EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach unijno-amerykańskiej ochrony prywatności (*Privacy Shield*)

(Pełny tekst niniejszej opinii jest dostępny w wersji angielskiej, francuskiej i niemieckiej na stronie internetowej EIOD: www.edps.europa.eu)

(2016/C 257/05)

Przepływy danych mają wymiar globalny. Unia Europejska jest zobowiązana do przestrzegania traktatów i Karty praw podstawowych Unii Europejskiej chroniących wszystkie jednostki w UE. Unia Europejska ma obowiązek podejmować wszystkie kroki konieczne do zapewnienia, aby prawa do prywatności i do ochrony danych osobowych przestrzegano we wszystkich działaniach polegających na przetwarzaniu danych, w tym ich przekazywaniu.

Od czasu ujawnienia działań w zakresie nadzoru w 2013 r. Unia Europejska i jej strategiczny partner – Stany Zjednoczone – dążyli do zdefiniowania nowego zestawu norm w oparciu o autocertyfikację na potrzeby przekazywania do Stanów Zjednoczonych w celach handlowych danych osobowych wysyłanych z UE. Podobnie jak krajowe organy ds. ochrony danych w UE, tak i EIOD – w erze globalnych, natychmiastowych i nieprzewidywalnych przepływów danych – uznaje wartość zrównoważonych ram prawnych na potrzeby handlowego przekazywania danych między Unią Europejską a Stanami Zjednoczonymi, która to relacja stanowi największe partnerstwo handlowe na świecie. Niemniej jednak ramy te muszą w pełni odzwierciedlać wspólne wartości demokratyczne i wartości oparte na prawach jednostki, wyrażone po stronie UE w traktacie lizbońskim oraz Karcie praw podstawowych UE, a po stronie Stanów Zjednoczonych – w konstytucji Stanów Zjednoczonych.

Projekt ochrony prywatności (*Privacy Shield*) może być krokiem we właściwym kierunku, ale w obecnym kształcie – w naszej ocenie – nie uwzględnia odpowiednio wszystkich właściwych środków zabezpieczających unijne prawa jednostek do prywatności i ochrony danych, również jeżeli chodzi o dochodzenie roszczeń na drodze sądowej. Jeżeli Komisja Europejska chce przyjąć decyzję w sprawie odpowiedniej ochrony danych osobowych, konieczne są znaczące ulepszenia. W szczególności UE powinna zyskać dodatkowe zapewnienia w kwestii konieczności i proporcjonalności, zamiast legitymizować rutynowy dostęp organów amerykańskich do przekazywanych danych na podstawie kryteriów wynikających z podstaw prawnych funkcjonujących w kraju otrzymującym, a nie funkcjonujących w UE kryteriów potwierdzonych traktatami, unijnymi orzeczeniami oraz tradycją konstytucyjną wspólną dla państw członkowskich.

Ponadto, w erze dużej hiperłączności i rozproszonych sieci samoregulacja dokonywana przez organizacje prywatne, jak również oświadczenia i zobowiązania urzędników publicznych mogą sprawdzić się w perspektywie krótkoterminowej, jednak w dłuższej perspektywie nie będą wystarczające do zabezpieczenia praw i interesów jednostek oraz pełnego zaspokojenia potrzeb zglobalizowanego świata cyfrowego, w którym wiele państw dysponuje obecnie zasadami ochrony danych.

Z tego względu w dialogu transatlantyckim oczekiwano by rozwiązań długoterminowych, które pozwoliłyby również na ustanowienie w wiążącym prawie federalnym co najmniej głównych zasad dotyczących jasno i zwięźle określonych praw, podobnie jak dzieje się to w przypadku innych państw spoza UE, które zostały „rygorystycznie ocenione" pod względem zapewnienia odpowiedniego poziomu ochrony; Trybunał Sprawiedliwości Unii Europejskiej w wyroku w sprawie Schrems określił je jako „merytorycznie równoważne" względem norm obowiązujących w prawie Unii, co według Grupy Roboczej Art. 29 oznacza zawierające „treść podstawowych zasad" ochrony danych.

Z zadowoleniem przyjmujemy zwiększoną przejrzystość po stronie organów amerykańskich w kwestii stosowania wyjątków od zasad ochrony prywatności (*Privacy Shield*) na potrzeby egzekwowania prawa, bezpieczeństwa narodowego i interesu publicznego.

Niemniej jednak, podczas gdy decyzja w sprawie zasad bezpiecznego transferu danych osobowych z 2000 r. (*Safe Harbour*) formalnie uznawała dostęp ze względu na bezpieczeństwo narodowe za wyjątek, uwaga poświęcona w projekcie decyzji w sprawie ochrony danych (*Privacy Shield*) dostępowi, filtrowaniu i analizowaniu przez organy ścigania i wywiadu danych osobowych przekazywanych w celach handlowych wskazuje na to, że wyjątek mógł stać się regułą. W szczególności EIOD zauważa na podstawie projektu decyzji i załączników do niej, że niezależnie od ostatnich tendencji przechodzenia z bezkrytycznego nadzoru na szeroką skalę w kierunku bardziej ukierunkowanych i wybiórczych metod, skala rozpoznania elektronicznego oraz ilość danych przekazywanych z UE, których dotyczyć może potencjalne gromadzenie i wykorzystywanie po przekazaniu oraz szczególnie podczas przekazywania, nadal może być duża, a zatem może być kwestionowana.

Chociaż praktyki te mogą odnosić się również do wywiadu w innych państwach i chociaż z zadowoleniem przyjmujemy przejrzystość organów amerykańskich w związku z taką nową rzeczywistością, obecny projekt decyzji może legitymizować tego rodzaju rutynowe działania. Z tego względu zachęcamy Komisję Europejską, aby dała wyraźniejszy sygnał: ze względu na zobowiązania nałożone na Unię przez traktat lizboński dostęp do danych i korzystanie

przez organy publiczne z danych przekazywanych w celach handlowych, w tym podczas przekazywania, powinny mieć miejsce jedynie w wyjątkowych okolicznościach oraz gdy jest to niezbędne w określonych celach wiążących się z interesem publicznym.

W kwestii przepisów dotyczących przekazywania danych w celach handlowych od administratorów nie należy oczekiwać ciągłej zmiany modelów zgodności. Tymczasem projekt decyzji opiera się na istniejących ramach prawnych UE, które zostaną zastąpione rozporządzeniem (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) w maju 2018 r., mniej niż rok po wdrożeniu ochrony prywatności (*Privacy Shield*) przez administratorów. Ogólne rozporządzenie o ochronie danych tworzy i wzmacnia obowiązki administratorów wykraczające poza dziewięć zasad opracowanych w ochronie prywatności (*Privacy Shield*). Niezależnie od ostatecznych zmian projektu zalecamy Komisji Europejskiej, aby kompleksowo oceniła przyszłe perspektywy już od pierwszego sprawozdania, aby na czas określić odpowiednie kroki na potrzeby rozwiązań długoterminowych służących zastąpieniu ochrony prywatności (*Privacy Shield*), jeżeli takie istnieją, solidniejszymi i stabilniejszymi ramami prawnymi na potrzeby poprawy relacji transatlantyckich.

Europejski Inspektor Ochrony Danych wydaje zatem konkretne zalecenia dotyczące ochrony prywatności (*Privacy Shield*).

I. **Wstęp**

W dniu 6 października 2015 r. Trybunał Sprawiedliwości Unii Europejskiej (zwany dalej „TSUE") unieważnił ([1]) decyzję w sprawie adekwatności programu ochrony danych *Safe Harbour* ([2]). W dniu 2 lutego 2016 r. Komisja Europejska osiągnęła polityczne porozumienie ze Stanami Zjednoczonymi w sprawie nowych ram przekazywania danych osobowych znanych jako „Unijno-amerykańska ochrona prywatności" (*Privacy Shield*; zwana dalej „ochroną prywatności"). W dniu 29 lutego Komisja Europejska upubliczniła projekt decyzji w sprawie odpowiedniej ochrony danych osobowych w ww. nowych ramach (dalej: projekt decyzji) ([3]) oraz siedem załączników do niej, w tym zasady ochrony prywatności i pisemne oświadczenia oraz zobowiązania urzędników i organów amerykańskich. Europejski Inspektor Ochrony Danych otrzymał projekt decyzji do konsultacji w dniu 18 marca br.

Europejski Inspektor Ochrony Danych wielokrotnie wyrażał swoje stanowisko w sprawie przekazywania danych osobowych między UE a Stanami Zjednoczonymi ([4]) i uczestniczył w tworzeniu opinii Grupy Roboczej Art. 29 (zwanej dalej Grupą Roboczą Art. 29) w sprawie projektu decyzji jako członek tej grupy ([5]). Grupa Robocza Art. 29 wyraziła poważne zaniepokojenie i zwróciła się do Komisji Europejskiej o zidentyfikowanie rozwiązań umożliwiających odpowiedź na te obawy. Członkowie Grupy Roboczej Art. 29 oczekują, że przedstawione zostaną wszystkie wyjaśnienia wymagane w opinii ([6]). W dniu 16 marca 27 organizacji non-profit wyraziło swoją krytykę wobec projektu decyzji w piśmie skierowanym do władz UE i Stanów Zjednoczonych ([7]). W dniu 26 maja Parlament Europejski przyjął rezolucję w sprawie transatlantyckich przepływów danych ([8]), w której wzywa Komisję do dalszego negocjowania lepszych ustaleń w zakresie ochrony prywatności z administracją Stanów Zjednoczonych w świetle obecnych niedociągnięć ([9]).

Jako niezależny doradca prawodawców UE na mocy rozporządzenia (WE) nr 45/2001 EIOD wydaje obecnie zalecenia stronom zaangażowanym w ten proces, w szczególności Komisji. Porada ta ma być zarówno oparta na zasadach, jak i pragmatyczna, tak by stanowiła proaktywne wsparcie dla UE w osiąganiu celów odpowiednimi środkami. Uzupełnia ona i podkreśla niektóre, lecz nie wszystkie, zalecenia zawarte w opinii Grupy Roboczej Art. 29.

([1]) Sprawa C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner, 6 października 2015 r. (zwana dalej „*Schrems*").

([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 (notyfikowana jako dokument nr C(2000) 2441) (Dz.U. L 215 z 25.8.2000, s. 7).

([3]) Decyzja wykonawcza Komisji XXX na podstawie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony zapewnianej przez unijno-amerykańską ochronę prywatności, dostępna na stronie internetowej pod adresem: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

([4]) Zob. opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady „Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi" oraz w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE, 20 lutego 2014 r. oraz pisma procesowego EIOD z rozprawy przed Trybunałem Sprawiedliwości UE w sprawie *Schrems*, dostępnego na stronie internetowej pod adresem: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf).

([5]) Grupa Robocza Art. 29 – opinia 01/2016 dotycząca decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach unijno-amerykańskiej ochrony prywatności (WP 238), dostępna na stronie internetowej pod adresem: http://ec.europa.eu/jus.tice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

([6]) Zob. również wystąpienie brytyjskiego komisarza ds. informacji Christophera Grahama podczas konferencji IAPP Europe Data Protection Intensive 2016 w Londynie. Wystąpienie dostępne jest na stronie internetowej pod adresem: https://iapp.org/news/video/iapp-europe-data-protection-intensive-2016-christopher-graham-keynote/.

([7]) Pismo do Grupy Roboczej Art. 29 i innych instytucji, podpisane przez Access Now i 26 innych organizacji pozarządowych.

([8]) Rezolucja Parlamentu Europejskiego z dnia 26 maja 2016 r. w sprawie transatlantyckich przepływów danych (2016/2727(RSP)).

([9]) *Idem*, pkt 14.

Projekt decyzji zawiera szereg ulepszeń w stosunku do decyzji w sprawie zasad ochrony danych (*Safe Harbour*), w szczególności w odniesieniu do zasad przetwarzania danych w celach handlowych. Jeżeli chodzi o dostęp organów publicznych do danych przekazywanych w ramach ochrony prywatności, z zadowoleniem przyjmujemy również zaangażowanie się po raz pierwszy w negocjacje przez Departament Sprawiedliwości, Departament Stanu i Urząd Dyrektora Krajowych Służb Wywiadowczych. Niemniej jednak postęp względem wcześniejszej decyzji w sprawie zasad ochrony danych (*Safe Harbour*) nie jest jeszcze wystarczający. Prawidłowym punktem odniesienia nie jest uprzednio unieważniona decyzja, ponieważ decyzja w sprawie odpowiedniej ochrony ma opierać się na obecnych ramach prawnych UE (w szczególności na samej dyrektywie, art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, jak również art. 7 i 8 Karty praw podstawowych UE zgodnie z wykładnią TSUE). Artykuł 45 ogólnego rozporządzenia UE o ochronie danych (zwanego dalej „ogólnym rozporządzeniem o ochronie danych) ([1]) będzie zawierać nowe wymogi dotyczące przekazywania danych w oparciu o decyzję w sprawie odpowiedniej ochrony danych osobowych.

W ubiegłym roku TSUE potwierdził, że progiem oceny odpowiedniości jest „merytoryczna równoważność" i domagał się rygorystycznej oceny względem tej wysokiej normy ([2]). Odpowiedniość nie wymaga przyjmowania ram identycznych jak istniejące w UE, ale w ogólnym rozrachunku ochrona prywatności i amerykański porządek prawny powinny obejmować wszystkie kluczowe elementy ram ochrony danych UE. Wymaga to zarówno ogólnej oceny porządku prawnego, jak i zbadania najważniejszych elementów ram ochrony danych UE ([3]). Zakładamy, że oceny należy dokonywać w ujęciu globalnym, jednak z poszanowaniem istoty tych elementów. Ponadto ze względu na traktat i Kartę praw podstawowych UE należy uwzględniać konkretne elementy, takie jak niezależny nadzór i dochodzenie odszkodowania na drodze sądowej.

Pod tym względem EIOD ma świadomość, że wiele organizacji po obydwu stronach Atlantyku czeka na rezultat decyzji w sprawie odpowiedniej ochrony danych osobowych. Niemniej jednak konsekwencje nowego unieważnienia przez TSUE mogą być duże pod względem niepewności prawnej z perspektywy podmiotów danych oraz obciążenia, w szczególności dla MŚP. Ponadto, jeżeli projekt decyzji zostanie przyjęty, a następnie unieważniony przez TSUE, wszelkie nowe ustalenia w sprawie odpowiedniej ochrony danych musiałyby być negocjowane na podstawie ogólnego rozporządzenia o ochronie danych. Z tego względu zalecamy podejście ukierunkowane na przyszłość z myślą o zbliżającej się dacie pełnego zastosowania ogólnego rozporządzenia o ochronie danych w terminie dwóch lat od chwili obecnej.

Projekt decyzji jest kluczowy dla relacji Unii i Stanów Zjednoczonych w chwili, gdy toczą się między nimi również negocjacje handlowe i inwestycyjne. Ponadto wiele elementów ujętych w naszej opinii dotyczy pośrednio zarówno ochrony prywatności, jak i i innych narzędzi przekazywania danych, takich jak wiążące reguły korporacyjne (zwane dalej „wiążącymi regułami korporacyjnymi") oraz standardowe klauzule umowne (zwane dalej „standardowymi klauzulami umownymi"). Ma to również znaczenie globalne, ponieważ wiele państw trzecich będzie postępować w ścisłej zgodności w kontekście przyjęcia nowych unijnych ram ochrony danych.

Z tego względu z zadowoleniem przyjęlibyśmy ogólne rozwiązanie dotyczące przekazywania danych między Unią Europejską a Stanami Zjednoczonymi, pod warunkiem że będzie ono kompleksowe i dostatecznie stabilne. Wymaga to solidnych ulepszeń w celu zapewnienia zrównoważonego długotrwałego poszanowania naszych podstawowych praw i swobód. W przypadku przyjęcia decyzji po pierwszej ocenie Komisji Europejskiej musi być ona terminowo poddana przeglądowi, aby można było określić odpowiednie kroki rozwiązań długoterminowych i zastąpić ochronę prywatności solidniejszymi i stabilniejszymi ramami prawnymi w celu poprawy relacji transatlantyckich.

Europejski Inspektor Ochrony Danych zauważa również na podstawie projektu decyzji i załączników do niej, że niezależnie od ostatnich tendencji przechodzenia z bezkrytycznego nadzoru na szeroką skalę w kierunku bardziej ukierunkowanych i wybiórczych metod, skala rozpoznania elektronicznego oraz ilość danych przekazywanych z UE, których dotyczyć może potencjalne gromadzenie po przekazaniu oraz szczególnie podczas przekazywania, nadal może być duża, a zatem może być kwestionowana.

Chociaż praktyki te mogą odnosić się również do wywiadu w innych państwach i chociaż z zadowoleniem przyjmujemy przejrzystość organów amerykańskich w związku z taką nową rzeczywistością, obecny projekt decyzji może być interpretowany jako legitymizacja tego rodzaju rutynowych działań. Kwestia wymaga poważnej publicznej demokratycznej analizy. Z tego względu zachęcamy Komisję Europejską, aby dała wyraźniejszy sygnał: ze względu na zobowiązania nałożone na Unię przez traktat lizboński dostęp do danych i korzystanie przez organy publiczne z danych przekazywanych w celach handlowych, w tym podczas przekazywania, powinny mieć miejsce jedynie w wyjątkowych okolicznościach oraz gdy jest to niezbędne w określonych celach wiążących się z interesem publicznym.

Ponadto zauważamy, że zasadnicze oświadczenia istotne dla życia prywatnego jednostek w UE sprawiają wrażenie omówionych w szczegółach jedynie w pismach wewnętrznych do organów amerykańskich (przykładowo oświadczenia dotyczące

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([2]) *Schrems*, pkt 71, 73, 74 i 96.

([3]) Podejście to zostało już uwzględnione w jednym z pierwszych pism Grupy Roboczej Art. 29 w sprawie przekazywania danych (WP12: „Dokument roboczy w sprawie przekazywania danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE w sprawie ochrony danych", 24 lipca 1998 r.).

rozpoznania elektronicznego przez łącza transatlantyckie, jeżeli dotyczy) ([1]). Chociaż nie kwestionujemy autorytetu autorów i rozumiemy, że po publikacji w Dzienniku Urzędowym i Rejestrze Federalnym oświadczenia te będą traktowane jako „pisemne zapewnienia" na podstawie, których odbywa się unijna ocena, ogólnie rzecz ujmując, zauważamy, że powaga niektórych z nich zasługiwałaby na większą wartość prawną.

Można analizować również dodatkowe rozwiązania praktyczne poza zmianami prawodawczymi i umowami międzynarodowymi ([2]). Nasza opinia ma na celu zapewnienie w tym względzie pragmatycznej porady.

IV. **Wnioski**

Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje działania podejmowane przez strony na rzecz znalezienia rozwiązania na potrzeby przekazywania danych osobowych z UE do Stanów Zjednoczonych w celach handlowych w ramach systemu autocertyfikacji. Niemniej jednak do osiągnięcia solidnych i stabilnych w perspektywie długoterminowej ram konieczne są gruntowne ulepszenia.

Sporządzono w Brukseli dnia 30 maja 2016 r.

Giovanni BUTTARELLI

Europejski Inspektor Ochrony Danych

([1]) Zob. przykładowo wyjaśnienia w załączniku VI pkt 1 lit. a), które rozporządzenie prezydenckie PPD-28 odnosiłoby do danych gromadzonych z łączy transatlantyckich przez amerykańską społeczność wywiadowczą.

([2]) Podczas rozprawy przed Trybunałem Sprawiedliwości Unii Europejskiej w sprawie *Schrems* EIOD stwierdził, że „[j]edynym skutecznym rozwiązaniem jest negocjowanie międzynarodowej umowy zapewniającej odpowiednią ochronę przeciwko bezkrytycznemu nadzorowi, w tym zobowiązania do kontroli, przejrzystość i prawa do dochodzenia odszkodowania na drodze sądowej oraz do ochrony danych"; pismo procesowe EIOD z rozprawy przed Trybunałem z dnia 24 marca 2015 r. w sprawie C-362/14 (Schrems przeciwko Data Protection Commissioner).