

II

(Akty, których publikacja nie jest obowiązkowa)

KOMISJA

DECYZJA KOMISJI

z dnia 14 maja 2004 r.

w sprawie odpowiedniej ochrony danych osobowych zawartych w *Passenger Name Record* (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych

(notyfikowana jako dokument nr K(2004) 1914)

(Tekst mający znaczenie dla EOG)

(2004/535/WE)

KOMISJA WSPÓLNOT EUROPEJSKICH,

elementów dotyczących przekazania i określonych w art. 25 ust. 2 wyżej wymienionej dyrektywy.

uwzględniając Traktat ustanawiający Wspólnotę Europejską,

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⁾, w szczególności jej art. 25 ust. 6,

a także mając na uwadze, co następuje:

- (1) Na mocy dyrektywy 95/46/WE Państwa Członkowskie są zobowiązane zapewnić, że przekazywanie danych osobowych do państwa trzeciego może odbywać się tylko wtedy, jeżeli dane państwo trzecie zapewnia odpowiedni poziom ochrony oraz jeżeli ustawodawstwo Państw Członkowskich wprowadzające w życie inne przepisy dyrektywy jest przestrzegane przed przekazaniem danych.
- (2) Komisja może stwierdzić, że państwo trzecie zapewnia odpowiedni poziom ochrony. W takim przypadku dane osobowe można przekazywać z Państw Członkowskich bez konieczności zapewniania dodatkowych gwarancji.
- (3) Na mocy dyrektywy 95/46/WE poziom ochrony danych należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji, zwracając szczególną uwagę na określoną liczbę

- (4) W ramach transportu lotniczego, PNR – „Zbiór informacji dotyczących podróży danego pasażera” [PNR – Passenger Name Record] jest zbiorem wymogów podróży każdego pasażera, zawierającym wszystkie niezbędne informacje umożliwiające przetwarzanie i kontrolowanie rezerwacji przez macierzyste i uczestniczące linie lotnicze. Dla celów niniejszej decyzji terminy „pasażer” i „pasażerowie” obejmują członków załogi. „Macierzysta linia lotnicza” oznacza linię lotniczą, w której pasażer dokonał pierwszej rezerwacji lub dodatkowej rezerwacji już po rozpoczęciu podróży. „Uczestnicząca linia lotnicza” oznacza linię lotniczą, do której rezerwująca linia lotnicza zwróciła się z prośbą o udostępnienie miejsca dla pasażera w trakcie jednego lub więcej lotów.
- (5) Biuro Celne i Ochrony Granic Stanów Zjednoczonych [the United States Bureau of Customs and Border Protection – CBP] Ministerstwa Bezpieczeństwa Wewnętrznego [Department of Homeland Security – DHS] wymaga od każdego przewoźnika obsługującego loty pasażerskie w zagranicznym ruchu powietrznym do lub ze Stanów Zjednoczonych zapewnienia elektronicznego dostępu do PNR w takim zakresie, w jakim PNR jest zebrany i zawarty w automatycznym systemie rezerwacji przewoźników lotniczych.
- (6) Wymagania przekazywania danych osobowych zawartych w PNR pasażerów lotniczych do CBP oparte są na ustawie uchwalonej przez Stany Zjednoczone w listopadzie 2001 r.⁽²⁾ oraz na przepisach wykonawczych przyjętych przez CBP na mocy wymienionej ustawy⁽³⁾.

⁽¹⁾ Dz.U. L 281 z 23.11.1995, str. 31; dyrektywa zmieniona rozporządzeniem (WE) nr 1882/2003 (Dz.U. L 284 z 31.10.2003, str. 1).

⁽²⁾ Title 49, United States Code, section 44909(c)(3).

⁽³⁾ Title 19, Code of Federal Regulations, section 122.49b.

- (7) Prawodawstwo Stanów Zjednoczonych, o którym mowa powyżej, dotyczy wzmocnienia bezpieczeństwa oraz warunków wjazdu do Stanów Zjednoczonych i wyjazdu z tego kraju – kwestie, podlegające suwerennej władzy Stanów Zjednoczonych w ramach ich jurysdykcji. Ponadto ustanowione wymogi nie są niezgodne z międzynarodowymi zobowiązaniami podjętymi przez Stany Zjednoczone. Stany Zjednoczone są krajem demokratycznym, opierającym się na zasadzie państwa prawnego oraz posiadającym silne tradycje swobód obywatelskich. Zasadność procesu stanowienia prawa oraz siła i niezależność wymiaru sprawiedliwości nie są kwestionowane. Wolność prasy stanowi kolejną silną gwarancję przeciwko naruszeniu swobód obywatelskich.
- (8) Wspólnota zobowiązuje się w pełni wspierać Stany Zjednoczone w walce z terroryzmem w granicach wyznaczonych prawem wspólnotowym. Prawo wspólnotowe przewiduje ustanowienie równowagi między wymogami bezpieczeństwa a ochroną prywatności. Na przykład, art. 13 dyrektywy 95/46/WE stanowi, że Państwa Członkowskie mogą przyjąć środki ustawodawcze w celu ograniczenia zakresu niektórych wymogów tej dyrektywy, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i ścigania przestępstw.
- (9) Przekazywanie danych, o którym mowa, dotyczy konkretnych służb kontrolnych, mianowicie linii lotniczych obsługujących przeloty między Wspólnotą a Stanami Zjednoczonymi, oraz tylko jednego odbiorcy w Stanach Zjednoczonych, mianowicie CBP.
- (10) Jakikolwiek ustalenie mające na celu zapewnienie ram prawnych dla przekazywania PNR do Stanów Zjednoczonych, w szczególności na podstawie niniejszej decyzji, powinno być ograniczone w czasie. Uzgodniono okres trzech i pół roku. W tym czasie okoliczności mogą ulec znaczącym zmianom i Wspólnota razem ze Stanami Zjednoczonymi uzgodnią, że niezbędny wówczas będzie przegląd ustaleń.
- (11) Przetwarzanie przez CBP przekazywanych mu danych osobowych zawartych w PNR pasażerów lotniczych regulują warunki określone w *Zobowiązaniach Ministerstwa Bezpieczeństwa Wewnętrznego Biura Celnego i Ochrony Granic (Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection) (CBP) z dnia 11 maja 2004 r. (zwanym dalej „Zobowiązaniem”)* oraz prawodawstwo Stanów Zjednoczonych w zakresie przewidzianym w *Zobowiązaniach*.
- (12) Jeżeli chodzi o prawodawstwo Stanów Zjednoczonych, Ustawa o Wolności Informacji [Freedom of Information Act – FOIA] ma zastosowanie w obecnej sytuacji, w zakresie w jakim reguluje warunki, na których CBP może sprzeciwiać się żądaniom o ujawnienie informacji i tym samym utrzymać PNR poufnym. Ustawa reguluje ponadto ujawnianie informacji zawartych w PNR osobom, których one dotyczą, ściśle związanych z prawem dostępu do danych, którym osoby te dysponują. FOIA stosuje się bez rozróżnienia w stosunku do obywateli Stanów Zjednoczonych i obywateli spoza Stanów Zjednoczonych.
- (13) W odniesieniu do Zobowiązań oraz zgodnie z tym, co przewiduje ich ust. 44, stwierdzenia zawarte w Zobowiązaniach będą lub już zostały włączone do ustaw, regulacji, wytycznych lub innych instrumentów polityki Stanów Zjednoczonych i posiadają zróżnicowany stopień skutków prawnych. Zobowiązania zostaną w całości opublikowane w Rejestrze Federalnym (Federal Register) na odpowiedzialność Ministerstwa Bezpieczeństwa Wewnętrznego (DHS). Jako takie, Zobowiązania stanowią poważne i przemyślane zobowiązanie polityczne ze strony DHS, a ich przestrzeganie będzie przedmiotem wspólnej kontroli dokonywanej przez Stany Zjednoczone oraz Wspólnotę. Brak zgodności, w danym przypadku, można zakwestionować drogą prawną, administracyjną i polityczną oraz, jeżeli się utrzymuje, może prowadzić do zawieszenia skutków niniejszej decyzji.
- (14) Normy, zgodnie z którymi CBP będzie przetwarzać zawarte w PNR dane osobowe pasażerów, na podstawie prawodawstwa Stanów Zjednoczonych oraz Zobowiązań, uwzględniają podstawowe zasady niezbędne dla zapewnienia odpowiedniego poziomu ochrony osób fizycznych.
- (15) Jeżeli chodzi o zasadę ograniczenia dla określonego celu, dane osobowe pasażerów lotniczych zawarte w PNR przekazywane do CBP będą przetwarzane w określonym celu, a następnie wykorzystane lub przekazane dalej, tylko jeżeli nie jest to niezgodne z celem przekazania danych. W szczególności dane zawarte w PNR będą wykorzystane wyłącznie do celów zapobiegania i zwalczania terroryzmu oraz związanych z nim przestępstw, innych poważnych przestępstw włącznie z przestępczością zorganizowaną, która z zasady ma charakter transnarodowy, oraz unikania kary aresztu lub więzienia za powyższe przestępstwa.
- (16) Jeżeli chodzi o zasadę jakości danych i proporcjonalności, którą należy uwzględnić w związku z zasadniczą podstawą interesu publicznego uzasadniającą przekazywanie danych zawartych w PNR, dane przekazane CBP nie będą następnie zmieniane przez CBP. Maksymalnie 34 kategorie danych zawartych w PNR będą przekazywane, a dodanie jakiegokolwiek nowej kategorii będzie wcześniej uzgadniane przez władzę Stanów Zjednoczonych z Komisją. Dodatkowe informacje osobowe postrzegane jako bezpośredni wynik danych zawartych w PNR będą uzyskiwane ze źródeł pozarządowych wyłącznie drogą prawną. Jako zasada ogólna, PNR będzie usuwany maksymalnie po okresie 3 lat i 6 miesięcy, z wyjątkiem danych udostępnionych na potrzeby szczególnych dochodzeń lub inaczej udostępnionych w trybie ręcznym.
- (17) Jeżeli chodzi o zasadę przejrzystości, CBP będzie udzielać podróżującym informacji na temat celu przekazywania i przetwarzania danych oraz tożsamości osoby dokonującej kontroli danych w kraju trzecim, oraz wszelkich innych informacji.

- (18) Jeżeli chodzi o zasadę bezpieczeństwa, CBP podejmuje techniczne i organizacyjne środki bezpieczeństwa na poziomie odpowiadającym ryzyku związanym z przetwarzaniem.
- (19) Prawo dostępu do danych i sprostowania uznaje się w granicach, w których dana osoba może zażądać kopii danych jej dotyczących zawartych w PNR oraz sprostowania błędnych danych. Przewidziane wyjątki są w dużej mierze porównywalne z ograniczeniami, które Państwa Członkowskie mogą nałożyć na mocy art. 13 dyrektywy 95/46/WE.
- (20) Dalsze przekazywanie danych dokonywane będzie, na zasadzie jednostkowych przypadków, do innych agencji rządowych, włącznie z zagranicznymi agencjami rządowymi odpowiedzialnymi za walkę z terroryzmem lub ściganie przestępstw, w celach odpowiadających tym ustanowionym w stwierdzeniu ograniczenia dla określonego celu. Przekazania danych będzie można także dokonać do celów ochrony podstawowych interesów osoby, której dane dotyczą lub innych osób, w szczególności w zakresie istotnego zagrożenia dla zdrowia, lub w ramach postępowań karnych oraz w innych przypadkach określonych przez prawo. Agencje otrzymujące informacje są zobowiązane, na mocy wyraźnie określonych warunków ujawniania, do wykorzystania danych wyłącznie do przewidzianych celów i nie mogą przekazać dalej tych danych bez zgody CBP. Żadna inna zagraniczna, federalna, stanowa czy lokalna agencja nie ma bezpośredniego dostępu elektronicznego do danych zawartych w PNR poprzez bazy danych CBP. CBP odmówi publicznego ujawnienia PNR na mocy wyłączeń przewidzianych przez właściwe przepisy FOIA.
- (21) CBP nie wykorzystuje danych szczególnie chronionych, jak określono w art. 8 dyrektywy 95/46/WE, a w oczekiwaniu na wprowadzenie systemu filtrów wyłączających takie dane z PNR przekazywanego do Stanów Zjednoczonych, CBP zobowiązuje się do wprowadzenia środków kasujących je oraz do niewykorzystywania ich w międzyczasie.
- (22) Jeżeli chodzi o mechanizmy mające na celu zapewnienie przestrzegania przez CBP wymienionych zasad, przewiduje się system szkolenia i informowania personelu CBP oraz sankcji dla poszczególnych pracowników. Główny Urzędnik ds. Prywatności (Chief Privacy Officer) w DHS, który jest urzędnikiem DHS, ale posiada jednocześnie szeroki zakres niezależności organizacyjnej i składa roczne sprawozdanie Kongresowi, odpowiedzialny jest za przestrzeganie przez CBP prywatności. Osoby, których dane zawarte w PNR zostały przekazane, mogą składać skargi do CBP, lub jeżeli kwestia pozostaje nierozstrzygnięta, do Głównego Urzędnika ds. Prywatności w DHS, bezpośrednio lub za pośrednictwem organów ochrony danych osobowych w Państwach Członkowskich. Urząd ds. Prywatności (Privacy Office) w DHS będzie rozpatrywać w trybie przyspieszonym skargi przekazane przez organy ochrony danych osobowych w Państwach Członkowskich w imieniu osób zamieszkujących we Wspólnocie, jeżeli osoba ta twierdzi, że jej skarga nie została rozpatrzona w zadowalający sposób przez CBP lub Urząd ds. Prywatności w DHS. Przestrzeganie zobowiązań będzie przedmiotem wspólnego rocznego przeglądu, dokonywanego przez CBP, w powiązaniu z DHS i grupą kierowaną przez Komisję.
- (23) W interesie przejrzystości i w celu zagwarantowania właściwym władzom w Państwach Członkowskich możliwości zapewnienia ochrony osób fizycznych odnośnie przetwarzania ich danych osobowych, należy wyszczególnić wyjątkowe okoliczności, w których zawieszenie przepływów danych może być usprawiedliwione, bez względu na to czy stwierdzono ich odpowiednią ochronę.
- (24) Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołana na mocy art. 29 dyrektywy 95/46/WE, wydała opinie w sprawie poziomu ochrony zapewnianego przez władze Stanów Zjednoczonych danym osobowym pasażerów, którymi Komisja kierowała się w trakcie negocjacji z DHS. Komisja wzięła pod uwagę wymienione opinie w trakcie przygotowywania niniejszej decyzji ⁽¹⁾.
- (25) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu utworzonego na mocy art. 31 ust. 1 dyrektywy 95/46/WE,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Dla celów art. 25 ust. 2 dyrektywy 95/46/WE Biuro Celne i Ochrony Granic Stanów Zjednoczonych (dalej zwane jako CBP) traktowane jest jako zapewniające odpowiedni poziom ochrony danych zawartych w PNR przekazywanych ze Wspólnoty na temat lotów do lub ze Stanów Zjednoczonych, zgodnie ze Zobowiązaniem określonymi w Załączniku.

Artykuł 2

Niniejsza decyzja dotyczy odpowiedniego poziomu ochrony zapewnianego przez CBP z punktu widzenia spełniania wymogów art. 25 ust. 1 dyrektywy 95/46/WE i nie wpływa na pozostałe warunki lub ograniczenia wprowadzające w życie pozostałe przepisy wymienionej dyrektywy, które mają zastosowanie do przetwarzania danych osobowych w Państwach Członkowskich.

⁽¹⁾ Opinia 6/2002 w sprawie przekazywania informacji na temat listy pasażerów i innych danych przez linie lotnicze Stanom Zjednoczonym, przyjęta przez grupę roboczą dn. 24 października 2002 r., dostępna na stronie internetowej w języku angielskim http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf
Opinia 4/2003 w sprawie poziomu ochrony zapewnianej przez Stany Zjednoczone przekazywaniu danych pasażerów, przyjęta przez grupę roboczą w dn. 13 czerwca 2003 r., dostępna na stronie internetowej w języku angielskim http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
Opinia 2/2004 w sprawie odpowiedniej ochrony danych osobowych zawartych w PNR pasażerów lotniczych do przekazania Biuru Celnemu i Ochrony Granic Stanów Zjednoczonych (CBP), przyjęta przez grupę roboczą w dn. 29 stycznia 2004 r., dostępna na stronie w języku angielskim http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

Artykuł 3

1. Bez uszczerbku dla uprawnień umożliwiających podjęcie działań w celu zagwarantowania przestrzegania przepisów krajowych przyjętych zgodnie z przepisami innymi niż zawarte w art. 25 dyrektywy 95/46/WE, właściwe władze Państw Członkowskich mogą wykonywać obecne uprawnienia w celu zawieszenia przepływu danych do CBP w celu ochrony osób fizycznych odnośnie do przetwarzania ich danych osobowych w jednym z poniższych przypadków:

- a) gdy właściwy organ Stanów Zjednoczonych ustalił, że CBP narusza obowiązujące normy ochrony; lub
- b) gdy istnieje wysokie prawdopodobieństwo, że normy ochrony określone w Załączniku są naruszane; gdy istnieją uzasadnione podstawy, aby domniemywać, iż CBP nie podejmuje, lub nie podejmie, odpowiednich i natychmiastowych kroków zmierzających do rozstrzygnięcia sprawy; gdy dalsze przekazywanie danych spowodowałoby realne niebezpieczeństwo wyrządzenia szkody osobom, których dotyczą dane osobowe, a właściwe organy w Państwie Członkowskim podjęły, odpowiednie w tych okolicznościach, wysiłki w celu dostarczenia CBP powiadomienia o powyższym oraz umożliwienia mu udzielenia odpowiedzi.

2. Zawieszenie ustaje, gdy tylko zapewnione zostaną normy ochrony, a właściwe organy danych Państw Członkowskich zostaną o tym powiadomione.

Artykuł 4

1. Państwa Członkowskie niezwłocznie informują Komisję środkami przyjętymi na mocy art. 3.
2. Państwa Członkowskie i Komisja informują się wzajemnie o każdej zmianie w normach ochrony oraz o przypadkach, w których działanie organów odpowiedzialnych za przestrzeganie przez CBP norm ochrony ustanowionych w Załączniku nie wystarcza do zapewnienia przestrzegania tych norm.

3. Jeżeli informacje zebrane zgodnie z art. 3 oraz zgodnie z ust. 1 i 2 niniejszego artykułu wykazują, że podstawowe zasady niezbędne do zapewnienia odpowiedniego poziomu ochrony osób fizycznych nie są już przestrzegane lub że jakikolwiek organ odpowiedzialny za przestrzeganie przez CBP norm ochrony ustanowionych w Załączniku nie spełnia swojej roli, CBP jest o tym informowane i, w razie potrzeby, stosuje się procedurę określoną w art. 31 ust. 2 dyrektywy 95/46/WE w celu uchylecia lub zawieszenia niniejszej decyzji.

Artykuł 5

Realizacja niniejszej decyzji zostanie oceniona, a wszelkie istotne informacje zostaną przekazane Komitetowi powołanemu na mocy art. 31 dyrektywy 95/46/WE, włącznie z dowodami, które mogłyby mieć wpływ na ocenę, dokonaną na mocy art. 1 niniejszej decyzji, odpowiedniego poziomu ochrony danych osobowych zawartych w PNR pasażerów lotniczych przekazywanych do CBP w rozumieniu art. 25 dyrektywy 95/46/WE.

Artykuł 6

Państwa Członkowskie podejmują wszelkie środki niezbędne w celu dostosowania się do niniejszej decyzji w terminie czterech miesięcy od dnia jej notyfikacji.

Artykuł 7

Niniejsza decyzja wygasa trzy lata i sześć miesięcy od dnia jej notyfikacji, chyba że zostanie przedłużona zgodnie z procedurą określoną w art. 31 ust. 2 dyrektywy 95/46/WE.

Artykuł 8

Niniejsza decyzja skierowana jest do Państw Członkowskich.

Sporządzono w Brukseli, dnia 14 maja 2004 r.

W imieniu Komisji
Frederik BOLKESTEIN
Członek Komisji

ZAŁĄCZNIK

ZOBOWIĄZANIA MINISTERSTWA BEZPIECZEŃSTWA WEWNĘTRZNEGO BIURA CELNEGO I OCHRONY GRANIC (CBP)

W celu poparcia planu Komisji Europejskiej (zwanej dalej Komisją) mającego na celu wykonywanie uprawnień powierzonych jej na mocy art. 25 ust. 6 dyrektywy 95/46/WE (zwanej dalej Dyrektywą) oraz przyjęcie decyzji uznającej Biuro Celne i Ochrony Granic (CBP) Ministerstwa Bezpieczeństwa Wewnętrznego jako zapewniające odpowiednią ochronę do celów przekazywania przez przewoźników lotniczych danych zawartych w PNR (zbiór informacji dotyczących podróży danego pasażera⁽¹⁾), które mogą wchodzić w zakres Dyrektywy, CBP zobowiązuje się do:

Podstawa prawna do otrzymania PNR

1. Na mocy ustawy (tytuł 49, *United States Code*, sekcja 44909(c)(3)) oraz jego przepisów wykonawczych (przejściowych) (tytuł 19, *Code of Federal Regulations*, sekcja 122.49b), każdy przewoźnik lotniczy obsługujący loty pasażerskie w zagranicznym ruchu powietrznym do lub ze Stanów Zjednoczonych musi zapewnić CBP (uprzednio Służby Celne Stanów Zjednoczonych) elektroniczny dostęp do danych zawartych w PNR w takim zakresie, w jakim są one zebrane i zawarte w automatycznym systemie rezerwacji przewoźników lotniczych/kontroli odlotów („systemy rezerwacji”);

Wykorzystanie danych zawartych w PNR przez CBP

2. CBP może uzyskać większość danych zawartych w PNR poprzez analizę danych zawartych na bilecie lotniczym pasażera oraz innych dokumentach podróży w drodze rutynowej kontroli granicznej, jednak możliwość otrzymania tych danych drogą elektroniczną znacząco zwiększa zdolność CBP do ułatwiania podróży *bona fide* i przeprowadzania skutecznej wcześniejszej oceny ryzyka w stosunku do pasażerów;
3. Dane zawarte w PNR są wykorzystywane przez CBP wyłącznie do celów zapobiegania i zwalczania 1) terroryzmu i związanych z nim przestępstw; 2) innych poważnych przestępstw włącznie z przestępczością zorganizowaną, która z zasady ma charakter transnarodowy; oraz 3) unikania kary aresztu lub więzienia za powyższe przestępstwa. Wykorzystanie danych zawartych w PNR do tych celów umożliwi CBP skoncentrowanie swoich zasobów na kwestiach wysokiego ryzyka, ułatwiając tym samym i lepiej chroniąc podróże *bona fide*;

Wymagania w stosunku do danych

4. Elementy danych wymagane przez CBP wymienione są w załączniku „A”. (Określone w ten sposób dane zwane są dalej „PNR” do celów niniejszych Zobowiązań). Mimo, że CBP wymaga dostępu do wszystkich trzydziestu czterech (34) elementów danych wymienionych w załączniku „A”, CBP twierdzi, że tylko w nielicznych przypadkach konkretny PNR będzie zawierał pełen zestaw określonych danych. W przypadkach, gdy PNR nie zawiera pełnego zestawu określonych danych, CBP nie będzie dążyć do uzyskania bezpośredniego dostępu z systemu rezerwacji przewoźników lotniczych do innych danych zawartych w PNR, które nie są wymienione w załączniku „A”;
5. W odniesieniu do danych określonych jako „OSI” i „SSI/SSR” (potocznie określane jako uwagi ogólne i pola otwarte), zautomatyzowany system CBP będzie przeszukiwał wymienione pola w poszukiwaniu innych danych określonych w załączniku „A”. Personel CBP nie będzie upoważniony do ręcznego przeglądania wszystkich informacji pól OSI i SSI/SSR, jeżeli osoba, której dotyczą dane zawarte w PNR, nie została określona przez CBP jako osoba o wysokim ryzyku w odniesieniu do jakiegokolwiek celu określonego w ust. 3 niniejszego dokumentu;
6. Dodatkowe informacje osobowe poszukiwane jako bezpośredni wynik danych zawartych w PNR będą uzyskiwane ze źródeł innych niż rządowe tylko drogą prawną, włącznie z wykorzystaniem kanałów wzajemnej pomocy prawnej, jeżeli będzie taka potrzeba, oraz tylko do celów ustanowionych w ust. 3 niniejszego dokumentu. Na przykład, jeżeli numer karty kredytowej jest wymieniony w PNR, można uzyskać informacje na temat transakcji związanych z kontem w drodze procedury prawnej, takiej jak wezwanie sądowe wydane przez wielką ławę przysięgłych lub nakaz sądowy, lub w inny sposób dozwolony przez prawo. Ponadto dostęp do zapisów związanych z kontami poczty elektronicznej pochodzących z PNR będzie wymagał zgodnie z prawem Stanów Zjednoczonych wezwań sądowych, nakazów sądowych, nakazów aresztowania, lub innych procedur dozwolonych przez prawo, w zależności od typu poszukiwanej informacji;
7. CBP będzie konsultować z Komisją zmiany w liście żądanych danych zawartych w PNR (załącznik „A”) zanim wprowadzi te zmiany, jeżeli CBP będzie wiedziało o dodatkowych rubrykach PNR, które linie lotnicze mogą wprowadzić do swoich systemów, a które mogłyby znacząco poprawić zdolność CBP do przeprowadzania oceny ryzyka w stosunku do pasażerów, lub jeżeli okoliczności wskazują, że uprzednio niewymagana rubryka PNR stanie się niezbędna do realizacji specyficznych celów określonych w ust. 3 niniejszych Zobowiązań;

⁽¹⁾ Dla celów niniejszej decyzji, określenia „pasażer” i „pasażerowie” obejmują członków załogi pokładowej.

8. CBP może przekazywać dane PNR w większych partiach do Administracji Bezpieczeństwa Transportu [Transportation Security Administration – TSA] do celów przeprowadzenia testów przez TSA ich Komputerowego Systemu Wstępnego Przeglądu Pasażerów II [Computer Assisted Passenger Prescreening System II - CAPPS II]. Informacje te nie zostaną przekazane do momentu uzyskania zgody na testowanie danych zawartych w PNR dotyczących krajowych lotów w Stanach Zjednoczonych. Przekazane w ten sposób dane zawarte w PNR nie będą przechowywane przez TSA ani żadną inną stronę bezpośrednio zaangażowaną w testowanie po okresie niezbędnym do celów testowania, ani nie zostaną przekazane stronie trzeciej⁽²⁾. Cel przetwarzania jest ściśle ograniczony do testowania systemu CAPPS II i jego interfejsów i, z wyjątkiem nagłych wypadków związanych z identyfikacją znanego terrorysty lub osoby blisko powiązanej z terroryzmem, nie będzie pociągał za sobą żadnych konsekwencji. Zgodnie z ust. 10, który przewiduje zautomatyzowaną metodę filtrowania danych, CBP dokona filtracji i wykasowania „danych szczególnie chronionych” przed przesłaniem PNR w większej partii do TSA zgodnie z niniejszym ustępem.

Przetwarzanie „danych szczególnie chronionych”

9. CBP nie będzie wykorzystywać „danych szczególnie chronionych” (tzn. danych osobowych wskazujących na pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne lub przynależność do związków zawodowych oraz danych dotyczących zdrowia i życia seksualnego) zawartych w PNR, jak opisano poniżej;
10. CBP wprowadzi w życie, możliwie najszybciej, zautomatyzowany system filtrujący i usuwający niektóre szczególnie chronione kody i określenia zawarte w PNR, określone przez CBP w porozumieniu z Komisją;
11. Do czasu wprowadzenia w życie takich filtrów, CBP deklaruje, że nie wykorzystuje i nie będzie wykorzystywać szczególnie chronionych danych zawartych w PNR oraz zobowiązuje się do usunięcia takich danych z wszelkich przypadków uznaniowego ujawnienia PNR na mocy ust. 28-34⁽³⁾;

Sposób dostępu do danych zawartych w PNR

12. W odniesieniu do danych zawartych w PNR, do których CBP ma dostęp (lub które otrzymuje) bezpośrednio z systemu rezerwacji przewoźnika lotniczego do celów identyfikacji osób mogących podlegać kontroli granicznej, pracownicy CBP będą mieć dostęp (lub otrzymywać) i wykorzystywać dane zawarte w PNR dotyczące osób, których podróż zawiera przelot do lub ze Stanów Zjednoczonych⁽⁴⁾;
13. CBP będzie „wyciągać” informacje na temat pasażerów z systemów rezerwacji przewoźników lotniczych do czasu, kiedy przewoźnicy lotniczy będą w stanie wprowadzić w życie system „wysyłający” dane do CBP;
14. CBP będzie wyciągać dane zawarte w PNR związane z konkretnym lotem nie wcześniej niż na 72 godziny przed odlotem, i będzie powtórnie sprawdzać system nie więcej niż trzykrotnie (3) pomiędzy odpowiednio pierwszym wyciągnięciem informacji, odlotem z miejsca poza granicami Stanów Zjednoczonych a przylotem do Stanów Zjednoczonych, lub pomiędzy pierwszym wyciągnięciem informacji a odlotem ze Stanów Zjednoczonych, w celu sprawdzenia, czy nie zaszły zmiany w informacjach. W momencie, gdy przewoźnicy lotniczy będą mieli możliwość wysyłania danych zawartych w PNR, CBP będzie musiało otrzymywać dane na 72 godziny przed odlotem, zakładając, że wszystkie zmiany w danych zawartych w PNR dokonane pomiędzy chwilą otrzymania danych a momentem przylotu do lub odlotu ze Stanów Zjednoczonych zostaną również przesłane do CBP⁽⁵⁾. W wyjątkowych przypadkach, gdyby CBP otrzymało wcześniejsze informacje, że szczególna osoba lub osoby mogą podróżować drogą powietrzną z, do Stanów Zjednoczonych lub przez Stany Zjednoczone, CBP może wyciągnąć (lub zażądać szczególnego przesłania) danych zawartych w PNR wcześniej niż na 72 godziny przed odlotem w celu zapewnienia podjęcia odpowiednich działań, jeżeli niezbędnym byłoby zapobieżenie lub zwalczanie wykroczenia wymienionego w ust. 3 niniejszego dokumentu. Praktycznie, w przypadkach, gdy CBP musi mieć dostęp do danych zawartych w PNR wcześniej niż na 72 godziny przed odlotem, CBP będzie wykorzystywać zwyczajowe procedury stosowania prawa;

⁽²⁾ Dla celów niniejszego przepisu, CBP nie jest traktowane jako strona bezpośrednio zaangażowana w testowanie systemu CAPPS II ani jako „strona trzecia”.

⁽³⁾ Przed wprowadzeniem w życie przez CBP zautomatyzowanego systemu filtrowania (jak wspomniano w ust. 10 niniejszego dokumentu), jeżeli dane szczególnie chronione są zawarte w PNR, które stało się przedmiotem przypadkowego ujawnienia przez CBP jak opisane w ust. 35 niniejszego dokumentu, CBP dołoży wszelkich starań, aby ograniczyć ujawnienia zawartych w PNR danych szczególnie chronionych, zgodnie z prawem Stanów Zjednoczonych.

⁽⁴⁾ Obejmie to osoby przejeżdżające tylko tranzytem przez Stany Zjednoczone.

⁽⁵⁾ W przypadku gdy przewoźnicy lotniczy zgodzą się na przesyłanie danych zawartych w PNR do CBP, agencja włączy się w dyskusje z przewoźnikami na temat możliwości przesyłania danych zawartych w PNR w stałych odstępach czasu odpowiednio w okresie między 72 godzinami przed odlotem z miejsca poza granicami Stanów Zjednoczonych a przylotem do Stanów Zjednoczonych lub też w okresie 72 godzin przed odlotem ze Stanów Zjednoczonych. CBP poszukuje metody przesyłania niezbędnych danych zawartych w PNR w sposób, który zaspokoi potrzeby agencji dla skutecznej oceny ryzyka przy minimalnym wpływie ekonomicznym na przewoźników lotniczych.

Przechowywanie danych zawartych w PNR

15. Podlegając zatwierdzeniu przez Krajową Administrację Archiwów i Rejestrów [National Archives and Records Administration] (tytuł 44, United States Code, sekcja 2101 i następne), CBP będzie ograniczać dostęp on-line do danych zawartych w PNR do uprawnionych użytkowników w CBP⁽⁶⁾ na okres siedmiu (7) dni, po którym liczba urzędników mających dostęp do danych zawartych w PNR zostanie jeszcze bardziej ograniczona na okres 3 lat i 6 miesięcy (3,5 roku) od daty otrzymania dostępu do nich lub otrzymania tych danych z systemów rezerwacji przewoźników lotniczych. Po okresie 3,5 roku dane zawarte w PNR, do których w tym czasie nie próbowano uzyskać dostępu ręcznie, zostaną zniszczone. Dane zawarte w PNR, do których dokonano ręcznego dostępu w trakcie początkowego okresu 3,5 roku, zostaną przekazane przez CBP do pliku skasowanych danych⁽⁷⁾, gdzie pozostaną przez okres ośmiu (8) lat przed ich całkowitym zniszczeniem. Harmonogram ten jednak nie będzie miał zastosowania do danych zawartych w PNR, które są połączone z konkretnym zapisem stosowania (takie dane pozostaną dostępne do czasu, kiedy dany zapis stosowania nie zostanie zarchiwizowany). W odniesieniu do PNR, do których CBP ma dostęp (lub otrzymał) bezpośrednio z systemów rezerwacji przewoźników lotniczych w trakcie obowiązywania niniejszych Zobowiązań, CBP będzie przestrzegać zasad przechowywania ustanowionych w powyższym ustępie, bez uszczerbku dla możliwego wygaśnięcia Zobowiązań zgodnie z ust. 46 niniejszego dokumentu;

Bezpieczeństwo systemu komputerowego CBP

16. Uprawnieni pracownicy CBP otrzymują dostęp do PNR poprzez zamknięty system intranetowy CBP w całości zaszyfrowany, a połączenie podlega kontroli Centrum Danych Celných [Customs Data Center]. Dane zawarte w PNR, przechowywane w bazie danych CBP, są ograniczone do dostępu „tylko do odczytu” przez uprawnionych pracowników, co oznacza, że format danych może zostać zmieniony, jednak treść danych nie może zostać zmieniona w znaczący sposób od momentu otrzymania przez CBP dostępu do systemu rezerwacji przewoźników lotniczych;
17. Żadna inna zagraniczna, federalna, stanowa czy lokalna agencja nie ma bezpośredniego dostępu elektronicznego do danych zawartych w PNR poprzez bazy danych CBP (w tym poprzez Międzyresortowy System Kontroli Granicznej [Interagency Border Inspection System - IBIS]);
18. Szczegóły dotyczące dostępu do informacji w bazach danych CBP (takie jak: kto, gdzie, kiedy (data i czas) oraz wszelkie zmiany w tych danych) są automatycznie zapisywane i rutynowo kontrolowane przez Biuro Spraw Wewnętrznych (Office of Internal Affairs), aby zapobiec nieuprawnionemu wykorzystaniu systemu;
19. Tylko niektórzy urzędnicy, pracownicy czy wykonawcy technologii informacyjnych⁽⁸⁾ CBP (pod nadzorem CBP), którzy pozytywnie przeszli badanie przeszłości, posiadają aktywne, chronione hasłem konto w systemie komputerowym CBP oraz posiadają stwierdzony urzędowy cel przeglądania danych zawartych w PNR, mają dostęp do danych zawartych w PNR;
20. Urzędnicy, pracownicy czy podwykonawcy CBP są zobowiązani do odbywania co dwa lata szkolenia w dziedzinie ochrony i prywatności danych, włącznie ze zdaniem testu. Kontrola systemu CBP jest wykorzystywana do monitorowania i zapewniania zgodności ze wszystkimi wymogami prywatności i ochrony danych;
21. Nieuprawniony dostęp pracowników CBP do systemu rezerwacji przewoźników lotniczych lub skomputeryzowanego systemu CBP, w którym przechowywane są dane zawarte w PNR, podlega surowemu postępowaniu dyscyplinarnemu (włącznie z możliwością zwolnienia z pracy) i może skutkować nałożeniem sankcji karnych (grzywny, więzienia do roku czasu, lub obu) (patrz tytuł 18, United States Code, sekcja 1030);
22. Polityka i przepisy CBP również zapewniają rygorystyczne postępowanie dyscyplinarne (które może obejmować zwolnienie z pracy), podejmowane przeciwko pracownikowi CBP, który ujawnił informacje pochodzące z komputerowego systemu CBP bez oficjalnego pozwolenia (tytuł 19, Code of Federal Regulations, sekcja 103.34);
23. Sankcje karne (grzywny, więzienie do roku czasu, lub obie) mogą zostać nałożone na każdego urzędnika lub pracownika w Stanach Zjednoczonych za ujawnienie danych zawartych w PNR uzyskanych w trakcie zatrudnienia, jeżeli ujawnienie to nie jest prawnie uzasadnione (patrz tytuł 18, United States Code, sekcje 641, 1030 i 1905);

⁽⁶⁾ Uprawnieni użytkownicy CBP będą obejmować pracowników przydzielonych do jednostek analitycznych w biurach terenowych, oraz pracowników przydzielonych do pracy w Krajowym Centrum Celów [National Targeting Center]. Jak zaznaczono wcześniej, osoby zobowiązane do utrzymywania, rozwijania lub audytowania baz danych CBP będą także mieć dostęp do wymienionych danych w ograniczonych celach.

⁽⁷⁾ Mimo, że rejestr PNR nie jest technicznie kasowany w momencie przesyłania go do Pliku Skasowanego Rejestru, jest on przechowywany w postaci pierwotnej (nie w postaci gotowych formularzy do wyszukania, a więc nie jest przydatny „tradycyjnym” śledztwom prowadzonym przez organy ścigania) i dostępne są dla upoważnionych pracowników Biura Spraw Wewnętrznych CBP (i w niektórych przypadkach Biura Głównego Inspektora w powiązaniu z audytem) oraz pracowników odpowiedzialnych za utrzymanie bazy danych Biura Technologii Informacyjnych CBP, na zasadzie „potrzebny”.

⁽⁸⁾ Dostęp dla „wykonawców” do danych zawartych w PNR przechowywanych w systemie komputerowym CBP zostanie przyznany osobom zatrudnionym przez CBP w celu pomocy w utrzymaniu i rozwijaniu systemu komputerowego CBP.

Przetwarzanie i ochrona przez CBP danych zawartych w PNR

24. CBP traktuje zawarte w PNR informacje na temat osób różnych narodowości i zamieszkujących w różnych krajach jako prawnie chronione, poufne informacje osobowe osoby, której dane dotyczą, oraz jako poufne informacje handlowe przewoźnika lotniczego; w związku z tym CBP nie ujawni tych danych publicznie, z wyjątkiem przypadków przewidzianych w niniejszych Zobowiązaniach lub w innych przypadkach, gdy wymaga tego prawo;
25. Publiczne ujawnienie danych zawartych w PNR jest ogólnie regulowane Ustawą o Wolności Informacji (FOIA) (tytuł 5, United States Code, sekcja 552), która umożliwia każdemu (niezależnie od narodowości i kraju zamieszkania) dostęp do rejestrów agencji federalnych Stanów Zjednoczonych, jeżeli zakres takiego rejestru (lub jego część) nie są chronione przed podaniem do wiadomości publicznej poprzez zastosowanie odpowiedniego wyłączenia zgodnie z FOIA. W ramach tych wyłączeń FOIA zezwala agencji na wstrzymanie ujawnienia rejestru (lub jego części), jeżeli informacje są poufnymi informacjami handlowymi, jeżeli ujawnienie informacji stanowiłoby wyraźne nieuzasadnione naruszenie prywatności lub jeżeli informacje są zbierane do celów ścigania przestępstw, w takim zakresie, że można się spodziewać, że ich ujawnienie będzie stanowić nieuzasadnione naruszenie prywatności (tytuł 5, United States Code, sekcje 552(b)(4), (6), (7)(C));
26. Przepisy CBP (tytuł 19, Code of Federal Regulations, sekcja 103.12), które regulują przetwarzanie wniosków o udzielenie informacji (takich jak dane zawarte w PNR) w zastosowaniu FOIA, szczególnie stanowią, że warunki ujawnienia informacji ustanowione w FOIA (podlegające określonym ograniczonym wyjątkom w przypadku wniosków składanych przez osobę, której dane dotyczą) nie mają zastosowania do rejestrów CBP odnoszących się do: (1) poufnych informacji handlowych; (2) materiałów dotyczących prywatności, których ujawnienie stanowiłoby wyraźne nieuzasadnione naruszenie prywatności; oraz (3) informacji zbieranych do celów ścigania przestępstw, w przypadku których można się spodziewać, że ich ujawnienie będzie stanowić nieuzasadnione naruszenie prywatności⁽⁹⁾.
27. CBP zajmie stanowisko w związku z postępowaniami administracyjnymi i sądowymi wynikającymi z wniosków składanych na mocy FOIA o ujawnienie informacji zawartych w PNR uzyskanych od przewoźników lotniczych, że rejestry te wyłączone są z ujawnienia zgodnie z FOIA;

Przekazywanie danych zawartych w PNR do innych organów rządowych

28. Z wyjątkiem przekazywania informacji między CBP a TSA zgodnie z ust. 8 niniejszego dokumentu, części Ministerstwa Bezpieczeństwa Wewnętrznego (DHS) będą traktowane jako „strony trzecie”, podlegające takim samym przepisom i warunkom w odniesieniu do dostępu do danych zawartych w PNR jak inne organy rządowe spoza DHS;
29. CBP będzie według własnego uznania dostarczać dane zawarte w PNR innym organom rządowym, włącznie z zagranicznymi, odpowiedzialnymi za walkę z terroryzmem lub ściganie przestępstw, na zasadzie jednostkowych przypadków, do celów zapobiegania i zwalczania przestępstw wymienionych w ust. 3 niniejszego dokumentu. (Organy, z którymi CBP może dzielić się takimi danymi zwane są dalej „Wyznaczonymi Organami”);
30. CBP będzie rozsądnie wykonywać swoje prawo do uznaniowego przekazywania danych zawartych w PNR dla wyżej wymienionych celów. CBP najpierw określi, czy powód do ujawnienia danych zawartych w PNR innemu Wyznaczonemu Organowi mieści się w ramach wymienionych celów (patrz ust. 29 niniejszego dokumentu). Jeżeli tak, CBP określi, czy dany Wyznaczony Organ jest odpowiedzialny za zapobieganie, prowadzenie dochodzeń i ściganie naruszeń, lub za stosowanie bądź wdrażanie statutu lub przepisów związanych z tymi celami, w przypadku, gdy CBP jest świadome wskazania naruszenia lub potencjalnego naruszenia prawa. Zasadność ujawnienia będzie wymagać przeglądu w świetle przedstawionych okoliczności;
31. Do celów uregulowania upowszechniania danych zawartych w PNR, które mogą być przekazywane innym Wyznaczonym Organom, CBP jest traktowane jako „właściciel” danych i „Wyznaczone Organy” są zobowiązane na mocy wyżej wymienionych warunków ujawnienia do: (1) wykorzystania danych zawartych w PNR wyłącznie do celów ustanowionych w ust. 29 lub 34 niniejszego dokumentu; (2) zapewnienia uporządkowanego trybu pozbywania się informacji zawartych w PNR, które zostały otrzymane, zgodnie z procedurami przechowywania danych w rejestrach Wyznaczonych Organów; oraz (3) otrzymania wyraźnej zgody CBP do dalszego ich upowszechniania. Niedotrzymanie warunków przesyłania danych może zostać zbadane i zgłoszone przez Głównego Urzędnika ds. Prywatności w DHS oraz spowodować, że Wyznaczony Organ nie będzie mogła dalej otrzymywać od CBP danych zawartych w PNR;

⁽⁹⁾ CBP będzie powoływać się na te wyłączenia w sposób jednolity, bez względu na narodowość lub kraj zamieszkania osoby, której dane dotyczą.

32. Każde ujawnienie przez CBP danych zawartych w PNR będzie uwarunkowane od traktowania ich przez agencję otrzymującą je jako poufnej informacji handlowej, prawnie chronionej, jako poufnych informacji osobowych osoby, której dotyczą, jak stwierdzone w ust. 25 i 26 niniejszego dokumentu, które powinny być traktowane jako wyłączone z ujawniania zgodnie z Ustawą o Wolności Informacji (tytuł 5, United States Code, sekcja 552). Dalej, agencja otrzymująca informacje otrzyma także informacje, że dalsze ujawnianie tych informacji jest niedozwolone bez wcześniejszego otrzymania wyraźnej zgody od CBP. CBP nie wyrazi zgody na dalsze przekazywanie danych zawartych w PNR do celów innych niż określone w ust. 29, 34 i 35 niniejszego dokumentu;
33. Osoby zatrudnione przez Wyznaczony Organ, które bez otrzymania odpowiedniego zezwolenia ujawniły dane zawarte w PNR, mogą podlegać sankcjom karnym (tytuł 18, United States Code, sekcje 641, 1030, 1905);
34. Żadne z powyższych stwierdzeń nie utrudni wykorzystania lub ujawnienia danych zawartych w PNR właściwemu organowi rządowemu, jeżeli jest to konieczne w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innych osób, w szczególności w odniesieniu do znacznego zagrożenia zdrowia. Ujawnienie dla powyższych celów podlega takim samym warunkom przekazywania jak ustalone w ust. 31 i 32 niniejszych Zobowiązaniach;
35. Żadne stwierdzenie w niniejszych Zobowiązaniach nie utrudni wykorzystania lub ujawnienia danych zawartych w PNR w postępowaniach karnych oraz w innych przypadkach wymaganych przez prawo. CBP będzie doradzać Komisji w sprawie prawodawstwa Stanów Zjednoczonych, które wpływa co do meritum na niniejsze Zobowiązania;

Zawiadomienie, dostęp do danych oraz środki odwoławcze dla osób, których dotyczą dane zawarte są w PNR

36. CBP będzie udzielać informacji podróżującym na temat wymogów dotyczących PNR oraz kwestii związanych z ich wykorzystaniem (np. ogólnych informacji dotyczących organu, z upoważnienia którego dane są zbierane, celu zbierania danych, ochrony danych, przekazywania danych, tożsamości urzędnika odpowiedzialnego, dostępnych środków odwoławczych oraz informacji kontaktowych dla osób mających pytania lub zgłaszających ewentualne problemy itp., poprzez zamieszczenie na stronie internetowej CBP, ulotkach dla podróżnych itp.);
37. Wnioski złożone przez osoby, których dane dotyczą, w sprawie otrzymania kopii danych zawartych w PNR znajdujących się w bazie danych CBP, odnoszących się do wnioskodawcy, są przetwarzane zgodnie z Ustawą o Wolności Informacji. Wnioski takie należy kierować do: pocztą do Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229; lub wnioski można składać do Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters, Washington, D.C. Dalsze informacje dotyczące procedur składania wniosków na mocy FOIA zawarte są w sekcji 103.5 w tytule 19 Kodeksu Przepisów Federalnych Stanów Zjednoczonych (U.S. Code of Federal Regulations). W przypadku wniosku złożonego przez osobę, której dane dotyczą, fakt, że CBP w innych przypadkach traktuje dane zawarte w PNR jako poufne informacje osobowe oraz poufne informacje handlowe przewoźnika lotniczego, nie będzie wykorzystany przez CBP jako podstawa zgodnie z FOIA do wstrzymania się od ujawnienia danych zawartych w PNR osobie, której te dane dotyczą;
38. W określonych wyjątkowych okolicznościach CBP może wykonywać swoje uprawnienia zgodnie z FOIA do odrzucenia lub odroczenia ujawnienia całej (lub części fragmentu) zawartości PNR osobie, której one dotyczą, na mocy tytułu 5 Kodeksu Stanów Zjednoczonych (United States Code), sekcji 552(b) (np. jeżeli „można oczekiwać, że ujawnienie zgodne z FOIA mogłoby zakłócać postępowanie wykonawcze” lub „ujawniłoby techniki i procedury działań organów ścigania... [co] mogłoby spowodować ryzyko obchodzenia prawa”). Zgodnie z FOIA, każdy wnioskodawca ma prawo do administracyjnego i sądowego zakwestionowania decyzji CBP w sprawie wstrzymania ujawnienia informacji (patrz tytuł 5, United States Code, sekcja 552(a)(4)(B); tytuł 19, Code of Federal Regulations, sekcja 103.7-103.9);
39. CBP zobowiązuje się do sprostowywania⁽¹⁰⁾ danych na żądanie pasażerów i członków załogi, przewoźników lotniczych oraz Organów Ochrony Danych (OOD) w Państwach Członkowskich UE (w zakresie szczegółowo określonym przez osobę, której dane dotyczą), jeżeli CBP określi, że baza danych zawiera takie dane i ich korekta jest uzasadniona i właściwie poparta. CBP będzie informować wyznaczone władze, które otrzymały dane zawarte w PNR, o każdym materiale zawierającym sprostowanie tych danych;

⁽¹⁰⁾ Poprzez „sprostowanie”, CBP chce jasno podkreślić, że nie będzie upoważnione do wprowadzania zmian w danych w ramach rejestru PNR, do których ma dostęp dzięki przewoźnikom lotniczym. Stworzony, raczej, zostanie oddzielny zapis połączony z rejestrem PNR w celu stwierdzenia, że dane zostały określone jako nieprawidłowe oraz wprowadzenia właściwej korekty. W szczególności, CBP będzie odnotowywać zapis wtórnego przeglądu danych przez pasażera w celu odzwierciedlenia, że określone dane zawarte w PNR mogą być lub są nieprawidłowe.

40. Wnioski o sprostowanie danych zawartych w PNR znajdujących się w bazie danych CBP oraz skargi osób fizycznych w sprawie traktowania tych danych przez CBP mogą być składane bezpośrednio lub przez właściwy OOD (w zakresie upoważnionym przez osobę, której dane dotyczą) do: Assistant Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229;
41. W przypadku gdy CBP nie jest w stanie rozstrzygnąć skargi, może ona zostać skierowana pisemnie do Głównego Urzędnika ds. Prywatności w Departamencie Bezpieczeństwa Wewnętrznego (Chief Privacy Officer, Department of Homeland Security Washington, DC 20528), który dokona przeglądu sytuacji i postara się rozstrzygnąć spór⁽¹¹⁾;
42. Ponadto Biuro ds. Prywatności Ministerstwa Bezpieczeństwa Wewnętrznego będzie rozpatrywać w trybie przyspieszonym skargi skierowane do niego przez OOD Państw Członkowskich UE w imieniu osoby zamieszkującej w UE w zakresie, w jakim osoba ta upoważniła OOD do działania w jej imieniu i która twierdzi, że jej skarga w sprawie ochrony danych zawartych w PNR nie została rozpatrzona w zadowalający sposób przez CBP (jak ustanowione w ust. 37-41 niniejszych Zobowiązaniach) lub Biuro ds. Prywatności Ministerstwa Bezpieczeństwa Wewnętrznego. Biuro ds. Prywatności przekaże swoje wnioski i doradzi właściwemu OOD w sprawie działań, jakie należy podjąć, jeżeli zachodzi taka potrzeba. Główny Urzędnik ds. Prywatności w Departamencie Bezpieczeństwa Wewnętrznego zawrze w swoim sprawozdaniu dla Kongresu kwestie związane z liczbą, treścią i rozpatrzeniem skarg dotyczących przetwarzania danych osobowych, takich jak zawarte w PNR⁽¹²⁾;

Przestrzeganie przepisów

43. CBP, wspólnie z DHS, zobowiązuje się do przeprowadzania raz do roku lub częściej za porozumieniem stron, wspólnego przeglądu wraz z Komisją wspieraną w razie potrzeby przez przedstawicieli europejskich organów ścigania przestępstw i/lub organów Państw Członkowskich Unii Europejskiej⁽¹³⁾, w sprawie wprowadzania w życie niniejszych Zobowiązań, w celu przyczynienia się do skutecznego działania procedur opisanych w niniejszych Zobowiązaniach.
44. CBP przyjmie regulacje, wytyczne oraz inne dokumenty polityczne obejmujące powyższe stwierdzenia, aby zapewnić zgodność z niniejszymi Zobowiązaniem urzędników, pracowników oraz wykonawców CBP. Jak wskazano w niniejszym dokumencie, niezastosowanie się urzędników, pracowników oraz wykonawców CBP do przepisów polityki CBP zawartej w niniejszym dokumencie może skutkować odpowiednio podejmowaniem rygorystycznych środków dyscyplinarnych oraz sankcji karnych;

Wzajemność

45. W przypadku wprowadzenia w życie w UE systemu identyfikacji pasażerów linii lotniczych, który zobowiązywałby je do zapewnienia władzom dostępu do danych zawartych w PNR pasażerów, których bieżąca trasa podróży obejmuje przelot do lub z Unii Europejskiej, CBP zobowiązuje się do zachęcania, na zasadzie wzajemności, linii lotniczych bazujących w Stanach Zjednoczonych do współpracy;

Przeгляд i wygaśnięcie Zobowiązań

46. Niniejsze Zobowiązania stosuje się przez okres trzech lat i sześciu miesięcy (3,5 roku) począwszy od daty wejścia w życie umowy pomiędzy Stanami Zjednoczonymi a Wspólnotą Europejską, zezwalającej na przetwarzanie danych zawartych w PNR przez przewoźników lotniczych do celów przesyłania ich do CBP, zgodnie z Dyrektywą. Po dwóch latach i sześciu miesiącach (2,5 roku) obowiązywania niniejszych Zobowiązań CBP w powiązaniu z DHS rozpocznie rozmowy z Komisją w celu przedłużenia Zobowiązań oraz wszelakich dodatkowych ustaleń na wzajemnie akceptowalnych zasadach. Jeżeli nie ma możliwości osiągnięcia wzajemnie akceptowalnego porozumienia przed datą wygaśnięcia niniejszych Zobowiązań, Zobowiązania te przestaną obowiązywać;

⁽¹¹⁾ Główny Urzędnik ds. Prywatności w Ministerstwie Bezpieczeństwa Wewnętrznego jest niezależny od wszystkich dyrekcji Ministerstwa Bezpieczeństwa Wewnętrznego. Jest statutowo zobowiązany do zapewnienia, że informacje osobowe wykorzystywane są w sposób zgodny z właściwym ustawodawstwem (patrz przypis 13). Ustalenia Głównego Urzędnika ds. Prywatności są wiążące dla Ministerstwa i nie mogą być podważone na podstawie kwestii politycznych.

⁽¹²⁾ Na mocy sekcji 222 Ustawy o Bezpieczeństwie Wewnętrznym [Homeland Security Act] z 2002 r. (zwana dalej Ustawą) (Prawo Publiczne 107-296, z dn. 25 listopada 2002 r.) Urzędnik ds. Prywatności w Ministerstwie Bezpieczeństwa Wewnętrznego jest zobowiązany do prowadzenia „oceny wpływu na prywatność” proponowanych przez Ministerstwo przepisów w sprawie „prywatności informacji osobowych, włącznie z rodzajem zbieranych informacji osobowych oraz liczbą osób, których to dotyczy” i musi dokonać corocznego sprawozdania przed Kongresem w odniesieniu do „działalności Ministerstwa, mającej wpływ na prywatność...” Ustęp 222 (5) Ustawy wyraźnie nakazuje Urzędnikowi ds. Prywatności w Ministerstwie Bezpieczeństwa Wewnętrznego wysłuchiwanie oraz dokonywanie sprawozdania przed Kongresem w sprawach „skarg o naruszenie prywatności”.

⁽¹³⁾ Strony uprzednio informują się wzajemnie o składzie zespołów obu stron i w skład mogą wchodzić właściwe władze związane z ochroną prywatności/danych, kontrolą celną oraz innymi formami stosowania prawa, bezpieczeństwem granic i/lub bezpieczeństwem lotnictwa. Od organów uczestniczących wymagane będzie otrzymanie niezbędnego upoważnienia do dostępu do informacji niejawnych i przestrzeganie poufności rozmów i dokumentacji, do której otrzymają dostęp. Poufność nie będzie jednak przeszkodą dla stron w sporządzeniu właściwego sprawozdania na temat wyników wspólnego przeglądu dla właściwych im władz, włączając Kongres Stanów Zjednoczonych i Parlament Europejski. Jednakże, w żadnych okolicznościach władzom uczestniczącym nie wolno ujawnić danych osobowych; władzom uczestniczącym nie wolno także ujawnić niepublicznych informacji zaczerpniętych z dokumentów, do których otrzymały dostęp, ani żadnych operacyjnych lub wewnętrznych informacji agencji, w których posiadanie weszły w trakcie przeprowadzania wspólnego przeglądu. Obie strony wzajemnie określą szczegółowe warunki przeprowadzania wspólnego przeglądu.

Klauzula o nieutworzeniu praw prywatnych lub precedensu

47. Niniejsze Zobowiązania nie tworzą ani nie przyznają żadnych praw lub korzyści osobom lub stronom tak prywatnym jak i publicznym.
48. Niniejsze Zobowiązania nie stanowią precedensu do przyszłych rozmów z Komisją, Unią Europejską, organizacjami związanymi lub państwami trzecimi na temat przekazywania danych w jakiegokolwiek formie.

Dnia 11 maja 2004 r.

ZAŁĄCZNIK „A”

Elementy danych zawartych w PNR wymaganych przez CBP od przewoźników lotniczych

1. Numer rezerwacji PNR
 2. Data rezerwacji
 3. Data/y planowanej podróży
 4. Nazwisko
 5. Inne nazwiska/imiona zawarte w PNR
 6. Adres
 7. Wszelkie informacje dotyczące płatności
 8. Adres na rachunku
 9. Kontaktowe numery telefonu
 10. Trasa całej podróży dla określonego PNR
 11. Informacje dotyczące osoby często podróżującej (ograniczone do ilości przeleciań mil i adresu(-ów))
 12. Biuro podróży
 13. Agent biura podróży
 14. Kod dzielonej informacji PNR
 15. Status podróży pasażera (*Travel status*)
 16. Podzielona informacja PNR
 17. Adres elektroniczny (e-mail)
 18. Informacje na temat wystawienia biletu
 19. Uwagi ogólne
 20. Numer biletu
 21. Numer miejsca
 22. Data wystawienia biletu
 23. Niepojawienie się pasażera, który dokonał rezerwacji (*No show*)
 24. Numeru przywieszki bagażowej
 25. Informacja o pasażerze, który nie dokonał uprzedniej rezerwacji (*Go show information*)
 26. Informacja OSI (innych usługach)
 27. Informacja SSI/SSR (specjalne usługi)
 28. Otrzymane z informacji
 29. Wszystkie zmiany wprowadzone do PNR
 30. Liczba podróżujących w ramach danego PNR
 31. Informacja na temat miejsca
 32. Bilety w jedną stronę
 33. Wszelkie zebrane informacje APIS (*Advanced Passenger Information System*)
 34. Pola ATFQ (*Automatic Ticketing Fare Quote*)
-