

**Opinia Europejskiego Inspektora Ochrony Danych 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**

(2011/C 181/02)

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 <sup>(1)</sup>,

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 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 <sup>(2)</sup>,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

## I. WPROWADZENIE

### I.1. Konsultacja EIOD

1. Dnia 2 lutego 2011 r. Komisja przyjęła 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 (zwany dalej „wnioskiem”) <sup>(3)</sup>. Tego samego dnia wniosek przekazano do EIOD do konsultacji.
2. EIOD z zadowoleniem przyjmuje fakt, że Komisja się z nim skonsultowała. Jeszcze przed przyjęciem wniosku EIOD miał możliwość przedstawienia nieformalnych uwag. Niektóre z tych uwag uwzględniono we wniosku i EIOD zauważa, że zasadniczo spowodowało to wzmocnienie zabezpieczeń w zakresie ochrony danych we wniosku. Wiele kwestii nadal jednak budzi niepokój, w szczególności w związku z zakresem i celami gromadzenia danych osobowych.

### I.2. Kontekst wniosku

3. Dyskusje na temat ewentualnego systemu PNR w UE są prowadzone od przyjęcia przez Komisję w roku 2007.

wniosku dotyczącego decyzji ramowej Rady w tej kwestii <sup>(4)</sup>. Głównym celem systemu UE-PNR jest ustanowienie systemu, w ramach którego przewoźnicy lotniczy obsługujący loty między UE i państwami trzecimi mieliby obowiązek przekazywania właściwym organom danych PNR wszystkich pasażerów w celu zapobiegania przestępstwom o charakterze terrorystycznym i poważnym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania. Dane byłyby scentralizowane i analizowane przez biura danych pasażerów, a wyniki analizy przekazywano by właściwym organom krajowym w każdym państwie członkowskim.

4. Od 2007 r. EIOD uważnie śledzi rozwój sytuacji w związku z ewentualnym systemem UE-PNR i jednocześnie rozwój sytuacji w zakresie systemów PNR państw trzecich. Dnia 20 grudnia 2007 r. EIOD przyjął opinię w sprawie tego wniosku Komisji <sup>(5)</sup>. Przy wielu dalszych okazjach nie tylko EIOD, ale również Grupa Robocza Art. 29 <sup>(6)</sup> poczynili spójne uwagi w kwestii zgodności przetwarzania danych PNR do celów egzekwowania prawa z zasadą proporcjonalności i konieczności oraz z innymi podstawowymi zabezpieczeniami w zakresie ochrony danych.
5. Główną kwestią konsekwentnie podnoszoną przez EIOD jest uzasadnienie konieczności dodania europejskiego systemu PNR do szeregu innych instrumentów umożliwiających przetwarzanie danych osobowych do celów egzekwowania prawa.
6. EIOD przyznaje, że w porównaniu z wersją, którą poprzednio z nim konsultowano, przedmiotowy wniosek zawiera widoczne usprawnienia w zakresie ochrony danych. Usprawnienia te dotyczą w szczególności zakresu stosowania wniosku, definicji roli różnych zainteresowanych stron (biur danych pasażerów), wyłączenia przetwarzania danych szczególnie chronionych, przechodzenia na system aktywnego przekazywania danych bez okresu przejściowego <sup>(7)</sup>, a także ograniczenia pod względem zatrzymywania danych.

<sup>(4)</sup> COM(2007) 654 wersja ostateczna.

<sup>(5)</sup> Opinia EIOD z dnia 20 grudnia 2007 r. w sprawie projektu wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa, (Dz.U. C 110 z 1.5.2008, s. 1).

<sup>(6)</sup> — Opinia z dnia 19 października 2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, dostępna pod adresem: <http://www.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC/OC2010>

— Opinie Grupy Roboczej Art. 29 dostępne są pod następującym adresem internetowym: [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index\\_en.htm#data\\_transfers](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers)

<sup>(7)</sup> Oznacza to, że dane PNR powinny być aktywnie przekazywane przez linie lotnicze, a nie „pobierane” przez władze publiczne dzięki bezpośredniemu dostępowi do bazy danych linii lotniczych.

<sup>(1)</sup> Dz.U. L 281 z 23.11.1995, s. 31.

<sup>(2)</sup> Dz.U. L 8 z 12.1.2001, s. 1.

<sup>(3)</sup> COM(2011) 32 wersja ostateczna.

7. EIOD z zadowoleniem przyjmuje również dodatkowe zmiany dotyczące oceny skutków pod kątem powodów dla wprowadzenia systemu UE-PNR. Mimo że wyraźnie widać wolę wyjaśnienia konieczności wprowadzenia tego systemu, według EIOD uzasadnienia te nie stanowią przekonującej podstawy do utworzenia przedmiotowego systemu, zwłaszcza w odniesieniu do zakrojonej na szeroką skalę „wstępnej oceny” wszystkich pasażerów. Analizę potrzeby i proporcjonalności przedstawiono poniżej w rozdziale II. Rozdział III dotyczy bardziej szczegółowych aspektów wniosku.

## II. KONIECZNOŚĆ I PROPORCJONALNOŚĆ WNIOSKU

### II.1. Wstępne uwagi dotyczące konieczności i proporcjonalności

8. Niezbędnym warunkiem opracowania systemu PNR jest wykazanie konieczności i proporcjonalności przetwarzania danych. Już przy wcześniejszych okazjach, szczególnie w kontekście ewentualnego przeglądu dyrektywy 2006/24/WE („dyrektywy w sprawie zatrzymywania danych”), EIOD podkreślał, że potrzeba przetwarzania lub przechowywania ogromnych ilości informacji powinna opierać się na wyraźnym wykazaniu związku między zastosowaniem i wynikami, oraz powinna umożliwić ocenę *sine qua non* kwestii, czy możliwe byłoby uzyskanie porównywalnych wyników przy zastosowaniu alternatywnych środków w mniejszym stopniu naruszających prywatność<sup>(1)</sup>.
9. W celu uzasadnienia wprowadzenia systemu, wniosek, a w szczególności towarzysząca mu ocena skutków, zawiera obszerną dokumentację i argumentację prawną, które mają na celu ugruntowanie zarówno potrzeby systemu, jak i jego zgodności z wymogami w zakresie ochrony danych. We wniosku posunięto się nawet dalej twierdząc, że system wnosi wartość dodaną pod względem harmonizacji standardów ochrony danych.
10. Po przeanalizowaniu tych elementów, EIOD uważa, że aktualna treść wniosku nie spełnia wymogów konieczności i proporcjonalności, nałożonych w art. 8 Karty praw podstawowych Unii Europejskiej, art. 8 EKPC i art. 16 TFUE. Powody, z których wynika ten pogląd, wyjaśniono w następujących punktach.

### II.2. Dokumenty i dane statystyczne udostępnione przez Komisję

11. EIOD odnotowuje, że w ocenie skutków zawarto obszernie wyjaśnienia i dane statystyczne na poparcie wniosku. Elementy te nie są jednak przekonujące. Ilustracją tego jest podanie w opisie zagrożenia terroryzmem i poważną przestępczością zawartym w ocenie skutków i w uzasadnieniu wniosku<sup>(2)</sup> liczby 14 000 przestępstw przypadają-

cych na 100 000 osób w państwach członkowskich w 2007 r. Chociaż liczba ta może robić wrażenie, dotyczy ona niezróżnicowanych rodzajów przestępstw i nie może stanowić argumentu na poparcie wniosku dotyczącego wyłącznie ograniczonego rodzaju poważnych przestępstw, przestępstw transgranicznych i terroryzmu oraz ich zwalczania. Ponadto w opinii EIOD cytowanie sprawozdania dotyczącego „problemów” narkotykowych bez powiązania danych statystycznych z rodzajem handlu narkotykami, którego dotyczy wniosek, nie stanowi uzasadnionego odniesienia. To samo dotyczy sygnalizowania skutków przestępstw, przytaczania „wartości skradzionych rzeczy” oraz psychologicznego i fizycznego wpływu na ofiary, które nie są danymi bezpośrednio związanymi z celem wniosku.

12. Ostatni przykład dotyczy oceny skutków, w której wskazuje się, że Belgia „podała, że 95 % wszystkich operacji zajęcia narkotyków w 2009 r. było możliwe wyłącznie lub w decydującym stopniu dzięki przetwarzaniu danych PNR”. Należy jednak podkreślić, że Belgia nie posiada (jeszcze) wdrożonego systematycznego systemu PNR porównywalnego z tym, jaki przewiduje się we wniosku. Mogłoby to oznaczać, że dane PNR mogą być przydatne w konkretnych przypadkach, czego EIOD nie kwestionuje. Istotne zastrzeżenia związane z ochroną danych raczej budzi szeroko zakrojone gromadzenie w celu systematycznej oceny wszystkich pasażerów.
13. EIOD uważa, że nie przedstawiono wystarczającej liczby odpowiednich i dokładnych dokumentów wykazujących konieczność wprowadzenia przedmiotowego instrumentu.

### II.3. Warunki ograniczenia pewnego prawa podstawowego

14. Chociaż w dokumencie zauważa się, że przedmiotowe środki przetwarzania danych naruszają postanowienia Karty, EKPC i art. 16 TFUE, bezpośrednio odniesiono się w nim do ewentualnych ograniczeń tych praw i zadowolono wnioskiem, że „ponieważ celem proponowanych działań byłoby zwalczanie terroryzmu i innych poważnych przestępstw, ujętych w akcie ustawodawczym, byłyby one wyraźnie zgodne z takimi wymogami, pod warunkiem, że są konieczne w demokratycznym społeczeństwie i zgodne z zasadą proporcjonalności”<sup>(3)</sup>. Brakuje jednak wyraźnego wykazania faktu, że przedmiotowe środki są niezbędne i że nie istnieją żadne mniej inwazyjne alternatywy.
15. W tym sensie fakt, że przewidziano takie dodatkowe cele jak egzekwowanie prawa w kwestiach imigracji, wykaz osób, którym zakazano lotów, i bezpieczeństwo zdrowotne, które ostatecznie nie zostały uwzględnione ze względów proporcjonalności, nie oznacza, iż „ograniczenie” przetwarzania danych PNR do poważnej przestępczości i terroryzmu jest faktycznie proporcjonalne ze względu na mniejszą inwazyjność. Nie oceniono również możliwości ograniczenia systemu do walki z terroryzmem, bez

<sup>(1)</sup> Zob. przemówienie Petera Hustinksa „The moment of truth for the Data Retention Directive” („Chwila prawdy o dyrektywie w sprawie zatrzymywania danych”) wygłoszone w Brukseli dnia 3 grudnia 2010 r. na konferencji „Taking on the Data Retention Directive” („Przyjmowanie dyrektywy w sprawie zatrzymywania danych”), dostępne na stronie [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03\\_Data\\_retention\\_speech\\_PH\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf)

<sup>(2)</sup> Ocena skutków rozdział 2.1.1 oraz Uzasadnienie rozdział 1 ust. 1.

<sup>(3)</sup> Ocena skutków rozdział 3.2 ust. 2.

uwzględniania dodatkowych przestępstw, jak przewidziano we wcześniejszych systemach PNR, w szczególności w australijskim systemie PNR. EIOD podkreśla, że w tym początkowym systemie, w odniesieniu do którego w 2004 r. Grupa Robocza Art. 29 przyjęła pozytywną opinię, cele ograniczono do „identyfikacji tych pasażerów, którzy mogą stanowić zagrożenie terrorystyczne lub zagrożenie związaną z nim działalnością przestępczą”<sup>(1)</sup>. W systemie australijskim nie przewidziano również zatrzymywania danych PNR z wyjątkiem danych dotyczących konkretnych pasażerów zidentyfikowanych jako osoby stanowiące szczególne zagrożenie<sup>(2)</sup>.

16. Ponadto w odniesieniu do przewidywalności nadzoru osób, których dane dotyczą, wątpliwe jest, aby wniosek Komisji spełniał wymogi solidnej podstawy prawnej w świetle prawa UE: „ocena” pasażerów (wcześniej sformułowana jako „ocena ryzyka”) będzie przeprowadzana na podstawie stale zmieniających się i nieprzejrzystych kryteriów. Jak wyraźnie stwierdzono w tekście, głównym celem systemu nie jest tradycyjna kontrola graniczna, tylko działalność wywiadowcza<sup>(3)</sup> i zatrzymywanie osób, które nie są podejrzane, zanim popełnią przestępstwo. Utworzenie takiego systemu na skalę europejską, oznaczającego gromadzenie danych dotyczących wszystkich pasażerów i podejmowanie decyzji na podstawie nieznanymi i zmieniającymi się kryteriów oceny, budzi poważne wątpliwości co do przejrzystości i proporcjonalności takiego środka.
17. Jedynym celem, który według EIOD byłby zgodny z wymogami przejrzystości i proporcjonalności, byłoby wykorzystanie danych PNR w poszczególnych przypadkach, o których mowa w art. 4 ust. 2 lit. c), lecz wyłącznie w razie poważnego lub konkretnego zagrożenia ustalonego na podstawie konkretnych wskaźników.

#### II.4. Ryzyko rozrostu funkcji

18. Artykuł 4 ust. 2 lit. b) stanowi, że biuro danych pasażerów może przeprowadzać ocenę pasażerów, w ramach której może porównywać dane PNR z innymi „właściwymi bazami danych”, jak wskazano w art. 4 ust. 2 lit. b). W przepisie tym nie wskazano, które bazy danych są właściwe. W związku z tym środek jest nieprzewidywalny,

<sup>(1)</sup> 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.

<sup>(2)</sup> W swojej opinii Grupa Robocza Art. 29 dalej wyjaśnia również, że „w odniesieniu do zatrzymywania danych PNR nie istnieje ustawowy obowiązek zatrzymywania danych PNR przez organy celne. Podobnie nie istnieje ustawowy zakaz przechowywania takich danych przez organy celne. Dane PNR dotyczące pasażerów ocenionych za pośrednictwem oprogramowania automatycznie analizującego profile i ocenionych jako niskie ryzyko (95 %–97 % pasażerów) nie są zatrzymywane i nie przechowywane się żadnych danych PNR ich dotyczących. Organów celne stosują zatem ogólną politykę niezatrzymywania w odniesieniu do tych danych. W odniesieniu do 0,05 %–0,1 % danych pasażerów, które przekazuje się do organów celnych 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”.

<sup>(3)</sup> Uzasadnienie rozdział 1. Kontekst wniosku, Spójność z innymi politykami i celami Unii.

a przewidywalność jest również wymogiem zawartym w Karcie i EKCP. Ponadto przepis ten poddaje w wątpliwość jego zgodności z zasadą celowości: według EIOD należy wykluczyć na przykład takie bazy danych jak Eurodac, którą opracowano do innych celów<sup>(4)</sup>. Ponadto takie działanie powinno być możliwe wyłącznie w razie wystąpienia określonej potrzeby w konkretnym przypadku, w którym dana osoba jest już podejrzana po dokonaniu przestępstwa. Przykładowo systematyczne porównywanie bazy danych wizowego systemu informacyjnego<sup>(5)</sup> ze wszystkimi danymi PNR byłoby działaniem nadmiernym i nieproporcjonalnym.

#### II.5. Wartość dodana wniosku pod względem ochrony danych

19. Koncepcja, zgodnie z którą wniosek zwiększy ochronę danych poprzez zapewnienie jednolitych równych szans w zakresie praw osób fizycznych, budzi wątpliwość. EIOD przyznaje, że gdyby uzasadniono konieczność i proporcjonalność systemu, zwiększono by pewność prawa dzięki jednolitym normom w UE, w tym dotyczącym ochrony danych. W obecnym brzmieniu wniosku, motyw 28, wspomina się jednak, że „niniejsza dyrektywa nie wpływa na możliwość ustanowienia przez państwa członkowskie, w swoim prawie krajowym, systemu gromadzenia danych PNR i zarządzania tymi danymi do celów innych niż te określone w niniejszej dyrektywie lub gromadzenia danych pochodzących od innych dostawców usług transportowych niż ci określani w niniejszej dyrektywie, w odniesieniu do lotów wewnętrznych [...]”.
20. Wynikająca z wniosku harmonizacja ma zatem ograniczony charakter. Może ona obejmować prawa osób, których dane dotyczą, lecz nie celowość, i można założyć, że zgodnie z tym brzmieniem systemy PNR już stosowane do zwalczania na przykład nielegalnej imigracji można będzie w dalszym ciągu stosować do tego celu na mocy przedmiotowej dyrektywy.
21. Oznacza to, że z jednej strony pozostałyby pewne różnice między państwami członkowskimi, które opracowały już system PNR, a z drugiej strony znacząca większość państw członkowskich, które nie gromadzą systematycznie danych PNR (21 z 27 państw członkowskich), zostałyby zobowiązane do ich gromadzenia. EIOD uważa, że z tego punktu widzenia jakakolwiek wartość dodana w rozumieniu ochrony danych jest wysoce wątpliwa.

<sup>(4)</sup> Celem Eurodac „jest określenie, które państwo członkowskie ma być właściwe zgodnie z Konwencją Dublińską do badania wniosków o azyl wniesionych w państwie członkowskim, jak również w celu ułatwienia stosowania Konwencji Dublińskiej zgodnie z warunkami określonymi w niniejszym rozporządzeniu” zgodnie z art. 1 ust. 1 rozporządzenia Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczącego ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej, (Dz.U. L 316 z 15.12.2000, s. 1).

<sup>(5)</sup> „Celem VIS jest poprawa realizacji wspólnej polityki wizowej, poprawa współpracy konsularnej i procesu konsultacji pomiędzy centralnymi organami wizowymi poprzez ułatwienie wymiany danych pomiędzy państwami członkowskimi o wnioskach i związanych z nimi decyzjach” zgodnie z art. 2 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), (Dz.U. L 218 z 13.8.2008, s. 60).



22. Wręcz przeciwnie, konsekwencjami motywu 28 jest poważne naruszenie zasady celowości. Zdaniem EIOD wniosek powinien jednoznacznie stanowić, że danych PNR nie można stosować do innych celów.

23. EIOD dochodzi do podobnego wniosku, jaki wyciągnął z oceny dyrektywy w sprawie zatrzymywania danych: w obu kontekstach brak jest faktycznej harmonizacji, a tym samym pewności prawa. Ponadto dodatkowe gromadzenie i przetwarzanie danych osobowych staje się obowiązkowe dla wszystkich państw członkowskich, w których nie ustalono faktycznej konieczności wprowadzenia systemu.

#### II.6. Związek z komunikatem w sprawie zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości

24. EIOD zauważa również, że zmiany w zakresie PNR wiążą się z prowadzoną ogólną oceną wszystkich instrumentów UE w dziedzinie zarządzania wymianą informacji rozpoczętą przez Komisję w styczniu 2010 r. i szerzej omówioną w niedawnym komunikacie w sprawie przeglądu zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości<sup>(1)</sup>. Istnieje wyraźny związek z obecną debatą dotyczącą europejskiej strategii zarządzania informacjami. W związku z tym EIOD uważa, że przy ocenie konieczności wprowadzenia UE-PNR należy wziąć pod uwagę wyniki obecnych prac nad europejskim modelem wymiany informacji, których należy oczekiwać w 2012 roku.

25. W tym kontekście i w świetle niedoskonałości wniosku, a w szczególności towarzyszącej mu oceny skutków, EIOD uważa, że istnieje konieczność przeprowadzenia szczegółowej oceny skutków w zakresie ochrony prywatności i danych w takich przypadkach, jak ten, gdy istota wniosku wpływa na prawa podstawowe do prywatności i ochrony danych. Ogólna ocena skutków jest niewystarczająca.

### III. UWAGI SZCZEGÓŁOWE

#### III.1. Zakres stosowania

26. W art. 2 lit. g), h) oraz i) wniosku zdefiniowano przestępstwa terrorystyczne, poważną przestępczość i poważną przestępczość transgraniczną. EIOD z zadowoleniem przyjmuje fakt, że uszczegółowiono definicje i zakres ich stosowania, wprowadzając rozróżnienie na poważną przestępczość i poważną przestępczość transgraniczną. Rozróżnienie to tym bardziej budzi zadowolenie, że wskazuje na różny sposób przetwarzania danych osobowych, wyłączając ocenę według wcześniej ustalonych kryteriów w przypadku poważnych przestępstw niemających charakteru transgranicznego.

27. Zdaniem EIOD definicja poważnych przestępstw jest jednak w dalszym ciągu zbyt ogólna. Fakt ten został potwierdzony we wniosku, w którym zaznacza się, że państwa członkowskie mogą nadal wyłączać *łżejsze przestępstwa* objęte definicją poważnych przestępstw<sup>(2)</sup>, które nie byłyby zgodne

z zasadą proporcjonalności. Takie sformułowanie oznacza, że definicja zawarta we wniosku może obejmować *łżejsze przestępstwa*, których przetwarzanie byłoby nieproporcjonalne. Nie jest oczywiste, jakie konkretnie przestępstwa zalicza się do *łżejszych*. Zdaniem EIOD, zamiast pozostawiać zdolność zawężenia zakresu stosowania państwom członkowskim, we wniosku należy wyraźnie wymienić przestępstwa, które powinny zostać objęte zakresem jego stosowania i przestępstwa, które należy wykluczyć, ponieważ są uważane za *łżejsze* i nie spełniają kryterium proporcjonalności.

28. Ta sama obawa dotyczy pozostawionej w art. 5 ust. 5 możliwości przetwarzania danych dotyczących każdego rodzaju przestępstwa, jeżeli zostanie ono wykryte w toku działań podejmowanych przez organy ścigania, a także zawartej w motywie 28 możliwości poszerzenia zakresu stosowania tak, aby obejmował inne cele niż te, które przewidziano we wniosku, lub innych dostawców usług transportowych.

29. EIOD ma również obawy co do przewidzianej w art. 17 możliwości włączenia lotów wewnętrznych do zakresu stosowania dyrektywy, w świetle doświadczeń zdobytych przez państwa członkowskie, które już gromadzą dane dotyczące tych lotów. Takie poszerzenie zakresu stosowania systemu PNR jeszcze bardziej zagroziłoby prawom podstawowym osób fizycznych i nie należy przewidywać takiego poszerzenia przed przeprowadzeniem jakiegokolwiek odpowiedniej analizy, w tym kompleksowej analizy skutków.

30. Podsumowując, pozostawienie otwartego zakresu stosowania i zapewnienie państwom członkowskim możliwości poszerzenia celu jest sprzeczne z wymogiem, zgodnie z którym dane można gromadzić jedynie do określonych i jednoznacznych celów.

#### III.2. Biura danych pasażerów

31. Rola biur danych pasażerów oraz zabezpieczenia w zakresie przetwarzania danych PNR budzą szczególne wątpliwości, przede wszystkim dlatego, że biura danych pasażerów otrzymują dane wszystkich pasażerów od przewoźników lotniczych i posiadają – na mocy tekstu wniosku – szerokie kompetencje w zakresie przetwarzania tych danych. Obejmuje to ocenę zachowania pasażerów, których nie podejrzewa się o popełnienie żadnego przestępstwa, i możliwości porównania danych PNR z nieokreślonymi bazami danych<sup>(3)</sup>. EIOD zauważa, że we wniosku przewidziano „dostęp na restrykcyjnych warunkach”, jednak uważa, że w świetle szerokich kompetencji biur danych pasażerów same te warunki nie wystarczą.

32. Przede wszystkim charakter i struktura organu wyznaczonego jako biuro danych pasażerów nadal nie są przejrzyste. We wniosku wspomniano o możliwości, zgodnie z którą pracownicy mogą być „oddelegowani z właściwych organów publicznych”, jednak nie zapewnia się żadnych

<sup>(1)</sup> COM(2010) 385 wersja ostateczna.

<sup>(2)</sup> Jak określono w decyzjach ramowych Rady 2008/84/WSiSW i 2002/584/WSiSW.

<sup>(3)</sup> W odniesieniu do biur danych pasażerów zob. także opinię z dnia 20 grudnia 2007 r.

gwarancji pod względem kwalifikacji i integralności personelu biura danych pasażerów. EIOD zaleca uwzględnienie takich wymogów w tekście dyrektywy, biorąc pod uwagę, że biuro danych pasażerów przetwarza wrażliwe dane.

33. Po drugie, we wniosku przewidziano możliwość wyznaczenia jednego biura danych pasażerów dla kilku państw członkowskich. Stwarza to możliwość zaistnienia ryzyka wykorzystywania i przekazywania danych niezgodnie z warunkami zawartymi we wniosku. EIOD przyznaje, że połączenie sił może być pożądane ze względu na skuteczność, szczególnie w przypadku mniejszych państw członkowskich, jednak zaleca włączenie do tekstu uwarunkowań dla takiej możliwości. W ramach tych uwarunkowań należy rozwiązać kwestię współpracy z właściwymi organami, a także kwestię nadzoru, w szczególności w odniesieniu do organu ochrony danych odpowiedzialnego za nadzór i w odniesieniu do egzekwowania praw osób, których dane dotyczą, ponieważ kilka organów może być właściwych w zakresie nadzoru jednego biura danych pasażerów.
34. Istnieje ryzyko rozrostu funkcji związanego z wyżej wymienionymi elementami, a w szczególności z uwagi na jakość personelu właściwego do analizy danych, oraz korzystania z biura danych pasażerów przez kilka państw członkowskich.
35. Po trzecie, EIOD kwestionuje zabezpieczenia przewidziane na wypadek nadużyć. Z zadowoleniem przyjmuje się obowiązek rejestracji, jednak jest on niewystarczający. Monitorowanie władnej działalności powinno być uzupełniane monitorowaniem zewnętrznym w bardziej zorganizowany sposób. EIOD sugeruje systematyczne organizowanie audytów co 4 lata. Należy opracować kompleksowy zestaw zasad bezpieczeństwa i wdrożyć go horyzontalnie we wszystkich biurach danych pasażerów.

### III.3. Wymiana danych między państwami członkowskimi

36. W art. 7 wniosku przewiduje się szereg scenariuszy umożliwiających wymianę danych między biurami danych pasażerów – przy czym jest to sytuacja normalna – lub między właściwymi organami państwa członkowskiego i biurami danych pasażerów w wyjątkowych sytuacjach. Warunki różnią się pod względem restrykcyjności w zależności od tego, czy wnioskuje się o dostęp do bazy danych przewidzianej w art. 9 ust. 1, w której dane są przechowywane przez pierwsze 30 dni, czy do bazy danych wspomnianej w art. 9 ust. 1, w której dane są przechowywane przez kolejne pięć lat.
37. Warunki dostępu są ściślej określone, jeżeli wniosek o udzielenie dostępu wykracza poza zwyczajową procedurę. EIOD zauważa jednak, że użyte sformułowanie wprowadza zamieszanie: art. 7 ust. 2 ma zastosowanie w „konkretnym przypadku [...] do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania”; w art. 7 ust. 3 mowa o „wyjątkowych okolicznościach, w reakcji na konkretne zagrożenie lub konkretne postępowanie przygotowawcze lub sądowe związane z przestępstwem terrorystycznym lub poważnym przestępstwem”, natomiast art. 7 ust. 4 dotyczy zapobiegania „bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego”, a w art. 7 ust. 5 wspomina się „konkretne i faktyczne zagrożenie związane z

przestępstwem terrorystycznym lub poważnym przestępstwem”. Na tych kryteriach oparte są warunki dostępu różnych zainteresowanych stron do baz danych. Różnica między konkretnym zagrożeniem, bezpośrednim poważnym zagrożeniem oraz konkretnym i faktycznym zagrożeniem nie jest jednak przejrzysta. EIOD podkreśla potrzebę dalszego określenia dokładnych warunków, na podstawie których przekazywanie danych będzie dozwolone.

### III.4. Prawo właściwe

38. Wniosek nawiązuje do decyzji ramowej Rady 2008/977/WSiSW jako ogólnej podstawy prawnej w zakresie zasad ochrony danych podaje się i rozszerza się zakres jej stosowania o przetwarzanie danych na szczeblu krajowym.
39. Już w 2007 r.<sup>(1)</sup> EIOD podkreślił niedociągnięcia przedmiotowej decyzji ramowej pod względem praw osób, których dane dotyczą. Do elementów brakujących w przedmiotowej decyzji ramowej należą w szczególności niektóre wymogi w zakresie informowania osoby, której dane dotyczą, w przypadku wniosku o udzielenie dostępu do jej danych: informacji należy udzielać w zrozumiałym sposób, należy podać cel przetwarzania danych, a także istnieje potrzeba lepiej dopracowanych zabezpieczeń w razie odwoływania się do organu ochrony danych w przypadku odmowy dostępu.
40. Z odwołania do przedmiotowej decyzji ramowej wynikają również konsekwencje dotyczące identyfikacji organu ochrony danych właściwego w zakresie monitorowania stosowania przyszłej dyrektywy, ponieważ nie musi być to ten sam organ ochrony danych, który jest właściwy w odniesieniu do (byłych) kwestii związanych z pierwszym filarem. W kontekście polizbońskim EIOD uważa wyłączną zależność od przedmiotowej decyzji ramowej za niewystarczającą, ponieważ jednym z głównych celów jest przyjęcie ram prawnych w celu zapewnienia wysokiego i zharmonizowanego poziomu ochrony w ramach (byłych) filarów. Uważa, że we wniosku należy zawrzeć dodatkowe przepisy w celu uzupełnienia odwołania do ramowej decyzji Rady, w której zidentyfikowano niedociągnięcia, szczególnie w odniesieniu do warunków dostępu do danych osobowych.
41. Obawy te są również w pełni uzasadnione w odniesieniu do przepisów dotyczących przekazywania danych państwom trzecim. We wniosku odniesiono się do art. 13 ust. 3 ppkt (ii) decyzji ramowej, w którym zawarto obszerne wyjątki od zabezpieczeń w zakresie ochrony danych: w szczególności odstępuje się w nim od warunku adekwatności, jeżeli w grę wchodzi „uzasadniony interes ogólny, zwłaszcza z uwagi na ważny interes publiczny”. Brzmienie tego wyjątku jest mało precyzyjne i przy szerokiej interpretacji może potencjalnie mieć zastosowanie do wielu przypadków przetwarzania danych PNR. EIOD uważa, że we wniosku należy wyraźnie zapobiec stosowaniu wyjątków przewidzianych w decyzji ramowej w kontekście przetwarzania danych PNR oraz utrzymać wymóg restrykcyjnej oceny adekwatności.

<sup>(1)</sup> Trzecia opinia Europejskiego Inspektora Ochrony Danych z dnia 27 kwietnia 2007 r. w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, (Dz.U. C 139 z 23.6.2007, s. 1).

### III.5. Zatrzymywanie danych

42. We wniosku przewidziano okres zatrzymywania wynoszący 30 dni i dodatkowy okres pięciu lat archiwizacji. Ten okres zatrzymywania jest znacznie krótszy w porównaniu z poprzednimi wersjami dokumentu, w których okres zatrzymywania sięgał pięciu plus osiem lat.
43. EIOD z zadowoleniem przyjmuje skrócenie pierwszego okresu zatrzymywania do 30 dni. EIOD kwestionuje jednak dodatkowy okres zatrzymywania wynoszący 5 lat: zdaniem EIOD nie jest oczywiste, czy istnieje potrzeba dalszego zatrzymywania danych w formie, która w dalszym ciągu umożliwia identyfikację osób fizycznych.
44. Podkreśla również kwestię terminologiczną w tekście, która niesie za sobą poważne konsekwencje prawne: w art. 9 ust. 2 wskazuje się, że dane pasażerów będą „maskowane” i w związku z tym będą „zanonimizowane”. Dalej w tekście jest jednak mowa, że nadal istnieje możliwość dostępu do „pełnych danych PNR”. Taka możliwość oznacza, że dane PNR nigdy nie były całkowicie zanonimizowane: pomimo ich zamaskowania, pozostały identyfikowalne. W związku z tym ramy ochrony danych w dalszym ciągu mają pełne zastosowanie, co rodzi podstawowe pytanie o konieczność i proporcjonalność zatrzymywania identyfikowalnych danych wszystkich pasażerów na okres pięciu lat.
45. EIOD zaleca zmianę brzmienia wniosku, aby zachować zasadę faktycznej anonimizacji bez możliwości odtworzenia identyfikowalnych danych, co oznacza, że nie należy zezwalać na żadne dochodzenie działające wstecz. Istniałaby możliwość dalszego – i wyłącznego – wykorzystywania tych danych do ogólnych celów wywiadowczych opartych na identyfikacji wzorców terrorystycznych i wzorców związanej przestępczości w przepływach migracyjnych. Należy to odróżnić od zatrzymywania danych w identyfikowalnej formie – pod warunkiem zastosowania pewnych zabezpieczeń – w przypadkach budzących konkretne podejrzenia.

### III.6. Wykaz danych PNR

46. EIOD z zadowoleniem przyjmuje fakt, że wykaz przetwarzanych danych nie uwzględnia danych szczególnie chronionych. EIOD podkreśla jednak, że we wniosku nadal przewidziano możliwość przesłania tych danych do biura danych pasażerów, które następnie ma obowiązek je usunąć (art. 4 ust. 1, art. 11). Z tego sformułowania nie wynika jednoznacznie, czy biura danych pasażerów nadal mają rutynowy obowiązek odfiltrowania danych szczególnie chronionych przesyłanych przez linie lotnicze, czy powinny tak postępować wyłącznie w wyjątkowych sytuacjach, w których linie lotnicze przesyłały takie dane przez pomyłkę. EIOD zaleca zmianę tekstu w celu wyraźnego stwierdzenia, że linie lotnicze nie powinny przysyłać żadnych danych szczególnie chronionych u samego źródła przetwarzania danych.
47. Z wyjątkiem danych szczególnie chronionych, wykaz danych, które można przekazywać, w dużej mierze odzwierciedla wykaz danych US PNR, który w wielu

opiniach Grupy Roboczej Art. 29<sup>(1)</sup> skrytykowany jako zbyt obszerny. EIOD uważa, że wykaz ten należy ograniczyć zgodnie z opinią grupy roboczej oraz że każdą dodaną pozycję należy należycie uzasadnić. Dotyczy to w szczególności pola „ogólne uwagi”, które należy wyłączyć z wykazu.

### III.7. Zautomatyzowane decyzje indywidualne

48. Zgodnie z art. 4 ust. 2 lit. a) i b) ocena na podstawie wcześniej ustalonych kryteriów lub porównania z innymi właściwymi bazami danych może wiązać się z automatycznym przetwarzaniem, jednak taką ocenę należy indywidualnie analizować w sposób niezautomatyzowany.
49. EIOD z zadowoleniem przyjmuje wyjaśnienia wprowadzone do tej nowej wersji tekstu. Niejasność poprzedniego zakresu stosowania przepisu w związku z zautomatyzowanymi decyzjami wywierającymi „szkodliwy skutek prawny na daną osobę lub znacząco na nią wpływającymi [...]” zastąpiono jaśniej sprecyzowanym brzmieniem. Obecnie wiadomo, że wszystkie przypadki skojarzenia danych będą analizowane indywidualnie.
50. Z nowej wersji jasno wynika również, że ocena nie może w żadnych okolicznościach opierać się na pochodzeniu rasowym lub etnicznym osób, ich wierzeniach religijnych lub filozoficznych, poglądach politycznych, przynależności do związków zawodowych albo zdrowiu lub życiu seksualnym. Innymi słowy, zgodnie z rozumieniem EIOD tego nowego brzmienia, żadna decyzja nie może zostać podjęta nawet częściowo na podstawie danych szczególnie chronionych. Jest to zgodne z przepisem, zgodnie z którym żadne dane szczególnie chronione nie mogą być przetwarzane przez biura danych pasażerów, i również przyjmuje się to z zadowoleniem.

### III.8. Przegląd i dane statystyczne

51. EIOD uważa, że sprawą najwyższej wagi jest przeprowadzenie szczegółowej oceny wdrożenia dyrektywy, jak przewidziano w art. 17. Uważa, że w ramach przeglądu należy ocenić nie tylko ogólną zgodność ze standardami ochrony danych, ale bardziej konkretnie i szczegółowo kwestię, czy systemy PNR stanowią konieczny środek. Z tego punktu widzenia ważną rolę odgrywają dane statystyczne, o których mowa w art. 18. EIOD uważa, że dane te powinny obejmować liczbę działań podejmowanych przez organy ścigania, jak przewidziano w projekcie, lecz również liczbę wyroków skazujących, które zapadły w wyniku – lub nie – tych działań organów ścigania. Tego rodzaju dane są niezbędne do uzyskania rozstrzygających wyników przeglądu.

### III.9. Stosunek do innych instrumentów prawnych

52. Przedmiotowy wniosek obowiązuje bez uszczerbku dla umów z państwami trzecimi (art. 19). EIOD uważa, że w tym przepisie należy wyraźniej odnieść się do docelowych globalnych ram zapewniających zharmonizowane

<sup>(1)</sup> Opinia z dnia 23 czerwca 2003 r. w sprawie poziomu ochrony zapewnianej w Stanach Zjednoczonych przy przekazywaniu danych pasażerów, WP78. Ta opinia grupy roboczej i kolejne dotyczące tej kwestii są dostępne na stronie internetowej: [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/index\\_en.htm#data\\_transfers](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers)



zabezpieczenia w zakresie ochrony danych w dziedzinie PNR w UE i poza nią, zgodnie z wnioskiem Parlamentu Europejskiego i opracowaniem Komisji w ramach komunikatu z dnia 21 września 2010 r. „w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim”.

53. W tym znaczeniu w umowach z państwami trzecimi nie należy zawierać postanowień, które nie odpowiadają poziomowi ochrony danych przewidzianemu w przedmiotowej dyrektywie. Ma to szczególne znaczenie obecnie w kontekście renegocjowanych umów ze Stanami Zjednoczonymi Ameryki, Australią i Kanadą w perspektywie globalnych – i zharmonizowanych – ram.

#### IV. WNIOSKI

54. Opracowanie systemu UE-PNR oraz negocjacje umów dotyczących PNR z państwami trzecimi stanowiły długo trwający projekt. EIOD przyznaje, że w porównaniu z wnioskiem dotyczącym decyzji ramowej Rady w sprawie UE-PNR z 2007 r. do przedmiotowego projektu wprowadzono widoczne ulepszenia. Korzystając z debat i opinii różnych zainteresowanych stron, w tym w szczególności Grupy Roboczej Art. 29, EIOD i Parlamentu Europejskiego, dodano zabezpieczenia w zakresie ochrony danych.

55. EIOD w zadowoleniu przyjmuje te ulepszenia, a w szczególności wysiłki służące ograniczeniu zakresu stosowania wniosku i wprowadzeniu bardziej restrykcyjnych warunków przetwarzania danych PNR. EIOD ma jednak obowiązek zwrócić uwagę, że we wniosku nie spełniono zasadniczego warunku opracowania systemu PNR – tj. zgodności z zasadami konieczności i proporcjonalności. EIOD przypomina, że jego zdaniem dane PNR mogą bez wątpienia być konieczne do celów egzekwowania prawa w szczególnych przypadkach i spełniać wymogi ochrony danych. Kwestią wzbudzającą szczególne obawy jest ich wykorzystywanie w systematyczny i masowy sposób w odniesieniu do wszystkich pasażerów.

56. W ocenie skutków zawarto elementy ukierunkowane na uzasadnienie konieczności danych PNR w walce z przestępczością, jednak informacje te są zbyt ogólne i nie stanowią argumentu na poparcie zakrojonego na szeroką skalę przetwarzania danych PNR do celów wywiadowczych. Zdaniem EIOD jedynym środkiem zgodnym z wymogami w zakresie ochrony danych byłoby stosowanie danych PNR w poszczególnych przypadkach, w których ustalono istnienie poważnego zagrożenia na podstawie konkretnych wskaźników.

57. Oprócz tego podstawowego niedociągnięcia, uwagi EIOD dotyczą następujących kwestii:

— zakres stosowania powinien być o wiele bardziej ograniczony w zależności od rodzaju zaistniałego przestępstwa; EIOD kwestionuje włączenie do wniosku poważnych przestępstw, które nie mają związku z terroryzmem. W każdym bądź razie lżejsze przestępstwa należy wyraźnie zdefiniować i wykluczyć. EIOD zaleca wyłączenie możliwości poszerzenia zakresu stosowania przez państwa członkowskie,

— nie zdefiniowano w wystarczający sposób charakteru różnych zagrożeń umożliwiających wymianę danych między biurami danych pasażerów lub państwami członkowskimi,

— mających zastosowanie zasad ochrony danych nie należy opierać wyłącznie na decyzji ramowej Rady 2008/977/WSiSW, która zawiera niedociągnięcia, w szczególności pod względem praw osób, których dane dotyczą, i przekazywania danych państwom trzecim. We wniosku należy opracować wyższy poziom zabezpieczeń w oparciu o zasady zawarte w dyrektywie 95/46/WE,

— żadnych danych nie należy zatrzymywać w identyfikowalnej formie na okres dłuższy niż 30 dni, z wyjątkiem przypadków uzasadniających prowadzenie dalszego dochodzenia,

— należy ograniczyć wykaz przetwarzanych danych PNR zgodnie z wcześniejszymi zaleceniami Grupy Roboczej Art. 29 i EIOD. W szczególności nie należy dołączać pola „ogólne uwagi”,

— ocenę dyrektywy należy przeprowadzić w oparciu o kompleksowe dane, w tym liczbę osób skazanych – a nie wyłącznie osób ściganych – na podstawie przetwarzania ich danych.

58. EIOD zaleca również przeprowadzenie oceny rozwoju sytuacji w zakresie UE-PNR w szerszej perspektywie obejmującej trwającą obecnie ogólną ocenę wszystkich instrumentów UE w dziedzinie zarządzania wymianą informacji rozpoczętą przez Komisję w styczniu 2010 r. W szczególności przy ocenie konieczności systemu UE-PNR należy uwzględnić wyniki obecnych prac nad europejskim modelem wymiany informacji, których należy oczekiwać w 2012 r.

Sporządzono w Brukseli dnia 25 marca 2011 r.

Peter HUSTINX  
Europejski Inspektor Ochrony Danych