I

(Informacje)

RADA

List Departamentu Bezpieczeństwa Wewnętrznego (DHS) Stanów Zjednoczonych Ameryki adresowany do Prezydencji Rady i Komisji w sprawie interpretacji niektórych postanowień zobowiązań wydanych przez DHS w dniu 11 maja 2004 r. w związku z przekazywaniem przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) [1]

(2006/C 259/01)

„Celem niniejszego pisma jest przedstawienie naszego punktu widzenia w odniesieniu do interpretacji niektórych postanowień zawartych w zobowiązaniach w sprawie danych dotyczących przelotu pasażera (PNR) (*Passanger Name Record (PNR) Undertakings*) wydanych przez Departament Bezpieczeństwa Wewnętrznego (*Department of Homeland Security* — DHS) w dniu 11 maja 2004 r. Do celów niniejszego pisma skrót DHS oznacza Biuro Ceł i Ochrony Granic (*Bureau of Customs and Border Protection*), Służby Imigracyjne i Celne USA (*U.S. Immigration and Customs Enforcement*) oraz Biuro Sekretarza (*Office of the Secretary*) i jednostki bezpośrednio je wspierające, ale nie obejmuje innych części składowych DHS, takich jak Służby ds. Obywatelstwa i Imigracji (*Citizenship and Immigration Services*), Administracja Bezpieczeństwa Transportu (*Transportation Security Administration*), Tajne Służby Stanów Zjednoczonych (*United States Secret Service*), Straż Przybrzeżna Stanów Zjednoczonych (*United States Coast Guard*) oraz Federalna Agencja Zarządzania Kryzysowego (*Federal Emergency Management Agency*). Oczekujemy na dalszą analizę kwestii poruszanych w niniejszym piśmie, jak i innych kwestii podczas przyszłych dyskusji zmierzających do osiągnięcia kompleksowego, wzajemnego porozumienia opartego na wspólnych zasadach.

Wymiana i ujawnianie danych PNR

Zgodnie z ustawą o reformie służb wywiadowczych i zapobieganiu terroryzmowi (*Intelligence Reform and Terrorism Prevention Act*) z 2004 roku prezydent jest zobowiązany stworzyć mechanizm wymiany informacji »*that facilitates the sharing of terrorism information*.« W związku z powyższym dnia 25 października 2005 roku prezydent wydał rozporządzenie wykonawcze 13388 (*Executive Order 13388*) zobowiązujące DHS i inne agencje do »*promptly give access to terrorism information to the head of each other agency that has counterterrorism functions*« i tworzące procedury uruchomienia mechanizmu wymiany informacji.

Zgodnie z punktem 35 zobowiązań (w którym stwierdza się, że »Żadne stwierdzenie w niniejszych Zobowiązaniach nie utrudni wykorzystania lub ujawnienia danych zawartych w PNR w postępowaniach karnych oraz w innych przypadkach wymaganych przez prawo« oraz zezwala się DHS na »[doradzanie] Komisji w sprawie prawodawstwa Stanów Zjednoczonych, które wpływa co do meritum na niniejsze Zobowiązania«) Stany Zjednoczone poinformowały UE, że zawarte w zobowiązaniach postanowienia — w tym zwłaszcza w punktach (w całości lub części) 17, 28, 29, 30, 31 i 32 — które ograniczają wymianę informacji między agencjami USA, mogą uniemożliwić uruchomienie mechanizmu wymiany informacji przewidzianego w przywołanej powyżej ustawie i rozporządzeniu wykonawczym.

W świetle powyższego i zgodnie z tokiem rozumowania w dalszej części niniejszego pisma zobowiązania powinny być interpretowane i stosowane w sposób, który nie utrudni wymiany danych PNR między DHS i innymi organami rządu USA odpowiedzialnymi za zapobieganie terroryzmowi i związanym z nim przestępstwom lub za ich zwalczanie, o czym mowa w punkcie 3 zobowiązań.

---

[1] Decyzja Rady i umowa PNR, patrz Dz.U. L 298 z 27.10.2006.

DHS pomoże zatem w uproszczeniu procedury ujawniania (przy czym uproszczenie to nie zakłada nieograniczonego bezpośredniego dostępu elektronicznego) danych PNR organom rządu USA wykonującym zadania związane ze zwalczaniem terroryzmu i potrzebującym danych PNR w celu zapobiegania terroryzmowi i związanym z nim przestępstwom lub walki z nimi (w tym danych dotyczących zagrożeń, przelotów, osób fizycznych i określonych tras przelotu) podczas badania spraw lub prowadzenia śledztw. DHS będzie czuwać nad tym, by wspomniane organy przestrzegały norm ochrony danych porównywalnych z normami obowiązującymi w DHS, zwłaszcza w odniesieniu do zasady ograniczenia celu, zatrzymywania danych, dalszego ujawniania danych, pogłębiania wiedzy i szkoleń, norm bezpieczeństwa i sankcji za naruszenia oraz postępowania dotyczącego uzyskiwania informacji, wnoszenia skarg i dokonywania sprostowań. Przed rozpoczęciem procedury ujawniania w trybie uproszczonym każdy organ występujący o takie ujawnienie przedstawia DHS pisemne potwierdzenie, że przestrzega powyższych norm. Przed wygaśnięciem umowy DHS poinformuje UE w formie pisemnej o przypadkach zastosowania procedury ujawniania w trybie uproszczonym i o przestrzeganiu norm obowiązujących w takich przypadkach.

Wcześniejszy dostęp do danych PNR

Punkt 14 ogranicza liczbę przypadków pobierania danych PNR, natomiast nie przewiduje on ograniczeń tego rodzaju dla przesyłania danych do DHS. System opierający się na przesyłaniu danych uważany jest w opinii UE za mniej inwazyjny biorąc pod uwagę ochronę danych. Niemniej jednak system ten nie przewiduje, aby linie lotnicze miały możliwość podejmowania decyzji co do tego, jakie dane, kiedy i w jaki sposób należy przesłać. Zgodnie z prawem USA decyzja ta leży w kompetencji DHS. Przyjmuje się zatem, że DHS będzie korzystać z metody przesyłania niezbędnych danych PNR, która spełnia jego wymogi przeprowadzania skutecznej oceny ryzyka, uwzględniając skutki ekonomiczne dla przewoźników lotniczych.

Jeżeli chodzi o kwestię, kiedy ma nastąpić pierwsze przesłanie danych, DHS może uzyskać dane PNR wcześniej niż 72 godziny przez rozpoczęciem lotu, jeżeli jest to niezbędne ze względu na zwalczanie jednego z przestępstw wymienionych w punkcie 3. Co więcej, chociaż zdarzają się przypadki, w których rząd USA ma konkretne informacje na temat konkretnego zagrożenia, to w większości przypadków dostępne informacje wywiadowcze są bardziej ogólne i wymagają szerszego spektrum działania umożliwiającego określenie rodzaju zagrożenia i zidentyfikowania powiązanych osób. Przyjmuje się zatem, że punkt 14 zezwala na dostęp do danych PNR wcześniej niż 72 godziny przed rozpoczęciem lotu w przypadkach, w których istnieją podstawy do przypuszczenia, że wcześniejszy dostęp może pomóc w reagowaniu na konkretne zagrożenie dotyczące danego lotu, grupy lotów, trasy przelotu lub na inną sytuację związaną z przestępstwami opisanymi w punkcie 3 zobowiązań. Wykonując swoje uprawnienia, DHS będzie działać rozsądnie i adekwatnie do sytuacji.

Jak tylko będzie to możliwe, DHS przejdzie na system opierający się na przesyłaniu danych PNR zgodnie z zobowiązaniami i do końca roku 2006 przeprowadzi konieczne testy przynajmniej jednego z obecnie opracowywanych systemów, o ile projekt systemu, który ma być testowany, spełni wymogi techniczne DHS. Bez naruszenia zawartych zobowiązań i w celu uniknięcia określenia ewentualnych przyszłych wymogów systemu wszelkie filtry stosowane w systemie opartym na przesyłaniu danych oraz sam projekt systemu muszą pozwalać na przesyłanie do DHS potrzebnych danych PNR, zawartych w rezerwacjach lotniczych lub w systemach kontroli odlotów, w wyjątkowych sytuacjach, w których ujawnienie o rozszerzonym zakresie jest niezbędne do zneutralizowania zagrożenia dotyczącego żywotnych interesów osoby, której dane dotyczą, lub innych osób.

Zatrzymywanie danych

Dane PNR mają ważne zastosowanie, na przykład w identyfikacji potencjalnych terrorystów; nawet dane sprzed ponad 3,5 roku mogą mieć zasadnicze znaczenie dla znalezienia powiązań między osobami podejrzanymi o prowadzenie działalności terrorystycznej. Umowa wygaśnie przed upływem terminu, w którym, zgodnie z punktem 15, należy zniszczyć wszystkie dane; do kwestii czy i kiedy należy zniszczyć dane PNR zgromadzone zgodnie ze zobowiązaniami, Stany Zjednoczone i Unia Europejska powrócą podczas przyszłych dyskusji.

Wspólny przegląd

Zważywszy na przeprowadzoną we wrześniu 2005 roku szeroko zakrojoną wspólną analizę zobowiązań oraz na fakt, że umowa wygaśnie przed datą kolejnego wspólnego przeglądu, kwestia dotycząca zasadności i sposobu przeprowadzenia wspólnego przeglądu w roku 2007 zostanie poruszona podczas dyskusji dotyczących przyszłej umowy.

Dane

W rubryce dotyczącej osób często podróżujących mogą znajdować się takie dane jak adresy, numery telefoniczne, adresy poczty elektronicznej; dane te, jak również numer, jaki osoba często podróżująca posiada w ramach programu »*frequent flyer*«, mogą dostarczyć koronnego dowodu powiązań z terroryzmem. Podobnie informacje o liczbie przewożonych przez pasażera sztuk bagażu mogą mieć znaczenie w kontekście zwalczania terroryzmu. Zobowiązania zezwalają DHS na dodawanie kolejnych danych do 34 rodzajów danych wymienionych w załączniku A do zobowiązań, jeżeli dane te są niezbędne do osiągnięcia celów określonych w punkcie 3.

Niniejsze pismo stanowi formę konsultacji — przewidzianą w punkcie 7 — między USA a UE w związku z punktem 11 załącznika A dotyczącym wniosku DHS o uzyskanie numeru, jaki osoba często podróżująca posiada w ramach programu »*frequent flyer*«, jak również każdego rodzaju danych wymienionych w załączniku A do zobowiązań, o ile istnieje możliwość znalezienia danych tego rodzaju.

Ochrona żywotnych interesów osoby, której dane dotyczą lub innych osób

Uznając istotną rolę, jaką dane PNR mogą odegrać w przypadku wystąpienia chorób zakaźnych i pojawienia się innych zagrożeń dla pasażerów, DHS potwierdza raz jeszcze, że dostęp do takich informacji jest możliwy na podstawie punktu 34 — przewiduje on, że zobowiązania nie mogą utrudniać wykorzystania danych PNR w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innych osób lub uniemożliwiać bezpośredniego dostępu do danych PNR właściwym organom działającym zgodnie z celami określonymi w punkcie 3 zobowiązań. Pojęcie »żywotne interesy« obejmuje sytuacje, w których życie osób, których dane dotyczą, lub innych osób może być zagrożone i zakłada dostęp do informacji niezbędnych do zapewnienia, że osoby, które mogą być nosicielami niebezpiecznych chorób zakaźnych, lub osoby, które były narażone na kontakt z takimi chorobami, mogą być bez trudu zidentyfikowane, zlokalizowane oraz niezwłocznie poinformowane o zagrożeniu. Takie dane będą chronione w sposób adekwatny do ich rodzaju i wykorzystywane wyłącznie do celów, do których je udostępniono.

Z poważaniem,

Stewart BAKER

Assistant Secretary for Policy"