



00664/11/PL
WP 181

**Opinia 10/2011 odnosząca się do 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**

Przyjęta dnia 5 kwietnia 2011 r.

Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określa art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 06/036.

Strona internetowa: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 ust. 1 lit. a) i ust. 3 wspomnianej dyrektywy, a także art. 15 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r., uwzględniając swój regulamin,

przyjmuje następującą opinię:

1. Wprowadzenie

Dnia 2 lutego 2011 r. Komisja Europejska opublikowała wniosek dotyczący 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. Grupa robocza przedstawiła opinię odnoszącą się do poprzedniego wniosku w sprawie wykorzystania danych PNR w UE (wniosek dotyczący decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa), przedstawionego przez Komisję dnia 6 listopada 2007r.¹ Ponadto wcześniej grupa robocza w kilku opiniach przedstawiła obszernie komentarze dotyczące różnych porozumień w sprawie danych PNR, obowiązujących między UE a państwami trzecimi, a także dotyczące podejścia Komisji przedstawionego w komunikacie z dnia 21 września 2010 r.² Poza tym grupa robocza powtórzyła swoje obawy odnoszące się do danych PNR w różnych pismach do komisarza Barrota, komisarz Malmström, dyrektora generalnego Faulla oraz komisji LIBE Parlamentu Europejskiego.

Niniejsza opinia jest skierowana do stron zaangażowanych w rozmowy dotyczące najnowszego wniosku i w jego rozwój, a zatem do Komisji, grupy roboczej Rady GENVAL i Parlamentu Europejskiego.

2. Konieczność i proporcjonalność

Wnioskowi z 2011 r. towarzyszy ocena skutków, mająca na celu bardziej szczegółową prezentację uzasadnienia wniosku oraz jego przepisów. Grupa robocza uważa, że zwalczanie terroryzmu i przestępczości zorganizowanej jest konieczne i uzasadnione, a dane osobowe, w szczególności niektóre dane pasażerów, mogą być cenne pod względem oceny ryzyka, a także zapobiegania terroryzmowi i zorganizowanej przestępczości oraz walki z nimi. W przypadku europejskiego systemu wykorzystania danych PNR ograniczenie podstawowych praw i wolności musi być jednakże dobrze umotywowane, a jego konieczność jasno wykazana, w sposób umożliwiający osiągnięcie odpowiedniej równowagi między potrzebą ochrony bezpieczeństwa publicznego a ograniczeniem prawa do prywatności.

Grupa robocza konsekwentnie kwestionowała konieczność i zasadność systemów wykorzystania danych PNR i zajmuje takie samo stanowisko w odniesieniu do wniosku z 2011 r. Doceniamy wprowadzenie dodatkowych szczegółów przedstawione w ocenie skutków, uważamy jednak, że nie stanowi ona właściwej oceny wykorzystania danych PNR i nie

¹ WP 145 – wspólna opinia z Grupą Roboczą ds. Współpracy Policyjnej i Sądowej.

² Opinie WP 103 (Kanada), WP 138 (USA), WP 151 (USA – informacja dla pasażerów) oraz WP 178 (globalne podejście Komisji).

wykazuje konieczności podjęcia proponowanych środków. Wniosek powinien jasno określać, czy celem jest walka z poważną (międzynarodową) przestępczością, obejmującą terroryzm, czy też celem jest tylko zwalczanie terroryzmu i przestępstw z nim powiązanych.

W rozdziale 3.2 oceny skutków („Kwestie praw podstawowych”) stwierdza się załedwie, że zastosowano listę kontrolną praw podstawowych, brakuje jednak dalszych informacji uzasadniających wyciągnięte wnioski. Ponadto wspomniany rozdział zawiera rozumowanie mające charakter błędnego koła, odnoszące się do ograniczenia prawa do prywatności na mocy art. 8 europejskiej konwencji praw człowieka oraz art. 7 i 8 Karty praw podstawowych Unii Europejskiej. Wstępnym warunkiem prawnym ograniczenia tego prawa jest jego „konieczność z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób”, a ponadto musi być ono „konieczne w demokratycznym społeczeństwie” oraz dokonywane „z zastrzeżeniem zasady proporcjonalności”. Fakt, że celem wniosku jest zapobieganie terroryzmowi i poważnej przestępczości nie oznacza, że wniosek jest w sposób oczywisty zgodny ze wspomnianymi wymogami; nadal należy wykazać konieczność i proporcjonalność. We własnym przeglądzie systemów zarządzania informacjami³ Komisja stwierdza:

„Konieczność

Ingerencja władzy publicznej w korzystanie z prawa do prywatności przysługującego każdej osobie fizycznej może być niezbędna z uwagi na bezpieczeństwo narodowe, bezpieczeństwo publiczne lub zapobieganie przestępstwom. Orzecznictwo Europejskiego Trybunału Praw Człowieka ustanawia trzy warunki, na mocy których wspomniane ograniczenia mogą być usprawiedliwione: ingerencja musi być przewidziana przez ustawę, służyć osiągnięciu zgodnego z prawem celu i musi być konieczna w demokratycznym społeczeństwie. Ingerencję w prawo do prywatności uważa się za konieczną, jeśli jest ona uzasadniona pilną potrzebą społeczną, jest proporcjonalna do wyznaczonego celu oraz jeśli przyczyny podane przez władzę publiczną dla jej uzasadnienia są odpowiednie i wystarczające. W kolejnych wnioskach dotyczących polityki realizowanej w tym zakresie Komisja oceni spodziewany wpływ inicjatywy na prawo do prywatności i ochrony danych osobowych osób fizycznych, a także określi, dlaczego wpływ ten jest konieczny i dlaczego proponowane rozwiązanie jest proporcjonalne do zgodnego z prawem celu utrzymania bezpieczeństwa wewnętrznego w Unii Europejskiej, zapobiegania przestępstwom lub zarządzania migracjami.”

Grupa robocza uważa, że Komisja nie wywiązała się z powyższych zobowiązań w odniesieniu do wniosku w sprawie wykorzystania danych PNR w UE. Argumenty dotyczące konieczności i proporcjonalności mają jeszcze wiele innych aspektów, które również omówiono poniżej.

2.1. Poprawa bezpieczeństwa

We wniosku i w ocenie wpływu stwierdza się, że system wykorzystania danych PNR w UE zapewniałby bezpieczeństwo oraz pozwoliłby uniknąć luk wynikających ze zniesienia wewnętrznych kontroli granicznych na podstawie konwencji z Schengen. Ten cel byłby zgodny z prawem, gdyby był właściwie uzasadniony, jednakże grupie roboczej nie przedstawiono jeszcze żadnych przekonujących dowodów wskazujących na to, że

³ Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, COM(2010)385 wersja ostateczna.

przetwarzanie danych PNR we wszystkich państwach członkowskich pozwalałoby na uniknięcie luk w systemie bezpieczeństwa wynikających z przetwarzania danych w tylko kilku państwach członkowskich.

Na poziomie UE istnieją już systemy i narzędzia kompensujące zniesienie kontroli granicznych między państwami strefy Schengen, bazujące na tzw. dorobku Schengen, zatem jeśli nadal istnieją luki w systemie bezpieczeństwa, pierwszym krokiem powinno być przeanalizowanie prawidłowego funkcjonowania istniejących systemów.

2.2. Istniejące systemy, narzędzia i współpraca

Przedstawiony przez Komisję przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości nie obejmował oceny skuteczności różnych istniejących systemów, nie wzięto również pod uwagę, czy razem zapewniają one właściwe narzędzia zwalczania terroryzmu i zorganizowanej przestępczości, a jeśli nie, to gdzie mogą występować luki. Grupa robocza uważa, że taka ocena jest niezbędna przed wprowadzeniem kolejnych, podobnych środków, takich jak system wykorzystania danych PNR w UE. Przyjęcie wniosku dotyczącego PNR spowoduje nałożenie na przewoźników dublujących się obowiązków i gromadzenie danych dostępnych już w innych systemach, a także stwarza poważne zagrożenie rozrostem funkcji. Przykładowo, postanowienia dyrektywy API zobowiązują przewoźników do przekazywania takich danych z wyprzedzeniem, a wykorzystanie takich danych nie jest ograniczone do kontroli granicznych, mogą one bowiem zostać również użyte do celów działań w zakresie egzekwowania prawa. Pomimo kilkukrotnego zwrócenia uwagi Komisji na tę kwestię, grupa robocza nie miała jeszcze możliwości zapoznania się z właściwą oceną skuteczności wspomnianej dyrektywy oraz jej wdrożenia na poziomie krajowym, a ponadto kwestionuje dalszą potrzebę jej stosowania w przypadku wprowadzenia ogólnounijnego systemu wykorzystania danych PNR.

Grupa robocza podaje w wątpliwość, czy wszystkie formy współpracy policyjnej i sądowej stosowane w UE, mające na celu zapobieganie przestępstwom i ściganie ich, obejmujące zwalczanie terroryzmu i poważnej przestępczości, stanowią adekwatne narzędzia do celu, któremu ma służyć wniosek w sprawie wykorzystania danych PNR w UE. Ocena skutków nie zawiera takiej analizy.

Grupa robocza przyjmuje do wiadomości fakt, że część państw członkowskich nienależących do strefy Schengen nie może korzystać z niektórych z wprowadzonych narzędzi i systemów, w związku z czym w odniesieniu do takich państw konieczne może być zastosowanie kryterium konieczności. Takie państwa członkowskie mogą jednak stosować i stosują dyrektywę API, należy zatem rozważyć, czy lepsze wykorzystanie istniejących systemów oraz usprawnienie współpracy między tymi a innymi państwami członkowskimi nie mogłoby w rzeczywistości zapewnić wszystkich potrzebnych informacji do odnośnych celów. Ponadto, co należy zaznaczyć, fakt, że dane PNR byłyby wykorzystywane jako narzędzie wywiadu, jak wspomniano w ocenie skutków, dodatkowo podnosi poziom wymogów w odniesieniu do gwarancji ochrony danych.

2.3. Proporcjonalność

Zgodnie z wnioskiem gromadzona będzie ogromna ilość danych osobowych wszystkich pasażerów przylatujących do UE i wylatujących z niej, bez względu na to, czy są to osoby podejrzane, czy nie. Gromadzenie i przetwarzanie danych PNR do celów zwalczania

terroryzmu i poważnej przestępczości nie powinno umożliwiać masowego śledzenia wszystkich podróżnych ani nadzoru nad nimi. Grupa robocza uważa gromadzenie i zatrzymywanie wszystkich danych wszystkich podróżnych z wszystkich lotów za nieproporcjonalne, a zatem niezgodne z art. 8 Karty praw podstawowych. Jak już wspomniano powyżej, ocena skutków nie zawiera pod tym względem przekonujących dowodów. Wnioski przedstawiane na poziomie UE powinny być szczegółowe i ukierunkowane na rozwiązanie konkretnego problemu, a w tym kontekście każdy wniosek powinien się skupiać na ryzyku związanym z terroryzmem i poważną przestępczością.

Grupa robocza wyraża poważne wątpliwości w odniesieniu do proporcjonalności systematycznej weryfikacji wszystkich pasażerów na podstawie ustalonych wcześniej kryteriów i nieokreślonych „właściwych baz danych”. Nie jest jasne, jak takie ustalone wcześniej kryteria i właściwe bazy danych mają być zdefiniowane, czy dane PNR będą wykorzystywane do określania lub aktualizacji takich kryteriów, a także w jakim zakresie wszyscy wytypowani podróżni będą automatycznie podlegać dodatkowym dochodzeniom. Grupa robocza pragnie także przypomnieć, że w niektórych państwach członkowskich podobne metody nadzoru są konstytucyjne, a zatem dostępne organom policyjnym, tylko z zastrzeżeniem zgody sądu oraz w określonych okolicznościach, takich jak szczególne zagrożenie. W proponowanym systemie wykorzystania danych PNR ta wyjątkowa metoda stałaby się zwykłym instrumentem pracy policyjnej.

Wprowadzone środki, które nie mogą zapewnić ochrony praw i wolności podróżnych, są proporcjonalne tylko wówczas, gdy stosuje się je tymczasowo w przypadku szczególnego zagrożenia, co nie ma miejsca w przypadku przedmiotowego wniosku. Naruszenie prywatności podróżnych musi być proporcjonalne do korzyści pod względem zwalczania terroryzmu i poważnej przestępczości. Grupie roboczej nie przedstawiono jeszcze żadnych danych statystycznych, z których wynikałoby, jaki jest współczynnik liczby niewinnych podróżnych, których dane PNR zgromadzono, do skali efektów w zakresie egzekwowania prawa osiągniętych dzięki gromadzeniu takich danych PNR.

Podsumowując, grupa robocza nadal uważa, że nie wykazano konieczności wprowadzenia systemu oraz że proponowane środki nie są zgodne z zasadą proporcjonalności. Pomimo tego grupa robocza uważa za wskazane skomentowanie również innych aspektów proponowanej dyrektywy, wymienionych poniżej.

3. Cele

Proponowana dyrektywa określa dwa ogólne cele przetwarzania i cztery szczegółowe działania. Dane PNR można przetwarzać tylko do celów:

- zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania poprzez ocenę pasażerów przed przylotem lub odlotem w drodze porównania ich danych PNR z właściwymi bazami danych (cel 1, działanie 1) i poprzez udzielanie odpowiedzi na wnioski właściwych organów w określonych przypadkach (cel 1, działanie 2); oraz
- zapobiegania przestępstwom terrorystycznym i poważnej przestępczości międzynarodowej, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania poprzez ocenę pasażerów przed przylotem lub odlotem w odniesieniu do właściwych baz danych (cel 2, działanie 3) i poprzez analizowanie danych PNR w celu aktualizowania lub ustanawiania nowych kryteriów (cel 2, działanie 4).

Nie jest jasne, co te cele oznaczają w praktyce. Cel 1, działanie 1 wydaje się oznaczać weryfikację w odniesieniu do list zagrożeń, SIS lub innych baz danych na poziomie UE i krajowym. Cel 1, działanie 2 wydaje się oznaczać wymianę informacji w indywidualnych przypadkach, na odpowiedni wniosek. Cel 2, działanie 3 wydaje się oznaczać porównywanie danych PNR z profilami poszczególnych rodzajów przestępczości, a z kolei cel 2, działanie 4 wydaje się oznaczać użycie danych PNR do tworzenia takich profili.

Podstawową zasadą ochrony danych jest ściśle definiowane celów i działań. Dokładniej zdefiniowane powinny być również „właściwe bazy danych”, być może także przez dodanie ich do listy właściwych organów, którą każde państwo członkowskie byłoby zobowiązane przedstawić Komisji. W każdym razie powinny to być bazy utworzone do tych samych celów, tj. zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania. Ponadto przepisy wykonawcze muszą jasno określać ograniczenia w wykorzystaniu takich baz danych. Grupa robocza przypomina również, że ważne jest dopilnowanie, aby wszelkie kryteria oceny stosowane przez państwa członkowskie w analizie danych były szczegółowe, konieczne, uzasadnione i aby regularnie podlegały przeglądowi.

3.1. Definicje

We wniosku „przestępstwa terrorystyczne” definiuje się jako przestępstwa przewidziane w prawie krajowym, o których mowa w art. 1–4 decyzji ramowej 2002/475/WSiSW. „Poważną przestępczość” i „poważną przestępczość międzynarodową” definiuje się jako przestępstwa przewidziane w prawie krajowym, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW. Grupa robocza podkreśla znaczenie konkretnych definicji w tej dziedzinie, jednakże definicja poważnej przestępczości jest dosyć obszerna, kwestionujemy zatem konieczność i proporcjonalność wykorzystania danych PNR w odniesieniu do niektórych z tych przestępstw.

W odniesieniu do tej kwestii, w motywie 12 wniosku stwierdza się, że państwa członkowskie mogą wykluczyć lżejsze przestępstwa, jeśli nie jest to sprzeczne z zasadą proporcjonalności, jednak wybór pozostawia się każdemu z państw członkowskich. Może to doprowadzić do sytuacji, w której przestępstwa są uwzględnione w jednym państwie członkowskim, a w innym nie. Nie jest jasne, kto podejmuje decyzję dotyczącą proporcjonalności i czy taka decyzja ma być zgłaszana Komisji, która mogłaby odegrać rolę w zakresie zapewnienia spójności oraz prawidłowego zastosowania zasady proporcjonalności.

Obawy grupy roboczej odnoszące się do potencjalnie szerokiego zakresu definicji poważnej przestępczości odnoszą się również do zawartych we wniosku przepisów w sprawie wymiany danych z innymi organami, zarówno w UE, jak i poza nią.

4. Zatrzymywanie danych

Proponowane okresy zatrzymywania są wyraźnie skrócone w porównaniu z poprzednim wnioskiem i różnymi porozumieniami w sprawie danych PNR na poziomie UE. Grupa robocza uważa jednak, że propozycja zatrzymywania danych, nawet zamaskowanych, przez pięć lat jest nieproporcjonalna. Od zawsze systemom wykorzystywania danych PNR towarzyszą obawy związane z faktem, że wszystkie dane wszystkich podróżnych zatrzymuje się na taki sam czas oraz że taki okres zatrzymywania sam w sobie jest nieproporcjonalny.

Grupie roboczej nie przedstawiono przekonujących dowodów, że konieczne jest zatrzymywanie danych wszystkich podróżnych i że takie dane muszą być zatrzymywane na pięć lat.

4.1. Maskowanie danych

We wniosku stwierdza się wprawdzie, że dane będą maskowane po 30 dniach i, zasadniczo, dostępne tylko dla niektórych członków personelu biura danych pasażerów, których rola polega na tworzeniu profili i wzorców w zakresie tras podróży, jednak pełny dostęp do wszystkich danych pozostawałby możliwy przez cały okres zatrzymywania. Mimo że maskowanie służy minimalizacji danych i kontroli dostępu, które są ważnymi zasadami ochrony danych, grupa robocza nadal kwestionuje konieczność posiadania wszystkich danych o wszystkich podróżnych, a także uważa, że dane podróżnych, którzy nie są podejrzani, powinny być usuwane.

Jeśli prawodawca zdecyduje się na zatrzymywanie danych przez ograniczony czas, dane powinny być chronione w sposób zapobiegający ujawnieniu informacji umożliwiających identyfikację. Taka ochrona powinna być zapewniana nie później niż w chwili przylotu. Dostęp do danych chronionych mający na celu pozyskanie informacji umożliwiających identyfikację powinien być uzależniony od decyzji sądu wydawanych w trybie indywidualnym do celów poszczególnych dochodzeń.

Grupa robocza pragnie także zdecydowanie podkreślić potrzebę użycia precyzyjnego języka, który nie prowadzi do pomyłek i nie wprowadza w błąd. We wniosku wspomina się zarówno o maskowaniu, jak i o anonimizacji. Nie jest to ten sam proces i jest oczywiste, że chodzi o maskowanie, nie o anonimizację, gdyż nadal można z łatwością pozyskać dane umożliwiające identyfikację osoby, której dane dotyczą. Wniosek nie powinien celowo ani w inny sposób prowadzić do pomyłek, a także nie powinien wprowadzać w błąd ani zawierać obietnic niemożliwych do spełnienia.

5. Prawo osób fizycznych do ochrony danych

Wniosek zawiera przepisy odnoszące się konkretnie do ochrony danych. Grupa robocza uważa za konieczne, aby każdy wniosek przedstawiany na poziomie UE, wpływający na prawa i wolności osób fizycznych, zawierał przepisy dotyczące prawa osób fizycznych do wglądu do swoich danych, do ich poprawienia, do odszkodowania i do sądowych środków ochrony prawnej. Jednakże prawa określone w przedmiotowym wniosku to prawa określone w decyzji ramowej 2008/977/WSiSW, nie w dyrektywie 95/46/WE. W rezultacie są to prawa bardziej ograniczone. Nie jest jasne, czy prawa mają zastosowanie tylko do danych przekazywanych innemu organowi, czy też dotyczą danych znajdujących się w posiadaniu organu krajowego. W niektórych państwach członkowskich wykorzystujących obecnie dane PNR, osobom fizycznym przysługuje prawo do wglądu w swoje dane, do poprawienia ich i do sądowych środków ochrony prawnej na mocy przepisów krajowych transponujących dyrektywę 95/46; w przypadku wejścia w życie dyrektywy w sprawie danych PNR wspomniane prawa zostaną ograniczone.

Istnieje również ryzyko dyskryminacji w wyniku tworzenia profili, gdyż omawiany system jest ukierunkowany na pasażerów linii lotniczych jako na grupę. Pasażerom nie przekazuje się żadnych informacji o kryteriach, według których są oceniani, co wpływa na korzystanie z przysługujących im praw przez osoby, których bezpośrednio dotyczy tworzenie profili.

Grupa robocza przypomina o znaczeniu uwzględnienia w przedstawianych na poziomie UE wnioskach, mających wpływ na prawa i wolności osób fizycznych, odpowiednich środków ochrony danych i zabezpieczeń, takich jak zasady poufności i bezpiecznego przetwarzania danych, obowiązki informowania osób fizycznych, zakaz przekazywania danych podmiotom prywatnym, a także zwraca uwagę, że decyzje nie powinny być podejmowane wyłącznie na podstawie zautomatyzowanego przetwarzania. Grupa robocza podkreśla także znaczenie uwzględnienia krajowych organów nadzorczych, odgrywających na poziomie krajowym rolę w zakresie transpozycji przepisów przyjętych na poziomie UE.

W odniesieniu do danych szczególnie chronionych we wniosku stwierdza się, że filtrowaniem i usuwaniem takich danych powinno się zajmować biuro danych pasażerów. W swoich opiniach dotyczących różnych porozumień w sprawie danych PNR zawieranych przez UE z państwami trzecimi grupa robocza zawsze popierała zakaz przetwarzania danych szczególnie chronionych w tym kontekście i zdecydowanie powtarza swój od dawna wyrażany pogląd, że filtrowanie powinien przeprowadzać przewoźnik przed przekazaniem danych organowi odbierającemu.

Grupa robocza podkreśla znaczenie dopilnowania, aby we wnioskach przedstawianych na poziomie UE, wpływających na prawa i wolności osób fizycznych, uwzględniano wymogi w zakresie monitorowania i przeglądu, w tym dotyczące rejestrowania wniosków o przetworzenie i o dane, w celu umożliwienia weryfikacji zgodności przetwarzania z prawem, monitorowania własnej działalności oraz zapewnienia odpowiedniej integralności i bezpieczeństwa danych przez krajowe organy ochrony danych. Ważne jest jednak zrozumienie, jak takie systemy będą działać w praktyce i w jaki sposób skuteczne rejestrowanie i dokumentacja będą zgodne ze wspomnianą powyżej zasadą minimalizacji danych.

6. Elementy danych

W przeciwieństwie do danych pasażera przekazywanych przed podróżą, dane PNR nie są weryfikowane, w związku z czym odznaczają się mniejszą wiarygodnością. Elementy danych wyszczególnione w załączniku do przedmiotowego wniosku są takie same, jak 19 elementów, które wymieniono w porozumieniach w sprawie danych PNR między UE a USA oraz między UE a Kanadą. Grupa robocza powtarza swoje stanowisko, że brakuje przekonujących dowodów wskazujących, które rubryki okazały się konieczne, a zatem taka lista jest nieproporcjonalna. Kategorie są ogólne i niektóre z nich obejmują dodatkowe podzbiory danych. Nawet przy zakazie przetwarzania szczególnie chronionych danych osobowych, lista elementów danych obejmuje rubrykę „uwagi ogólne”, w której można zamieścić wszelkie rodzaje informacji, takie jak zamówienia na posiłki, usługi specjalne itp. Grupie roboczej nie przedstawiono jeszcze przekonujących dowodów wskazujących, które elementy danych PNR okazały się skuteczne lub zostały z powodzeniem wykorzystane do celów egzekwowania prawa. Ponadto nie wszyscy przewoźnicy gromadzą dane PNR.

7. Właściwe organy i dalsze przekazywanie danych

We wniosku stwierdza się, że państwa członkowskie mają obowiązek przekazania Komisji listy właściwych organów w ciągu 12 miesięcy od wejścia dyrektywy w życie, a lista ta zostanie opublikowana w Dzienniku Urzędowym. Grupa robocza popiera środki w zakresie przejrzystości, zapewniające jasne określenie, kto jest uprawniony do odbioru i przetwarzania

danych. Jednakże role (administrator danych/przetwarzający) właściwych organów i biur danych pasażerów nie są precyzyjnie przedstawione.

Grupa robocza powtarza swoje obawy dotyczące szerokiej definicji poważnej przestępczości, w szczególności w odniesieniu do dalszego przekazywania danych, zarówno w UE, jak i poza nią.

8. Przegląd i wzajemność

Zgodnie z wnioskiem dyrektywa będzie podlegać przeglądowi co cztery lata od wejścia w życie. Specjalny przegląd odbędzie się w ciągu dwóch lat od wejścia dyrektywy w życie i będzie dotyczył rozszerzenia zakresu dyrektywy w celu objęcia nim lotów wewnętrznych w UE. Grupa robocza podkreśla potrzebę stosowania w procesie przeglądu ustawodawstwa UE jasnych kryteriów konieczności i skuteczności systemu. Ponadto grupa robocza ponownie zwraca uwagę na istotność włączenia krajowych organów ochrony danych do każdego przeglądu, zwłaszcza że przewidują to inne instrumenty na poziomie UE, takie jak porozumienia w sprawie danych PNR zawierane przez UE z państwami trzecimi.

W odniesieniu do przygotowania wniosków na poziomie UE, grupa robocza podkreśla znaczenie uwzględnienia konsekwencji potencjalnych wymogów w zakresie wzajemności. Europejski model wykorzystania danych PNR może skutkować wystąpieniem z podobnymi wymaganiami, na zasadzie wzajemności, przez kraje niedemokratyczne lub kraje niezapewniające wystarczającej ochrony podstawowych praw i wolności, w tym w zakresie danych osobowych i prywatności. Jest oczywiste, że osoby fizyczne mogą ponieść poważne konsekwencje w przypadku otrzymania przez takie kraje danych PNR z UE.

9. Wniosek

Grupa robocza uważa, że nie wykazano jeszcze konieczności wprowadzenia systemu wykorzystania danych PNR w UE oraz że proponowane środki nie są zgodne z zasadą proporcjonalności, w szczególności dlatego, że system przewiduje gromadzenie i zatrzymywanie wszystkich danych wszystkich podróżnych z wszystkich lotów. Grupa robocza wyraża również poważne wątpliwości w odniesieniu do proporcjonalności systematycznej weryfikacji wszystkich pasażerów na podstawie ustalonych wcześniej kryteriów.

Grupa robocza zaleca przeprowadzenie w pierwszej kolejności oceny istniejących systemów i metod współpracy oraz przeanalizowanie, jak współgrają one ze sobą w celu określenia luk w systemie bezpieczeństwa. W przypadku stwierdzenia luk, kolejnym krokiem powinno być rozpatrzenie, jaki jest najlepszy sposób ich eliminacji, co niekoniecznie oznacza wprowadzenie całego nowego systemu. Nadal można korzystać z istniejących mechanizmów i je doskonalić.

Jeśli proponowana dyrektywa wejdzie w życie, powinna zapewniać właściwe i adekwatne środki i zabezpieczenia w zakresie ochrony danych. Komisja powinna rozważyć, czy w efekcie można wycofać któreś z istniejących systemów, takie jak system określony dyrektywą API, w celu uniknięcia dublujących się środków.

Grupa robocza będzie nadal uważnie obserwować rozwój sytuacji i chętnie skorzysta z każdej okazji przedstawienia i dokładniejszego zaprezentowania swoich poglądów różnym stronom, których dotyczy przedmiotowy wniosek. Grupa robocza będzie również nadal wydawać opinie w sytuacjach, kiedy jest to właściwe i konieczne.

Sporządzono w Brukseli dnia
5 kwietnia 2011 r.

*W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM*