I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych 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)

(2011/C 322/01)

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 art. 41 rozporządzenia (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 ([2]),

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1. WPROWADZENIE

1.1. Konsultacje z EIOD

1. Dnia 19 maja 2011 r. Komisja przyjęła wniosek 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) ([3]). Wniosek został przesłany do EIOD dnia 23 maja.

2. Nieformalne konsultacje z EIOD odbyły się w maju 2011 r. w ramach procedury przyspieszonej i dotyczyły wniosku w sprawie umowy między Unią Europejską a Australią w sprawie przetwarzania i przekazywania danych PNR.

3. Uwzględniając fakt, że uwagi EIOD pozostają aktualne w odniesieniu do treści wniosku przyjętego przez Komisję i przedłożonego Radzie oraz Parlamentowi, EIOD podjął decyzję o udostępnieniu swoich uwag szerszemu gronu odbiorców w formie opinii publicznej. Uwagi Komisji będą dzięki temu uwzględnione w debatach na temat wniosku w przyszłości.

4. EIOD korzysta z tej okazji, aby podjąć inne tematy, oraz zachęca Radę i Parlament do uwzględniania przedstawionych opinii przy podejmowaniu decyzji w sprawie wniosku zgodnie z art. 218 TFUE.

1.2. Kontekst wniosku

5. Umowa między UE a Australią dotycząca danych PNR jest kolejnym krokiem podjętym w ramach agendy UE obejmującej globalne wytyczne dotyczące danych PNR, opracowanie systemu UE-PNR i negocjowanie umów z państwami trzecimi ([4]).

([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) 281 wersja ostateczna.
([4]) Zob. w szczególności komunikat Komisji z dnia 21 września 2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, COM(2010) 492 wersja ostateczna.

6. EIOD uważnie śledzi zmiany i postępy w zakresie danych PNR i wydał ostatnio dwie opinie na temat „pakietu PNR" Komisji oraz wniosek w sprawie dyrektywy o UE-PNR ([1]). Poglądy wyrażone przez EIOD na temat systemów PNR uzupełniają poglądy wyrażane przez Grupę Roboczą Art. 29 ([2]), a także inne niedawno przyjęte dokumenty, w tym opinię Komitetu Ekonomiczno-Społecznego ([3]) oraz opinię Agencji Praw Podstawowych UE ([4]), oraz są w dużej mierze z nimi zgodne.

7. Jak wykazano poniżej, konsekwentne podejście EIOD polegało zawsze na konfrontacji celów systemu PNR z fundamentalnymi wymogami w zakresie konieczności i proporcjonalności, a następnie na szczegółowym analizowaniu przepisów, co umożliwia proponowanie niezbędnych usprawnień.

1.3. **Uwagi wstępne**

8. EIOD z zadowoleniem przyjmuje ogólne podejście, którego celem jest harmonizacja mechanizmów ochrony danych w poszczególnych umowach dotyczących PNR zawieranych z krajami trzecimi. W dalszym ciągu pozostaje jednak kilka kwestii, które należy rozwiązać.

9. W opiniach EIOD i opiniach Grupy Roboczej Art. 29 wielokrotnie i konsekwentnie powtarzana jest uwaga, która ma również zastosowanie do wniosku w sprawie australijskich PNR: należy wykazać konieczność i proporcjonalność systemów PNR.

10. Te dwa podstawowe wymogi są zasadniczymi aspektami prawa ochrony danych, zgodnie z treścią art. 7 i 8 Karty praw podstawowych oraz art. 16 TFUE. UE musi zagwarantować, że spełniane są wymogi wynikające ze wspólnotowych przepisów prawa ochrony danych, również wtedy, gdy dane dotyczące obywateli UE są przetwarzane i przekazywane z terytorium UE do państwa trzeciego. W takich przypadkach przed podpisaniem jakiejkolwiek umowy należy ocenić i ustalić konieczność i proporcjonalność działań. Poza elementami dowodzącymi konieczności wprowadzenia systemu PNR, proporcjonalność wymaga zachowania odpowiedniej równowagi pomiędzy realizowanym celem a przetwarzaniem ogromnych ilości danych, czego rezultatem jest ingerencja w prywatne życie jednostek.

11. Jeśli chodzi o systemy PNR, ich celem jest zwalczanie terroryzmu i poważnej (międzynarodowej) przestępczości poprzez wykorzystanie ogromnej ilości danych dotyczących wszystkich pasażerów, co pozwala na przeprowadzenie oceny ryzyka w oparciu o te dane. Do tej pory EIOD nie odnalazł żadnych przekonujących argumentów w uzasadnieniach przedstawionych w odniesieniu zarówno do istniejących, jak i planowanych systemów PNR, takich jak system UE-PNR, który został przez niego szczegółowo przeanalizowany w opinii wydanej w marcu 2011 r. ([5]).

12. Ponadto EIOD podkreśla, że w razie zaistnienia konieczności wymóg proporcjonalności również musi zostać spełniony. Kwestionuje on równowagę pomiędzy przetwarzaniem danych osobowych na wielką skalę a celowością takiego działania, szczególnie w obliczu różnych przestępstw objętych zakresem stosowania projektu umowy. EIOD wskazuje, że istnieją inne skuteczne instrumenty walki z terroryzmem i poważną przestępczością.

13. Szczegółowe uwagi przedstawione poniżej pozostają bez uszczerbku dla tej wstępnej i podstawowej uwagi. EIOD z zadowoleniem przyjmuje przepisy, w których przewiduje się specjalne gwarancje, takie jak ochrona danych, egzekwowanie prawa i nadzór, a także odnoszące się do dalszego przekazywania danych. Jednocześnie, poza kwestiami konieczności i proporcjonalności, EIOD wyraża obawę co do zakresu definicji oraz warunków zatrzymywania danych.

2. **ANALIZA WNIOSKU**

2.1. **Podstawa prawna**

14. EIOD odnotowuje, że umowę sporządzono na podstawie art. 82 ust. 1 lit. d), art. 87 ust. 2 lit. a) i art. 218 ust. 6 lit. a) Traktatu o funkcjonowaniu Unii Europejskiej. Przypomina, że obiektywne czynniki, jakie należy uwzględnić

([1]) — 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 19 października 2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim.
Obie opinie dostępne na stronie: http://www.EIOD.europa.eu/EIODWEB/EIOD/cache/off/Consultation

([2]) Opinia Grupy Roboczej Art. 29 10/2011 z dnia 5 kwietnia 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: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

([3]) Opinia Europejskiego Komitetu Ekonomiczno-Społecznego 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, COM(2011) 32 wersja ostateczna.

([4]) Opinia Agencji Praw Podstawowych Unii Europejskiej z dnia 14 czerwca 2011 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania (COM(2011) 32 wersja ostateczna).

([5]) 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; zob. również opinia Grupy Roboczej Art. 29, o której mowa powyżej.

podczas wyboru podstawy prawnej, obejmują w szczególności cel i treść środka ([1]). W przypadku gdy analiza wspólnotowego aktu prawnego wykaże, że wyznaczono takiemu aktowi dwa cele lub ma on dwie części składowe, a jeden z tych aspektów można zidentyfikować jako główny lub przeważający, podczas gdy drugi jest jedynie pomocniczy, wówczas ten akt prawny należy wydać na pojedynczej podstawie prawnej, tj. na tej podstawie, która wymagana jest z racji głównego lub przeważającego celu lub części składowej ([2]). W wyjątkowych przypadkach natomiast, jeśli zostanie ustalone, że dany akt prawny realizuje większą ilość celów lub ma większą ilość części składowych, które są nierozerwalnie związane, przy czym żaden z aspektów nie jest drugorzędny lub pośredni w stosunku do drugiego, wówczas taki akt prawny należy wydać na odpowiadających im różnych podstawach prawnych ([3]).

15. W kontekście ustalonego orzecznictwa, które pokrótce przedstawiono powyżej, EIOD twierdzi, że poza art. 218 ust. 6 lit. a) umowa powinna opierać się nie na art. 82 ust. 1 lit. d) i art. 87 ust. 2 lit. a), ale na art. 16 TFUE.

16. Biorąc pod uwagę cel, należy przypomnieć, że umowy w sprawie danych PNR negocjowane przez UE wynikają z potrzeby pogodzenia obowiązku linii lotniczych związanego z koniecznością dostarczania danych PNR władzom państw trzecich z podstawowym prawem do ochrony danych osobowych ([4]). Co więcej, tekst wniosku odnosi się w wielu miejscach do celu ochrony danych osobowych ([5]).

17. W zakresie treści postanowienia dotyczące ochrony danych wyraźnie przeważają w umowie. Poza art. 3, 4 i 6 kwestia ochrony danych obejmuje niemal całość postanowień umowy. Wyraźnie widać to w art. 1 (cel), art. 2 (definicje), art. 5 (adekwatność) oraz art. 7–19 (gwarancje stosowane w procesie przetwarzania danych PNR).

18. Jeśli chodzi o postanowienia dotyczące gwarancji (art. 7–19), należy zauważyć, że ich treść jest typowa dla przepisów o ochronie danych ([6]). Fakt, iż akt prawny zawiera przepisy typowe dla konkretnej dziedziny prawa, został uznany przez Trybunał za element uzasadniający istnienie jednej szczegółowej podstawy prawnej ([7]).

19. Krótko mówiąc, EIOD uważa, że celem umowy nie jest usprawnienie współpracy policji, ale raczej przekazanie kompetencji i upoważnienie do przekazywania danych osobowych przez operatorów prywatnych w odpowiedzi na wniosek państwa trzeciego. O ile, zgodnie z treścią przepisów prawa europejskiego, taki przekaz do państwa trzeciego z zasady nie byłby możliwy, celem umowy w sprawie danych PNR jest umożliwienie przekazywania danych osobowych zgodnie z europejskimi wymogami ochrony danych poprzez przyjęcie szczególnych zabezpieczeń.

20. Z wyżej wymienionych powodów EIOD uważa, że umowa powinna, przynajmniej zasadniczo, opierać się na treści art. 16 TFUE ([8]).

2.2. **Cel i definicje**

21. EIOD odnotowuje, że w art. 3 wniosku szczegółowo definiuje się cele, w jakich dane PNR mogą być przetwarzane. Ubolewa on zarazem nad tym, że obecne definicje są szersze niż definicje zawarte we wniosku w sprawie dyrektywy o UE-PNR, której treść powinna była zostać doprecyzowana, szczególnie w odniesieniu do lżejszych przestępstw.

22. O ile definicje zawarte we wniosku dotyczącym UE-PNR uwzględniają konsekwencje działań zdefiniowanych jako „terrorystyczne", takich jak konkretne szkody ponoszone przez osoby i rządy (śmierć, atak na integralność cielesną osoby, zniszczenie systemu transportowego, elementu infrastruktury itp.), niniejszy wniosek jest mniej szczegółowy, a bardziej zorientowany na cel, kiedy odnosi się do zastraszania osób, rządów lub poważnej destabilizacji podstawowych struktur politycznych lub gospodarczych.

([1]) Sprawa C-491/01, British American Tobacco, w szczególności pkt 92–93.

([2]) Sprawa C-42/97 Parlament przeciw Radzie, pkt 39 i 40.

([3]) Zob. podobnie sprawa C-491/01, British American Tobacco, pkt 92–93, sprawa C-42/97 Parlament przeciw Radzie, pkt 38.

([4]) Trybunał uznał to w argumentacji odnoszącej się do okoliczności faktycznych wyroków w sprawie danych PNR, sprawy połączone C-317/04 i C-318/04, pkt 33.

([5]) — W uzasadnieniu uznano, że przepisy prawa wspólnotowego dotyczące ochrony danych nie pozwalają przewoźnikom na przekazywanie danych PNR do krajów niegwarantujących odpowiedniego poziomu ochrony. Stąd też „potrzebne jest rozwiązanie tworzące podstawy prawne przekazu […], aby zapewnić […] poszanowanie praw jednostek do ochrony danych osobowych".

— Cel, jakim jest zapewnienie poszanowania prawa do ochrony danych osobowych wynika dość jasno z preambuły, a konkretnie z motywu cytującego art. 6 TUE, art. 16 TFUE, art. 8 EKPC, Konwencję 108 itd.

— Preambuła odwołuje się również do odpowiednich przepisów prawa australijskiego w materii ochrony danych osobowych, wskazując na to, że przewidują one ochronę danych, prawo dostępu i prawo do złożenia skargi, poprawienia i przedstawienia uwag oraz środki zaradcze i sankcje w przypadku niewłaściwego wykorzystania danych osobowych.

— Artykuł 1 umowy, zatytułowany „Cel porozumienia", stanowi, że w umowie przewiduje się przekazywanie danych PNR. Ponadto w umowie „określa się warunki, na jakich możliwe jest przekazywanie i wykorzystywanie tych danych, oraz sposób ich ochrony" (kursywa autora).

([6]) Takie jak przepisy prawne dotyczące danych szczególnie chronionych, bezpieczeństwa danych, odpowiedzialności i rozliczalności, przejrzystości, prawa dostępu, poprawienia, usunięcia, prawa do złożenia skargi, przetwarzania automatycznego itp.

([7]) Opinia 2/2000, protokół kartageński, pkt 33.

([8]) W tym kontekście należy odnieść się do Deklaracji 21 w sprawie „ochrony danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych", dołączonej do traktatu lizbońskiego. Z treści Deklaracji 21 jasno wynika, że nawet w przypadkach, w których mamy do czynienia z pewnym elementem współpracy policyjnej, instrument ochrony danych na tym obszarze powinien nadal opierać się na treści art. 16 TFUE (a w razie potrzeby również na innych przepisach). Analiza ta w żaden sposób nie narusza podziału zadań w Komisji Europejskiej.

23. EIOD uważa, że konieczna jest większa precyzja w odniesieniu do wyrażeń „zastraszanie, zmuszanie i wymuszanie", a także „podstawowe polityczne, konstytucjonalne, gospodarcze lub (szczególnie) społeczne struktury kraju lub organizacji międzynarodowej". Zapobiegłoby to wprowadzeniu w życie systemu PNR w przypadkach, które nie powinny być objęte jego zakresem, na przykład w odniesieniu do działań legalnych (na przykład demonstracji pokojowych) w kontekście społecznym, kulturowym lub politycznym ([1]).

24. Możliwość przetwarzania danych w innych wyjątkowych przypadkach budzi dodatkowe wątpliwości, zwłaszcza gdy odnosi się do „zagrożenia zdrowia". EIOD uważa, że takie rozszerzenie celu jest nieproporcjonalne, szczególnie biorąc pod uwagę możliwość udostępnienia alternatywnych i bardziej specyficznych procedur w sytuacji zagrożenia zdrowia, w razie potrzeby dostosowanych do konkretnego przypadku. Ponadto, dane PNR nie są najodpowiedniejszym narzędziem identyfikacji pasażerów: istnieją bardziej niezawodne dane, a konkretnie dane API.

25. EIOD odnotowuje również, że lista danych PNR dołączona do wniosku wykracza poza to, co w opiniach Grupy Roboczej Art. 29 organy ochrony danych uznały za proporcjonalne ([2]). Listę tę należy zredukować. Szczególnie włączenie pola „Uwagi ogólne", które może zawierać nieistotne dane, chociaż potencjalnie również te szczególnie chronione, jest nieuzasadnione, i powinno ono zostać usunięte.

2.3. **Dane szczególnie chronione**

26. EIOD z zadowoleniem przyjmuje fakt, że wykaz przetwarzanych danych nie uwzględnia danych szczególnie chronionych, zgodnie z treścią art. 8 wniosku. Jednocześnie projekt tego przepisu nadal sugeruje, że dane szczególnie chronione mogą być „przetwarzane". Przepis ten zezwala najpierw na przesyłanie tych danych przez linie lotnicze, a następnie na ich usuwanie przez organy publiczne. Przesyłanie danych przez linie lotnicze stanowi ich przetwarzanie. EIOD uważa, że linie lotnicze powinny mieć obowiązek odfiltrowania danych szczególnie chronionych u źródła przetwarzania.

2.4. **Bezpieczeństwo danych**

27. Z zadowoleniem przyjęto art. 9 wniosku, który stanowi obszerny przepis na temat bezpieczeństwa i integralności danych. EIOD popiera w szczególności obowiązek informowania o przypadkach zagrożenia bezpieczeństwa urząd australijskiego komisarza ds. informacji. W odniesieniu do dalszego przesyłania informacji do Komisji Europejskiej potrzebne byłyby dodatkowe wyjaśnienia dotyczące wdrażanej procedury. Ponadto EIOD uważa, że organy ochrony danych również należy uznać za właściwych odbiorców tego rodzaju informacji oraz że należy je wymienić we wniosku.

2.5. **Nadzór i egzekwowanie**

28. Z zadowoleniem przyjęto system nadzoru obejmujący środki nadzoru i rozliczalności oraz eliminujący dyskryminację ze względu na narodowość lub miejsce zamieszkania. EIOD również wspiera podstawowe prawa każdej jednostki do administracyjnego dochodzenia roszczeń i skutecznej ochrony prawnej. Uważa, że urząd australijskiego komisarza ds. informacji odgrywa ważną rolę jako gwarant możliwości dochodzenia roszczeń i ochrony praw osób, których dotyczą dane.

2.6. **Zautomatyzowane decyzje indywidualne**

29. Zgodnie z treścią art. 15, interpretowanego *a contrario*, zautomatyzowana decyzja, która nie „wpływa w sposób istotny lub nie wywiera szkodliwego skutku prawnego dla pasażera" może zostać podjęta w oparciu o zautomatyzowany proces przetwarzania danych. Zabezpieczenie to ma zastosowanie jedynie wtedy, gdy decyzja mogłaby w wyraźny sposób wpłynąć na pasażera. Biorąc pod uwagę szeroki zakres zautomatyzowanego przetwarzania danych osobowych uwzględniony w systemie PNR, EIOD uważa, że ograniczenie to można zakwestionować. Aby zapobiec elastycznej interpretacji przepisu, zaleca on usunięcie wyrażenia „znacząco" i zapewnienie, że żadna zautomatyzowana decyzja mogąca wywołać szkodliwy skutek dla zainteresowanej osoby nie zostanie podjęta.

2.7. **Zatrzymywanie danych**

30. EIOD uważa, że okres zatrzymywania danych przewidziany w art. 16 stanowi jedną z najważniejszych trudności związanych z wnioskiem. Okres zatrzymywania danych, wynoszący pięć i pół roku, w tym trzy lata bez maskowania danych, jest w oczywisty sposób nieproporcjonalny, szczególnie w porównaniu z okresem zatrzymywania danych ustalonym w poprzednim australijskim systemie PNR, który przewidywał przechowywanie danych wyłącznie na podstawie decyzji podejmowanych dla każdego przypadku indywidualnie ([3]). Tak długi okres zatrzymywania danych, którego w poprzednim australijskim systemie PNR nie uznano za niezbędny, wymaga uzasadnienia.

31. Zgodnie ze stanowiskiem przyjętym w opinii w sprawie wniosku dotyczącego dyrektywy w sprawie UE-PNR EIOD uważa, że wszystkie dane powinny zostać poddane pełnej (tj. nieodwracalnej) anonimizacji, najpóźniej po upływie 30 dni, jeżeli nie bezpośrednio po analizie.

([1]) W tym zakresie nie dość precyzyjne prawodawstwo nie powinno naruszać m.in. podstawowej wolności zrzeszania się (art. 12 Karty praw podstawowych).

([2]) Opinia z dnia 23 czerwca 2003 r. w sprawie poziomu ochrony zapewnianej w Stanach Zjednoczonych przy przekazywaniu danych pasażerów, WP78.

([3]) Zob. podobnie pozytywna opinia Grupy Roboczej Art. 29: opinia 1/2004 z dnia 16 stycznia 2004 r. dotycząca poziomu ochrony zapewnionego w Australii w związku z przekazywaniem przez linie lotnicze danych pasażera, WP 85. W opinii uwzględnia się fakt, iż „organy celne stosują ogólną politykę niezatrzymywania w odniesieniu do tych danych. W odniesieniu do 0,05–0,1 % danych pasażerów, które przekazuje się organom celnym do celów dalszej oceny, dane PNR linii lotniczych są tymczasowo zatrzymywane w oczekiwaniu na wyniki oceny granicznej, jednak nie są przechowywane. Po uzyskaniu wyników dane PNR tych pasażerów są usuwane z komputera danego funkcjonariusza celnej jednostki analizy pasażerów i nie są wprowadzane do australijskiej bazy danych".

2.8. **Dalsze przekazywanie danych**

32. Gwarancje przewidziane w art. 18 i 19 zostały przychylnie przyjęte przez EIOD, w szczególności z uwagi na fakt, że obejmują one listę odbiorców danych w Australii w poszczególnych przypadkach przesyłania danych, a także ocenę konieczności przekazywania danych w każdym konkretnym przypadku. EIOD odnotowuje jednak, że przepis ten można obejść stosując wyjątek przewidziany w art. 18 ust. 1 lit. c), który przewiduje wymianę danych pozbawionych cech umożliwiających identyfikację osoby, nawet jeśli decyzja nie jest podejmowana oddzielnie dla każdego przypadku. Depersonalizacja nie oznacza jednak usuwania elementów pozwalających na identyfikację, ale ich zamaskowanie przy zachowaniu pełnego dostępu do danych. Z tego powodu EIOD zaleca rezygnację z możliwości stosowania wyjątku od przekazywania danych na zasadzie „indywidualnej". Jako dodatkowy mechanizm zabezpieczający EIOD proponuje ograniczenie przekazywania danych organom, „których zadanie polega na walce z terroryzmem lub przestępczością międzynarodową", zamiast udostępniania ich organom, których funkcje są „bezpośrednio związane z przeciwdziałaniem (tym) przestępstwom".

33. Popiera się przekazywanie danych do państw trzecich pod warunkiem, że państwa te zapewniają „takie same" zabezpieczenia, jak zabezpieczenia przewidziane w oryginalnej umowie. Biorąc pod uwagę, że dalszy przekaz oznacza utratę kontroli nad sposobami przetwarzania danych, a także brak umowy międzynarodowej gwarantującej skuteczne stosowanie zabezpieczeń przez nowych odbiorców, EIOD sugeruje, aby przekazywanie danych wymagało uprzedniego uzyskania zezwolenia prawnego.

34. We wniosku przewiduje się, że kiedy dane dotyczące rezydenta jednego z państw członkowskich UE zostają przekazane do państwa trzeciego, zainteresowane państwo członkowskie powinno zostać poinformowane o zaistniałej sytuacji w zakresie, w jakim australijska służba celna i straż graniczna jest tego świadoma (artykuł 19 ust. 1 lit. f)). EIOD uważa, że należy uwzględnić obowiązek przekazania państwu członkowskiemu dodatkowych szczegółów wyjaśniających cel takiej transmisji danych. Jeżeli przekazanie ma wpływ na osobę, której dotyczą dane, należy przedstawić dodatkowe uzasadnienie i zastosować dodatkowe zabezpieczenia.

35. Wreszcie, jeżeli chodzi o przekazywanie danych na terytorium Australii i do państw trzecich, zarówno w art. 18 jak i art. 19 przewiduje się ogólną zasadę, zgodnie z którą nic nie może zapobiec ujawnieniu danych PNR jeżeli jest ono wymagane do realizacji celu określonego w art. 3 ust. 4 ([1]), tj. w razie wyjątkowych okoliczności w celu ochrony żywotnych interesów jednostki, w tym zagrożenia zdrowia. EIOD zakwestionował już ryzyko szerokiej interpretacji tego wyjątku. Ponadto nie widzi on powodu, dla którego jakiekolwiek przekazanie danych w wyjątkowych okolicznościach nie miałoby być objęte zabezpieczeniami przewidzianymi w art. 18 i 19, szczególnie w zakresie ograniczenia celu i minimalizacji danych, a także w odniesieniu do ochrony tożsamości odbiorców i poziomu ochrony zagwarantowanego danym osobowym.

([1]) A także dla celów określonych w art. 10, kiedy dane przekazywane są na terytorium Australii.

2.9. **Przekazywanie danych przez linie lotnicze**

36. Zgodnie z treścią art. 21 ust. 3, w wyjątkowych okolicznościach możliwe jest przekazanie danych PNR organom więcej niż pięć razy w ciągu lotu w razie wystąpienia szczególnego zagrożenia. Aby zwiększyć pewność prawną, warunki takich dodatkowych przekazów danych powinny być określone bardziej szczegółowo, a przede wszystkim należy przewidzieć dodatkowy wymóg zaistnienia bezpośredniego zagrożenia.

2.10. **Przegląd umowy**

37. EIOD uważa, że warunki przeglądu powinny być bardziej szczegółowo określone pod kilkoma względami. Po dokonaniu wstępnego przeglądu należy określić częstotliwość kolejnych. Ponadto ograny ochrony danych powinny być wyraźnie reprezentowane w zespole przeglądowym, a nie tylko na zasadzie warunkowej.

38. EIOD sugeruje, by przegląd koncentrował się również na ocenie konieczności i proporcjonalności środków poprzez gromadzenie danych statystycznych na temat liczby osób zainteresowanych i rzeczywiście skazanych w oparciu o dane PNR, jak również na przestrzeganiu praw osób, których dotyczą dane. W ramach oceny należy sprawdzić, w jaki sposób wnioski składane przez osoby, których dotyczą dane, są przetwarzane w praktyce, szczególnie w przypadkach, w których nie wyrażono zgody na bezpośredni dostęp.

3. **WNIOSKI**

39. EIOD w zadowoleniem przyjmuje zabezpieczenia zaproponowane we wnioskach, zwłaszcza w odniesieniu do wykonania umowy. W szczególnie satysfakcjonujący sposób opracowano kwestie związane z bezpieczeństwem danych, nadzorem i wykonaniem. EIOD podkreśla, że każda jednostka ma prawo zwrócić się do australijskiego organu ochrony danych, a także do australijskich władz sądowych. Gwarancje te są jednymi z najistotniejszych, jakie przewidziano we wnioskach.

40. EIOD podkreśla jednak, że pozostają kwestie wymagające udoskonalenia, szczególnie w odniesieniu do zakresu umowy, definicji terroryzmu oraz włączenia pewnych szczególnych celów, a także okresu zatrzymywania danych PNR. W porównaniu z poprzednim australijskim systemem PNR, a także z propozycją UE-PNR, okres zatrzymywania danych jest nieproporcjonalny.

41. Należy ponownie rozważyć podstawę prawną umowy. Uwzględniając ustalone orzecznictwo, EIOD uważa, że poza art. 218 ust. 6 lit. a) umowa powinna przede wszystkim opierać się na art. 16 TFUE, a nie na art. 82 ust. 1 lit. d) i art. 87 ust. 2 lit. a) TFUE. Jest to w pełni zgodne z treścią Deklaracji 21 dołączonej do traktatu lizbońskiego.

42. Uwagi te należy odczytywać w szerszym kontekście legitymacji jakiegokolwiek systemu PNR, postrzeganego jako systematyczne gromadzenie danych na temat pasażerów na potrzeby oceny ryzyka. Wniosek może spełnić inne wymogi tworzące ramy ochrony danych tylko pod warunkiem, że system spełnia podstawowe wymogi konieczności i proporcjonalności, zgodnie z art. 7 i 8 Karty praw podstawowych oraz art. 16 TFUE.

43. W związku z powyższym EIOD stwierdza, że należy poświęcić więcej uwagi podstawowym wymogom w trakcie przeprowadzania ocen końcowych poprzedzających zawarcie umowy.

Sporządzono w Brukseli dnia 15 lipca 2011 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych