Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Rady w sprawie podpisania 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/C 35/03)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 8,

uwzględniając dyrektywę 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 ([1]),

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, w szczególności jego art. 41 ([2]),

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1. WPROWADZENIE

1.1. Konsultacje z EIOD oraz cel opinii

1. Dnia 28 listopada 2011 r. Komisja przyjęła wniosek dotyczący decyzji Rady w sprawie podpisania umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych ([3]) (zwanej dalej „umową").

2. Dnia 9 listopada 2011 r. odbyły się w ramach procedury przyspieszonej nieformalne konsultacje z EIOD dotyczące projektu wniosku. Dnia 11 listopada 2011 r. EIOD zgłosił pewne uwagi, których nie udostępniono publicznie. Celem obecnej opinii jest uzupełnienie tych uwag w świetle obecnego wniosku oraz publiczne udostępnienie poglądów EIOD. Opinia stanowi też rozwinięcie pewnych wcześniejszych interwencji EIOD i Grupy Roboczej Art. 29 w odniesieniu do danych dotyczących przelotu pasażera (danych PNR).

1.2. Kontekst wniosku

3. Celem umowy jest zapewnienie mocnej podstawy prawnej dla przekazywania danych dotyczących przelotu pasażera (danych PNR) z UE do USA. Przekazywanie to opiera się obecnie na umowie z 2007 r. ([4]), gdyż Parlament zdecydował się odłożyć głosowanie nad zgodą do czasu spełnienia jego postulatów związanych z ochroną danych. W szczególności w rezolucji z dnia 5 maja 2010 r. ([5]) Parlament wskazał następujące wymagania:

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) COM(2011) 807 wersja ostateczna.
([4]) Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Dz.U. L 204 z 4.8.2007, s. 18).
([5]) Rezolucja Parlamentu Europejskiego z dnia 5 maja 2010 r. dotycząca rozpoczęcia negocjacji w sprawie umów dotyczących rejestru nazwisk pasażerów (PNR) ze Stanami Zjednoczonymi, Australią i Kanadą (Dz.U. C 81E z 15.3.2011, s. 70). Zob. też rezolucje Parlamentu Europejskiego z dnia 13 marca 2003 r. w sprawie przekazywania danych osobowych przez linie lotnicze w przypadku lotów transatlantyckich (Dz.U. C 61E z 10.3.2004, s. 381), z dnia 9 października 2003 r. w sprawie przekazywania danych przez linie lotnicze w przypadku lotów transatlantyckich (Dz.U. C 81E z 31.3.2004, s. 105), z dnia 31 marca 2004 r. w sprawie projektu decyzji Komisji określającej odpowiedni poziom ochrony danych osobowych zawartych w rejestrze nazwisk pasażerów (PNR) przekazywanych do Amerykańskiego Biura Ceł i Ochrony Granic (Dz.U. C 103E z 29.4.2004, s. 665), zalecenie dla Rady z dnia 7 września 2006 r. w sprawie negocjacji porozumienia ze Stanami Zjednoczonymi Ameryki w sprawie wykorzystywania danych dotyczących nazwisk pasażerów (PNR) w celu zapobiegania aktom terroryzmu i przestępczości transgranicznej, w tym przestępczości zorganizowanej (Dz.U. C 305E z 14.12.2006, s. 250), rezolucję z dnia 14 lutego 2007 r. w sprawie SWIFT, porozumienia dotyczącego PNR oraz dialogu transatlantyckiego w tych kwestiach (Dz.U. C 287E z 29.11.2007, s. 349) oraz rezolucję z dnia 12 lipca 2007 r. w sprawie porozumienia ze Stanami Zjednoczonymi w sprawie udostępniania danych osobowych pasażerów (PNR) (teksty przyjęte, P6_TA(2007)0347). Wszystkie dokumenty są dostępne na stronie: http://www.europarl.europa.eu

— zgodność z przepisami dotyczącymi ochrony danych na szczeblu krajowym i europejskim,

— ocenę wpływu na prywatność przed przyjęciem jakiegokolwiek instrumentu legislacyjnego,

— test proporcjonalności dowodzący, że istniejące instrumenty prawne są niewystarczające,

— ścisłe ograniczenie celów ([6]) oraz ograniczenie wykorzystania danych PNR do konkretnych przestępstw lub zagrożeń w oparciu o ocenę poszczególnych przypadków,

— ograniczenie ilości gromadzonych danych,

— ograniczenie okresu zatrzymywania danych,

— zakaz eksploracji danych lub tworzenia profili,

— zakaz podejmowania automatycznych decyzji mających istotny wpływ na obywateli ([7]),

— odpowiednie mechanizmy niezależnego przeglądu i nadzoru sądowego oraz kontroli demokratycznej,

— wszelkie międzynarodowe przekazywanie danych powinno być zgodne z normami UE w zakresie ochrony danych i podlegać ustaleniu adekwatności.

4. Obecną umowę należy rozważać w kontekście ogólnoświatowego podejścia do danych PNR – trwają negocjacje z innymi państwami trzecimi (mianowicie z Australią ([8]) i Kanadą ([9])), pojawił się też wniosek dotyczący systemu PNR na szczeblu UE ([10]). Jest ona także elementem trwających negocjacji dotyczących umowy między UE a USA o wymianie danych osobowych w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych ([11]). W szerszym kontekście umowę tę parafowano kilka tygodni przed oczekiwanym przyjęciem wniosków dotyczących przeglądu ogólnych ram ochrony danych ([12]).

5. EIOD z zadowoleniem przyjmuje to globalne podejście, którego celem jest zapewnienie umowom PNR spójnych ram prawnych zgodnych z wymaganiami prawnymi UE. Z ubolewaniem stwierdza jednak, że przyjęty harmonogram nie pozwala w praktyce zapewnić spójności tych umów z nowymi zasadami UE w sprawie ochrony danych. Pragnie również przypomnieć, że do umowy między UE a USA w sprawie danych PNR zastosowanie powinna mieć ogólna umowa między UE a USA o wymianie danych.

([6]) Ograniczenie do celów związanych z egzekwowaniem prawa i bezpieczeństwem w przypadkach zorganizowanej poważnej przestępczości międzynarodowej lub terroryzmu transgranicznego na podstawie definicji prawnych podanych w decyzji ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3) oraz w decyzji ramowej Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania (Dz.U. L 190 z 18.7.2002, s. 1).

([7]) „Decyzja o zakazie wstępu na pokład lub decyzja o wszczęciu dochodzenia lub wniesieniu oskarżenia nie może być podjęta wyłącznie w oparciu o wyniki takiego zautomatyzowanego przeszukiwania baz danych".

([8]) Umowa między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR), podpisana dnia 29 września 2011 r.

([9]) Umowa między Wspólnotą Europejską a Rządem Kanady o przetwarzaniu zaawansowanych informacji o pasażerach oraz zapisu danych dotyczących nazwiska pasażera (Dz.U. L 82 z 21.3.2006, s. 15).

([10]) Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania (COM(2011) 32 wersja ostateczna).

([11]) W dniu 3 grudnia 2010 r. Rada wydała upoważnienie do otwarcia negocjacji dotyczących umowy między UE a USA o ochronie danych osobowych przekazywanych lub przetwarzanych w celu zapobiegania przestępstwom, w tym terroryzmowi, ich wykrywania i ścigania oraz prowadzenia postępowań sądowych w takich sprawach w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Zob. komunikat prasowy Komisji pod adresem: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1661

([12]) Zob. komunikat Komisji w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej z dnia 4 listopada 2010 r., COM(2010) 609 wersja ostateczna, i działania następcze z nim związane.

2. UWAGI OGÓLNE

6. Zgodnie z Kartą praw podstawowych UE wszelkie ograniczenia dotyczące praw i wolności podstawowych muszą być konieczne, proporcjonalne oraz przewidziane ustawą. Jak wielokrotnie wskazywał EIOD ([13]) i Grupa Robocza Art. 29 ([14]), jak dotąd nie wykazano konieczności i proporcjonalności systemów PNR oraz masowego przekazywania danych PNR państwom trzecim. Opinię tę podzielają też Europejski Komitet Ekonomiczno-Społeczny i Agencja Praw Podstawowych Unii Europejskiej ([15]). Konkretne uwagi zamieszczone poniżej pozostają bez uszczerbku dla tego wstępnego i podstawowego spostrzeżenia.

7. Chociaż omawiana umowa zawiera pewne udoskonalenia w porównaniu z umową z 2007 r. i uwzględniono w niej wystarczające zabezpieczenia związane z bezpieczeństwem danych i nadzorem, wydaje się, że nie zażegnano żadnej z głównych obaw wyrażonych w powyższych opiniach ani też nie spełniono żadnego z warunków wyrażenia zgody przez Parlament Europejski ([16]).

3. KONKRETNE UWAGI

3.1. Konieczność wyjaśnienia celu

8. W art. 4 ust. 1 umowy stwierdza się, że Stany Zjednoczone przetwarzają dane PNR dla celów zapobiegania a) przestępstwom terrorystycznym oraz przestępstwom powiązanym i b) przestępstwom podlegającym karze pozbawienia wolności na czas nie krótszy niż trzy lata i mającym charakter międzynarodowy oraz dla celów ich wykrywania, ścigania i prowadzenia odnośnych dochodzeń. Niektóre z tych pojęć są dodatkowo zdefiniowane.

9. Chociaż definicje te są bardziej precyzyjne niż w umowie z 2007 r., nadal występują pewne niejasne koncepcje i wyjątki, które mogłyby skutkować pominięciem zasady celowości oraz podważeniem pewności prawa. W szczególności:

— w art. 4 ust. 1 lit. a) ppkt (i) sformułowanie: „działania, które […] wydaje się, że zostały podjęte w celu zastraszenia […] lub wymuszenia […] określonych działań" lub „wywarcia wpływu na politykę rządu" może odnosić się również do działań, których nie można uznać za przestępstwa terrorystyczne zgodnie z decyzją ramową Rady 2002/475/WSiSW ([17]). Aby wykluczyć taką możliwość, należy wyjaśnić znaczenia pojęć „wydaje się", „zastraszenie" i „wywarcie wpływu",

— w art. 4 ust. 1 lit. b) należy zawrzeć konkretny wykaz przestępstw. Odniesienie do „innych przestępstw podlegających karze pozbawienia wolności na czas nie krótszy od lat trzech" nie jest wystarczające, gdyż próg ten obejmuje odmienne przestępstwa w UE i USA, jak też w poszczególnych państwach członkowskich UE i stanach USA,

([13]) Opinia EIOD z dnia 25 marca 2011 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania; opinia EIOD z dnia 15 lipca 2011 r. w sprawie wniosku dotyczącego decyzji Rady w sprawie zawarcia umowy między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR); opinia EIOD z dnia 19 października 2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (danych PNR) państwom trzecim oraz opinia EIOD z dnia 20 grudnia 2007 r. w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących przelotu pasażera do celów egzekwowania prawa. Wszystkie dokumenty są dostępne na stronie: http://www.edps.europa.eu

([14]) Opinia 10/2011 Grupy Roboczej Art. 29 w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania; opinia 7/2010 w sprawie komunikatu Komisji Europejskiej w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim; opinia 5/2007 w sprawie umowy następczej w stosunku do umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, zawartej w lipcu 2007 r. oraz opinia 4/2003 w sprawie poziomu ochrony zapewnianej przez Stany Zjednoczone przy przekazywaniu danych pasażerów. Wszystkie dokumenty są dostępne pod adresem: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

([15]) Opinia Agencji Praw Podstawowych Unii Europejskiej z dnia 14 czerwca 2011 r. w sprawie wniosku dotyczącego dyrektywy w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania (dostępna pod adresem: http://fra.europa.eu/fraWebsite/attachments/FRA-PNR-Opinion-June2011.pdf) oraz opinia EKES z dnia 5 maja 2011 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania (dostępna pod adresem: http://www.eesc.europa.eu/?i=portal.en.soc-opinions15579).

([16]) Porównaj przypis 5.

([17]) Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

— z zakresu umowy należy wyraźnie wyłączyć drobne wykroczenia,

— w art. 4 ust. 2 należy zdefiniować pojęcie „poważnego zagrożenia", a wykorzystywanie danych PNR „o ile nakaże tak sąd" powinno ograniczać się do przypadków, o których mowa jest w art. 4 ust. 1,

— podobnie w celu uniknięcia zastosowania art. 4 ust. 3 do celów takich, jak kontrola graniczna, należy wyszczególnić, że tylko osoby podejrzane o udział w jakimkolwiek z przestępstw wymienionych w art. 4 ust. 1 mogą zostać „poddane dokładniejszemu przesłuchaniu lub badaniu".

3.2. **Wykaz przekazywanych danych PNR należy zawęzić**

10. W załączniku I do umowy zapisano 19 rodzajów danych, które będą przesyłane do USA. W większości obejmują one różne kategorie danych i są identyczne z polami danych w umowie z 2007 r., które EIOD oraz Grupa Robocza Art. 29 uznali już za nieproporcjonalne ([18]).

11. Odnosi się to w szczególności do pola „Uwagi ogólne, w tym OSI ([19]), SSI ([20]) i SSR ([21])", w którym mogą zostać ujawnione dane odnoszące się do wierzeń religijnych (np. preferencje dotyczące posiłków) lub stanu zdrowia (np. prośba o wózek inwalidzki). Takie dane szczególnie chronione należy wyraźnie wyłączyć z wykazu.

12. Przy ocenie proporcjonalności wykazu należy też wziąć pod uwagę, że w związku z uprzednim przekazywaniem danych (art. 15 ust. 3 umowy) kategorie te będą odnosić się nie tylko do rzeczywistych pasażerów, ale również do osób, które ostatecznie nie odbędą lotu (np. w związku z anulowaniem).

13. Ponadto obecność otwartych pól danych może podważyć pewność prawa. Należy precyzyjniej zdefiniować kategorie, takie jak „Wszystkie dostępne informacje kontaktowe", „Wszystkie informacje o bagażu" i „Uwagi ogólne".

14. W związku z tym wykaz należy zawęzić. Zgodnie z opinią Grupy Roboczej Art. 29 ([22]) uważamy, że dane należy ograniczyć do następujących informacji: numeru rejestracji PNR, daty rezerwacji, daty/dat planowanej podróży, nazwiska pasażera, innych nazwisk zawartych w PNR, trasy całej podróży, identyfikatorów bezpłatnych biletów, biletów w jedną stronę, informacji podanych na bilecie, danych ATFQ (Automatic Ticket Fare Quote), numeru biletu, daty wystawienia biletu, informacji o lotach, na które pasażer nie stawił się w przeszłości, liczby sztuk bagażu, numerów przywieszek bagażowych, informacji o pasażerach, którzy nie dokonali uprzedniej rezerwacji, liczby sztuk bagażu na każdy segment lotu, zamawianych/niezamawianych zamian klasy na wyższą, zmian historycznych danych PNR w odniesieniu do powyższych pozycji.

3.3. **Departament Bezpieczeństwa Wewnętrznego nie powinien przetwarzać danych szczególnie chronionych**

15. W art. 6 umowy stwierdza się, że Departament Bezpieczeństwa Wewnętrznego (DHS) będzie automatycznie filtrować i maskować dane szczególnie chronione. Dane szczególnie chronione będą jednak przechowywane przez co najmniej 30 dni i mogą zostać wykorzystane w konkretnych przypadkach (art. 6 ust. 4). EIOD pragnie podkreślić, że nawet po zamaskowaniu dane te pozostaną wrażliwe i będą się odnosić do możliwych do zidentyfikowania osób fizycznych.

16. Jak EIOD wskazał już wcześniej, DHS nie powinien przetwarzać danych szczególnie chronionych odnoszących się do obywateli UE, nawet jeżeli zostają one zamaskowane przy odbiorze. EIOD zaleca zawarcie w treści umowy postanowienia stwierdzającego, że przewoźnicy nie powinni przekazywać DHS danych szczególnie chronionych.

([18]) Zob. przywoływane wyżej opinie EIOD i Grupy Roboczej Art. 29.
([19]) Informacje o innych usługach.
([20]) Informacje o usługach specjalnych.
([21]) Prośby o usługi specjalne.
([22]) Zob. przywoływaną wyżej opinię 4/2003 Grupy Roboczej Art. 29.

3.4. **Okres zatrzymywania danych jest zbyt długi**

17. W art. 8 stwierdza się, że dane PNR będą zatrzymywane w aktywnej bazie danych przez okres maksymalnie pięciu lat, po czym zostaną przeniesione do archiwalnej bazy danych na okres do dziesięciu lat. Ten maksymalny okres zatrzymywania wynoszący 15 lat jest w oczywisty sposób nieproporcjonalny niezależnie od tego, czy dane są przechowywane w „aktywnej" czy „archiwalnej" bazie danych, co podkreślił już zarówno EIOD, jak i Grupa Robocza Art. 29.

18. W art. 8 ust. 1 stwierdza się, że po upływie sześciu miesięcy od chwili otrzymania przez DHS dane pozbawiane są cech umożliwiających identyfikację osoby oraz maskowane. Jednak zarówno dane „zamaskowane", jak i dane przechowywane w „archiwalnej bazie danych" są danymi osobowymi do chwili ich zanonimizowania. Dane należy zatem zanonimizować (w nieodwracalny sposób) lub usunąć bezpośrednio po analizie lub po co najwyżej 6 miesiącach.

3.5. **Wykorzystywanie metody „push" i częstotliwość przekazywania**

19. EIOD z zadowoleniem przyjmuje art. 15 ust. 1, w którym stwierdza się, że dane będą przekazywane za pomocą metody „dostarczania" (metody „push"). W art. 15 ust. 5 wymaga się jednak od przewoźników „zapewnienia dostępu" do danych PNR w wyjątkowych okolicznościach. W celu definitywnego wykluczenia wykorzystania systemu pobierania danych („pull") oraz w obliczu uwag podkreślonych ponownie ostatnio przez Grupę Roboczą Art. 29 ([23]) zdecydowanie zalecamy, aby w umowie wyraźnie zakazano umożliwiania urzędnikom amerykańskim uzyskiwania osobnego dostępu do danych za pośrednictwem systemu „pull".

20. W umowie należy określić liczbę i częstotliwość transferów danych od przewoźników do DHS. Aby zwiększyć pewność prawną, należy także bardziej szczegółowo określić warunki, w jakich dopuszczalne będą dodatkowe transfery.

3.6. **Bezpieczeństwo danych**

21. EIOD z zadowoleniem przyjmuje art. 5 umowy dotyczący bezpieczeństwa i integralności danych, a w szczególności obowiązek informowania o naruszeniach prywatności osób, których naruszenia te dotyczą. Należy jednak wyjaśnić następujące elementy informowania o przypadkach naruszenia poufności danych:

— odbiorcy informacji: należy określić, które „odpowiednie organy europejskie" powinny zostać poinformowane. W każdym razie wśród nich powinny się znaleźć krajowe organy ochrony danych. Należy też poinformować właściwy organ amerykański,

— próg informowania wspomnianych organów: należy zdefiniować, co stanowi „przypadek naruszenia poufności danych",

— należy określić treść informacji przekazywanych osobom fizycznym i organom.

22. EIOD popiera obowiązek rejestrowania lub dokumentowania każdorazowego dostępu do danych PNR i ich przetwarzania, gdyż umożliwi to weryfikację, czy DHS wykorzystuje dane PNR we właściwy sposób i czy doszło do nieupoważnionego dostępu do systemu.

3.7. **Nadzór i egzekwowanie prawa**

23. EIOD z zadowoleniem przyjmuje fakt, że zgodnie z art. 14 ust. 1 zgodność działania z zabezpieczeniami przewidzianymi w umowie będzie przedmiotem niezależnego przeglądu i nadzoru ze strony departamentalnych urzędników ds. prywatności, jak np. głównego urzędnika ds. prywatności w DHS. W celu zapewnienia skutecznego korzystania przez osoby, których dane dotyczą,

([23]) Zob. list z dnia 19 stycznia 2011 r. od Grupy Roboczej Art. 29 do komisarz Malmström w sprawie umów PNR UE z USA, Kanadą i Australią.

z ich praw, EIOD i krajowe organy ochrony danych powinni wszakże współpracować z DHS nad opracowaniem procedur i trybu korzystania z tych praw ([24]). EIOD z zadowoleniem przyjąłby odniesienie do tej współpracy w umowie.

24. EIOD zdecydowanie popiera prawo do dochodzenia roszczeń „niezależnie od narodowości, kraju pochodzenia lub miejsca zamieszkania" wskazane w art. 14 ust. 1 akapit drugi. Z ubolewaniem stwierdza jednak, iż w art. 21 wskazano wyraźnie, że umowa „nie tworzy ani nie przyznaje, zgodnie z prawem Stanów Zjednoczonych, żadnych praw czy korzyści żadnym osobom". Nawet jeżeli na mocy umowy zostanie przyznane w USA prawo do „kontroli sądowej", może ono nie być równoważne prawu do skutecznego dostępu do wymiaru sprawiedliwości w UE, zwłaszcza w świetle ograniczenia zawartego w art. 21.

3.8. **Dalsze krajowe i międzynarodowe przekazywanie danych**

25. W art. 16 zabrania się przekazywania danych organom krajowym, które nie zapewniają w odniesieniu do danych PNR „takich samych lub równorzędnych" zabezpieczeń, jak określone w umowie. EIOD z zadowoleniem przyjmuje to postanowienie. Należy jednak doprecyzować wykaz organów, które mogą otrzymywać dane PNR. Jeżeli chodzi o przekazywanie międzynarodowe, w umowie stwierdza się, że może ono nastąpić wyłącznie wówczas, jeżeli cel, w jakim odbiorca zamierza wykorzystywać dane, jest zgodny z umową, a ochrona prywatności danych jest „porównywalna" do zapewnionej w umowie, z wyjątkiem nadzwyczajnych okoliczności.

26. W odniesieniu do użytych w umowie sformułowań „porównywalny" lub „równorzędny" EIOD pragnie podkreślić, że nie powinno dochodzić do krajowego lub dalszego międzynarodowego przekazywania danych przez DHS, chyba że odbiorca wskaże zabezpieczenia nie mniej rygorystyczne od tych, które ustanawia umowa. W umowie należy też wyjaśnić, że przekazywanie danych PNR będzie dokonywane na podstawie analizy poszczególnych przypadków, co zapewni przekazanie odpowiednim odbiorcom wyłącznie niezbędnych danych, przy czym nie należy dopuszczać wyjątków. Ponadto EIOD zaleca, aby przekazywanie danych państwom trzecim wymagało uprzedniego zezwolenia sądu.

27. W art. 17 ust. 4 stwierdza się, że jeśli DHS ma świadomość, iż dane rezydenta państwa członkowskiego UE są przekazywane państwu trzeciemu, powiadamia o tym właściwe organy danego państwa członkowskiego. Warunek ten należy skreślić, gdyż DHS powinien zawsze wiedzieć o dalszym przekazywaniu danych państwom trzecim.

3.9. **Forma i przegląd umowy**

28. Nie jest jasne, jaką formę prawną zawarcia omawianej umowy przyjmą Stany Zjednoczone i w jaki sposób stanie się ona prawnie wiążąca w tym kraju. Należy to wyjaśnić.

29. Artykuł 20 ust. 2 odnosi się do spójności z możliwym unijnym systemem PNR. EIOD zauważa, że konsultacje dotyczące dostosowania omawianej umowy mają w szczególności skupiać się na tym, czy „standardy w zakresie ochrony danych osobowych stosowane w przypadku przyszłego unijnego systemu PNR byłyby mniej rygorystyczne niż standardy ustanowione w niniejszej Umowie". W celu zapewnienia spójności przy wszelkim dostosowaniu należy również (i w szczególności) uwzględnić bardziej rygorystyczne zabezpieczenia w dowolnym przyszłym systemie PNR.

30. Przeglądu umowy należy też dokonać w obliczu nowych ram ochrony danych i możliwego zawarcia ogólnej umowy między UE a USA o wymianie danych osobowych w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Można dodać nowe postanowienie podobne do art. 20 ust. 2 stwierdzające: „w przypadku i w chwili przyjęcia w UE nowych ram prawnych ochrony danych lub zawarcia nowej umowy o wymianie danych między UE a USA, Strony skonsultują się

([24]) Grupa Robocza Art. 29 przedstawiła już na przykład wskazówki dotyczące dostarczania informacji pasażerom (zob. opinię 2/2007 Grupy Roboczej Art. 29 z dnia 15 lutego 2007 r. (poprawioną i zaktualizowaną w dniu 24 czerwca 2008 r.) w sprawie informacji dla pasażerów na temat przekazywania danych dotyczących przelotu pasażera (PNR) władzom Stanów Zjednoczonych, dostępną pod adresem: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp151_pl.pdf).

celem ustalenia, czy niniejsza Umowa wymaga dostosowania. Konsultacje te będą w szczególności dotyczyć tego, czy jakakolwiek przyszła modyfikacja ram prawnych ochrony danych w UE lub jakakolwiek przyszła umowa między UE a USA o ochronie danych narzuci bardziej rygorystyczne zabezpieczenia dotyczące ochrony danych niż przewidziane w niniejszej umowie".

31. Jeżeli chodzi o przegląd umowy (art. 23), zdaniem EIOD należy zamieścić wyraźny zapis, zgodnie z którym krajowe organy ochrony danych zostaną uwzględnione w zespole dokonującym przeglądu. Przegląd powinien również skupić się na ocenie konieczności i proporcjonalności środków oraz skutecznym korzystaniu z praw osób, których dane dotyczą, jak też uwzględniać weryfikację sposobu, w jaki w praktyce przetwarzane są wnioski osób, których dane dotyczą, zwłaszcza w przypadkach, gdzie nie jest możliwy dostęp bezpośredni. Należy określić częstotliwość przeglądów.

4. **WNIOSKI**

32. EIOD z zadowoleniem przyjmuje zabezpieczenia dotyczące bezpieczeństwa danych i nadzoru przewidziane w umowie oraz udoskonalenia w porównaniu z umową z 2007 r. Pozostaje jednak wiele powodów do niepokoju, zwłaszcza w odniesieniu do spójności globalnego podejścia do danych PNR, celowości, kategorii danych, które mają być przekazywane DHS, przetwarzania danych szczególnie chronionych, okresu zatrzymywania, wyjątków w odniesieniu do metody „push", praw osób, których dane dotyczą, i dalszego przekazywania danych.

33. Spostrzeżenia te pozostają bez uszczerbku dla wymogów dotyczących konieczności i proporcjonalności jakiegokolwiek zgodnego z prawem systemu PNR i umowy przewidującej masowe przekazywanie danych PNR z UE państwom trzecim. Jak potwierdził w swojej rezolucji z dnia 5 maja Parlament Europejski: „konieczność i proporcjonalność stanowią priorytety, bez których walka z terroryzmem nigdy nie będzie skuteczna".

Sporządzono w Brukseli dnia 9 grudnia 2011 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych