednoczonych, a także zwiększonej przejrzystości działań wywiadowczych i dalszego wzmacniania nadzoru. W wyniku tych zmian przywrócono by zaufanie do wymiany danych między Unią Europejską i Stanami Zjednoczonymi oraz promowano by korzystanie z usług internetowych wśród Europejczyków.

danych osobowych obywatelom USA i Unii. Zobowiązaliśmy się do pracy na rzecz rozwiązania pozostałych kwestii poruszonych przez obie strony, w tym związanych z sądowymi środkami odwoławczymi (kluczowa kwestia dla UE). Naszym celem jest zakończenie negocjacji dotyczących umowy przed latem 2014 r.”.

²⁵ Zob. odpowiedni fragment wspólnego oświadczenia prasowego opublikowanego po posiedzeniu ministerialnym wymiaru sprawiedliwości i spraw wewnętrznych UE-USA, które odbyło się w dniu 18 listopada 2013 r. w Waszyngtonie: „Podkreślamy także wartość Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej. Podtrzymujemy nasze zobowiązanie do zapewnienia szerokiego i skutecznego stosowania tej umowy do celów dowodowych w postępowaniu karnym. Przeprowadziliśmy również dyskusje na temat konieczności wyjaśnienia faktu, iż dane osobowe będące w posiadaniu podmiotów prywatnych na terytorium drugiej strony nie zostaną udostępnione organom ścigania poza prawnie dozwolonymi kanałami. Zgodziliśmy się również dokonać przeglądu funkcjonowania umowy o wzajemnej pomocy prawnej, jak przewidziano w umowie, i konsultować się w razie potrzeby z drugą stroną”.

Jeżeli chodzi o rozszerzenie gwarancji dostępnych obywatelom i osobom mającym prawo pobytu w Stanach Zjednoczonych na obywateli Unii, należy dokonać przeglądu norm prawnych w stosunku do amerykańskich programów nadzoru, które traktują obywateli Stanów Zjednoczonych i Unii Europejskiej w odmienny sposób, w tym z perspektywy konieczności i proporcjonalności, mając na uwadze bliskie partnerstwo transatlantyckie w zakresie bezpieczeństwa oparte na wspólnych wartościach, prawach i wolnościach. Pozwoliłoby to zmniejszyć skalę wpływu programów gromadzenia danych przez amerykańskie służby wywiadowcze na obywateli Unii.

Konieczna jest większa przejrzystość ram prawnych w odniesieniu do programów gromadzenia danych przez amerykańskie służby wywiadowcze i ich interpretacji przez sądy amerykańskie, jak również większa przejrzystość wymiaru ilościowego programów gromadzenia danych. Na tych zmianach skorzystaliby również obywatele Unii.

Dzięki wzmocnieniu roli sądu ds. nadzoru wywiadu zagranicznego (j.ang. Foreign Intelligence Surveillance Court) i wprowadzeniu środków odwoławczych dla osób fizycznych poprawie uległby nadzór nad programami gromadzenia danych przez amerykańskie służby wywiadowcze. Mechanizmy te mogłyby ograniczyć proces przetwarzania danych osobowych Europejczyków, które nie są istotne do celów bezpieczeństwa narodowego.

3.5. Promowanie norm z zakresu prywatności na szczeblu międzynarodowym

Kwestie związane ze stosowaniem nowoczesnych metod ochrony danych nie ograniczają się do transferu danych między Unią Europejską i Stanami Zjednoczonymi. Wysoki poziom ochrony danych osobowych należy również zagwarantować każdej osobie fizycznej. Przepisy UE dotyczące gromadzenia, przetwarzania i przekazywania danych należy promować na szczeblu międzynarodowym.

Ostatnio zaproponowano szereg inicjatyw mających na celu promowanie ochrony prywatności, w szczególności w internecie²⁶. Unia Europejska powinna zapewnić, aby w ramach tych inicjatyw, o ile będą one realizowane, w pełni uwzględniono zasady ochrony praw podstawowych, wolności wypowiedzi, danych osobowych i prywatności, zgodnie z prawem UE i europejską strategią bezpieczeństwa cybernetycznego, a także nie podważano wolności, otwartości i bezpieczeństwa cyberprzestrzeni. Oznacza to demokratyczny i efektywny model zarządzania obejmujący wiele zainteresowanych stron.

Trwające reformy przepisów z zakresu ochrony danych po obu stronach Atlantyku stanowią również wyjątkową okazję dla Unii Europejskiej i Stanów Zjednoczonych do ustanowienia norm na poziomie międzynarodowym. Wymiana danych na obszarze Atlantyku i poza nim odniesie znaczne korzyści ze wzmocnienia amerykańskich krajowych ram prawnych, w tym fragmentu „Karty praw konsumentów w zakresie prywatności” ogłoszonej przez prezydenta Obamę w lutym 2012 r. w ramach kompleksowego planu działania mającego na celu poprawę ochrony prywatności konsumentów. Istnienie zbioru konsekwentnych i podlegających wykonaniu przepisów z zakresu ochrony danych przewidzianych w unijnym i amerykańskim prawie stanowiłoby solidną podstawę dla transgranicznych przepływów danych.

Z uwagi na promowanie norm prywatności na szczeblu międzynarodowym należy również zachęcać do przystąpienia do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych („Konwencja 108”), która jest otwarta dla państw niebędących członkami Rady Europy²⁷. Zabezpieczenia i gwarancje uzgodnione na forach międzynarodowych powinny przyczynić się do wysokiego poziomu ochrony zgodnego z wymogami prawa UE.

²⁶ Zob. w tym kontekście projekt rezolucji zaproponowany Zgromadzeniu Ogólnemu ONZ przez Niemcy i Brazylię – w którym wzywa się do ochrony prywatności w internecie i poza nim.

²⁷ USA jest już stroną innej konwencji Rady Europy tj. Konwencji o cyberprzestępczości z 2001 r. (znanej również jako „konwencja z Budapesztu”).

4. WNIOSKI I ZALECENIA

Kwestie zidentyfikowane w niniejszym komunikacie wymagają podjęcia działań przez Stany Zjednoczone, Unię Europejską i jej państwa członkowskie.

Obawy związane z transatlantycką wymianą danych to przede wszystkim sygnał ostrzegawczy dla UE i jej państw członkowskich świadczący o konieczności przeprowadzenia szybkiej i ambitnej reformy ochrony danych. Jak widać, konsekwentne ramy legislacyjne z jasnymi przepisami, wykonalnymi również w sytuacjach, gdy dane przekazuje się zagranicę, są konieczne w jeszcze większym stopniu niż kiedykolwiek do tej pory. Instytucje UE powinny kontynuować zatem prace nad przyjęciem reformy ochrony danych do wiosny 2014 r., aby mieć pewność, że dane osobowe są skutecznie i spójnie chronione.

Z uwagi na znaczenie transatlantyckich przepływów danych istotne jest, aby instrumenty, na których opiera się ta wymiana, właściwie uwzględniały wyzwania i możliwości związane z erą cyfrową i nowymi rozwiązaniami technologicznymi takimi jak chmura obliczeniowa. Istniejące i przyszłe porozumienia i umowy powinny zapewnić ciągłość wysokiego poziomu ochrony po obu stronach Atlantyku.

Sprawnie działający program „Bezpieczna przystań” leży w interesie obywateli Unii Europejskiej i Stanów Zjednoczonych oraz przedsiębiorstw. Program ten należy udoskonalić poprzez lepsze monitorowanie i wdrażanie w perspektywie krótkoterminowej, a na tej podstawie również poprzez dokładniejszy przegląd jego funkcjonowania. Ulepszenia są niezbędne, aby zagwarantować, że pierwotne cele decyzji w sprawie ochrony prywatności w ramach „Bezpiecznej przystani”, tj. ciągłość ochrony danych, pewność prawa i swobodny przepływ danych między Unią Europejską i Stanami Zjednoczonymi, są w dalszym ciągu realizowane.

W ramach tych ulepszeń amerykańskie władze powinny przede wszystkim skupić się na poprawie nadzoru i monitorowania przedsiębiorstw, które poświadczyły zgodność, pod względem przestrzegania zasad bezpiecznego transferu danych osobowych.

Istotne jest również, aby klauzulę bezpieczeństwa narodowego przewidzianą decyzją w sprawie ochrony prywatności w ramach „Bezpiecznej przystani” wykorzystywano jedynie w zakresie, który jest bezwzględnie konieczny i proporcjonalny.

W obszarze egzekwowania prawa trwające negocjacje dotyczące umowy ramowej powinny skutkować wysokim poziomem ochrony obywateli po obu stronach Atlantyku. Taka umowa zwiększy zaufanie obywateli Unii do wymiany danych między Unią Europejską a Stanami Zjednoczonymi i będzie stanowić podstawę do dalszego rozwijania współpracy i partnerstwa w zakresie bezpieczeństwa między Unią Europejską a Stanami Zjednoczonymi. W ramach negocjacji należy uzyskać zobowiązania, z których wynikałoby, że gwarancje procesowe, w tym sądowe środki odwoławcze, będą dostępne dla obywateli Unii, którzy nie mają prawa pobytu w Stanach Zjednoczonych.

Należy zabiegać o to, aby amerykańska administracja zobowiązała się do zagwarantowania, że dane osobowe będące w posiadaniu podmiotów prywatnych w UE nie zostaną w sposób bezpośredni udostępnione amerykańskim organom ścigania poza formalnymi kanałami współpracy, takimi jak umowa o wzajemnej pomocy prawnej i umowy sektorowe zawarte między Unią Europejską a Stanami Zjednoczonymi – np. umowa w sprawie danych dotyczących przelotu pasażera i umowa w sprawie programu TFTP, zezwalającymi na tego typu transfery na ściśle określonych warunkach, z wyjątkiem jasno zdefiniowanych, wyjątkowych sytuacji podlegających kontroli sądowej.

Stany Zjednoczone powinny również rozszerzyć gwarancje przysługujące obywatelom i osobom mającym prawo pobytu w Stanach Zjednoczonych na obywateli Unii, zapewnić konieczność i proporcjonalność programów, większą przejrzystość ram prawnych mających zastosowanie do amerykańskich krajowych organów bezpieczeństwa i nadzór nad tymi ramami.

Obszary wymienione w niniejszym komunikacie będą wymagać konstruktywnego zaangażowania po obu stronach Atlantyku. Unia Europejska i Stany Zjednoczone – wspólnie

jako partnerzy strategiczni – są w stanie przezwyciężyć obecne napięcia w stosunkach transatlantyckich i odbudować zaufanie do przepływów danych między Unią Europejską i Stanami Zjednoczonymi. Podejmowanie wspólnych zobowiązań politycznych i prawnych w zakresie dalszej współpracy w tych obszarach przyczyni się do wzmocnienia ogólnych stosunków transatlantyckich.