

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/681**z dnia 27 kwietnia 2016 r.****w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwu terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania**

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 82 ust. 1 lit. d) i art. 87 ust. 2 lit. a),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ⁽¹⁾,

po konsultacji z Komitetem Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ⁽²⁾,

a także mając na uwadze, co następuje:

- (1) W dniu 6 listopada 2007 r. Komisja przyjęła wniosek dotyczący decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa. Jednakże w związku z wejściem w życie w dniu 1 grudnia 2009 r. traktatu lizbońskiego wniosek Komisji, który nie został do tego dnia przyjęty przez Radę, stał się nieaktualny.
- (2) W „Programie sztokholmskim – otwarta i bezpieczna Europa dla dobra i ochrony obywateli” ⁽³⁾ zaapelowano do Komisji o przedłożenie wniosku dotyczącego wykorzystywania danych PNR w celu zapobiegania terroryzmowi i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.
- (3) W komunikacie z dnia 21 września 2010 r. zatytułowanym „Globalne podejście do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim” Komisja przedstawiła kilka zasadniczych elementów polityki unijnej w tej dziedzinie.
- (4) Dyrektywa Rady 2004/82/WE ⁽⁴⁾ reguluje przekazywanie przez przewoźników lotniczych właściwym organom krajowym danych pasażera przekazanych przed podróżą (zwanych dalej „danymi API”) w celu poprawy kontroli granicznej i zwalczania nielegalnej imigracji.
- (5) Celem niniejszej dyrektywy jest, między innymi, zapewnienie bezpieczeństwa ogólnego, ochrona życia i bezpieczeństwa osób oraz stworzenie ram prawnych służących ochronie danych PNR w związku z ich przetwarzaniem przez właściwe organy.
- (6) Skuteczne wykorzystywanie danych PNR, między innymi poprzez porównanie danych PNR z danymi zawartymi w różnych bazach danych poszukiwanych osób i przedmiotów, jest niezbędne do zapobiegania przestępstwu terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, a tym samym do zwiększania bezpieczeństwa wewnętrznego, do zebrania dowodów, a – w odpowiednich przypadkach – do wykrycia współsprawców przestępstw i rozpracowania siatek przestępczych.
- (7) Sprawdzenie danych PNR umożliwia identyfikację osób, które przed dokonaniem takiego sprawdzenia nie były podejrzewane o udział w przestępstwach terrorystycznych lub w poważnej przestępczości i które powinny być poddane dalszemu sprawdzeniu przez właściwe organy. Dzięki wykorzystywaniu danych PNR można reagować na zagrożenie przestępstwami terrorystycznymi i poważną przestępczością z innej perspektywy niż w przypadku przetwarzania innych kategorii danych osobowych. Jednakże aby ograniczyć przetwarzanie danych PNR do niezbędnego minimum, ustalanie i stosowanie kryteriów dokonywania sprawdzeń należy ograniczyć do

⁽¹⁾ Dz.U. C 218 z 23.7.2011, s. 107.⁽²⁾ Stanowisko Parlamentu Europejskiego z dnia 14 kwietnia 2016 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 21 kwietnia 2016 r.⁽³⁾ Dz.U. C 115 z 4.5.2010, s. 1.⁽⁴⁾ Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (Dz.U. L 261 z 6.8.2004, s. 24).

przestępstw terrorystycznych i poważnej przestępczości, w przypadku których stosowanie takich kryteriów jest właściwe. Ponadto kryteria dokonywania sprawdzeń powinny zostać określone w taki sposób, by ograniczyć do minimum liczbę osób niewinnych błędnie zidentyfikowanych przez system.

- (8) Przewoźnicy lotniczy już zbierają i przetwarzają dane PNR swoich pasażerów do celów prowadzonej przez siebie działalności gospodarczej. Niniejsza dyrektywa nie powinna nakładać na przewoźników lotniczych żadnych obowiązków dotyczących zbierania lub zatrzymywania jakichkolwiek dodatkowych danych pochodzących od pasażerów ani nie powinna nakładać na pasażerów żadnych obowiązków dotyczących dostarczania jakichkolwiek innych danych niż te, które już są dostarczane przewoźnikom lotniczym.
- (9) Niektórzy przewoźnicy lotniczy zatrzymują zebrane przez nich dane API jako część danych PNR, podczas gdy inni przewoźnicy tego nie czynią. Wykorzystywanie danych PNR wraz z danymi API stanowi wartość dodaną w zakresie pomocy państwom członkowskim w weryfikacji tożsamości osób, zwiększając tym samym przydatność wyników tych działań dla ścigania przestępczości i minimalizując ryzyko dokonywania sprawdzeń i prowadzenia postępowań przygotowawczych w stosunku do osób niewinnych. Ważne jest zatem zapewnienie, by przewoźnicy lotniczy, którzy zbierają dane API, przekazywali je bez względu na to, czy środki techniczne, za pomocą których zatrzymują dane API, są takie same jak w przypadku innych danych PNR.
- (10) W celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania istotne jest, by wszystkie państwa członkowskie ustanowiły przepisy nakładające na przewoźników lotniczych obsługujących loty pozaunijne obowiązek przekazywania zebranych danych PNR, w tym danych API. Państwa członkowskie powinny mieć również możliwość rozszerzenia tego obowiązku na przewoźników lotniczych obsługujących loty wewnątrzunijne. Przepisy te nie powinny naruszać dyrektywy 2004/82/WE.
- (11) Przetwarzanie danych osobowych powinno być proporcjonalne do szczególnych celów dotyczących bezpieczeństwa, którym służy niniejsza dyrektywa.
- (12) Definicja przestępstw terrorystycznych przyjęta na potrzeby niniejszej dyrektywy powinna być taka sama jak definicja w decyzji ramowej Rady 2002/475/WSiSW⁽¹⁾. Definicja poważnej przestępczości powinna obejmować rodzaje przestępstw wymienione w załączniku II do niniejszej dyrektywy.
- (13) Dane PNR powinny być przekazywane do jednej wyznaczonej jednostki do spraw informacji o pasażerach (zwanej dalej „JIP”) we właściwym państwie członkowskim, tak by zapewnić przejrzystość i ograniczyć koszty ponoszone przez przewoźników lotniczych. JIP może mieć swoje oddziały w jednym państwie członkowskim; państwa członkowskie mogą także wspólnie ustanowić jedną JIP. Państwa członkowskie powinny wymieniać między sobą informacje za pośrednictwem odpowiednich sieci wymiany informacji, aby ułatwić dzielenie się informacjami i zapewnić interoperacyjność.
- (14) Koszty związane z wykorzystywaniem, zatrzymywaniem i wymianą danych PNR powinny ponosić państwa członkowskie.
- (15) Wykaz danych PNR otrzymywany przez JIP należy sporządzać w taki sposób, by czynił on zadość zarówno uzasadnionym potrzebom organów publicznych w związku z zapobieganiem przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywaniem, prowadzeniem postępowań przygotowawczych w ich sprawie i ich ściganiem, przyczyniając się tym samym do poprawy bezpieczeństwa wewnętrznego w Unii, jak również ochrony praw podstawowych, w szczególności prawa do prywatności i ochrony danych osobowych. W tym celu należy stosować wysokie standardy zgodnie z Kartą praw podstawowych Unii Europejskiej (zwaną dalej „Kartą praw podstawowych”), Konwencją o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zwaną dalej „Konwencją nr 108”) i Konwencją o ochronie praw człowieka i podstawowych wolności (zwaną dalej „Konwencją praw człowieka”). Wykaz taki nie powinien opierać się na rasie ani pochodzeniu etnicznym, na religii ani przekonaniach, na poglądach politycznych ani jakichkolwiek innych poglądach, na przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby. Dane PNR powinny zawierać wyłącznie informacje dotyczące rezerwacji i tras podróży pasażerów, które umożliwią właściwym organom identyfikację pasażerów lotniczych stanowiących zagrożenie dla bezpieczeństwa wewnętrznego.
- (16) Dostępne są dwie metody przekazywania danych: metoda „pobierania”, polegająca na tym, że właściwe organy państwa członkowskiego potrzebujące danych PNR mogą skorzystać z dostępu do systemu rezerwacji przewoźnika lotniczego i pobrać (ang. *pull*) kopię potrzebnych danych PNR; oraz metoda „dostarczania”, polegająca na tym, że przewoźnicy lotniczy przekazują (ang. *push*) potrzebne dane PNR danemu organowi na jego wniosek, co pozwala im zachować kontrolę nad tym, jakie dane są przekazywane. Uznaje się, że metoda „dostarczania” zapewnia wyższy poziom ochrony danych i powinna być obowiązkowa dla wszystkich przewoźników lotniczych.

(¹) Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3).

- (17) Komisja popiera wytyczne Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO) dotyczące PNR. Wytyczne te powinny zatem stanowić podstawę określenia, jakie formaty danych będą obsługiwane na potrzeby przekazywania danych PNR przez przewoźników lotniczych państwom członkowskim. W celu zapewnienia jednolitych warunków wdrożenia obsługiwanych formatów danych oraz właściwych protokołów obowiązujących przy przekazywaniu danych przez przewoźników lotniczych, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ⁽¹⁾.
- (18) Państwa członkowskie powinny podjąć wszelkie niezbędne środki, aby umożliwić przewoźnikom lotniczym wypełnianie obowiązków nałożonych na nich na podstawie niniejszej dyrektywy. Wobec przewoźników lotniczych, którzy nie wypełniają obowiązków w zakresie przekazywania danych PNR, państwa członkowskie powinny przewidzieć skuteczne, proporcjonalne i odstraszające sankcje, w tym kary finansowe.
- (19) Każde państwo członkowskie powinno odpowiadać za ocenę potencjalnych zagrożeń związanych z przestępstwami terrorystycznymi i poważną przestępczością.
- (20) Uwzględniając w pełni prawo do ochrony danych osobowych oraz prawo do niedyskryminacji, nie można podejmować wyłącznie na podstawie automatycznego przetwarzania danych PNR żadnych decyzji, które miałyby negatywne skutki prawne dla danej osoby lub znacząco wpływałyby na jej sytuację. Ponadto, mając na uwadze art. 8 i 21 Karty praw podstawowych, żadna taka decyzja nie powinna nikogo dyskryminować ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną. Komisja powinna również uwzględnić te zasady dokonując przeglądu stosowania niniejszej dyrektywy.
- (21) Wyniki przetwarzania danych PNR nie powinny w żadnym przypadku być wykorzystywane przez państwa członkowskie jako powód do obejścia międzynarodowych zobowiązań wynikających z Konwencji z dnia 28 lipca 1951 r. dotyczącej statusu uchodźców, zmienionej protokołem z dnia 31 stycznia 1967 r.; wyniki te nie powinny być również wykorzystywane do odmawiania osobom ubiegającym się o azyl bezpiecznego i legalnego wjazdu na terytorium Unii w celu skorzystania z przysługującego im prawa do ochrony międzynarodowej.
- (22) Uwzględniając w pełni zasady przedstawione w najnowszym orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej dotyczącym przedmiotowej kwestii, przy stosowaniu niniejszej dyrektywy należy zapewnić pełne poszanowanie praw podstawowych, prawa do prywatności i zasady proporcjonalności. Należy również zapewnić faktyczną zgodność z celami, jakimi są konieczność i proporcjonalność, w celu realizacji interesu publicznego uznanego przez Unię oraz potrzeby zapewnienia ochrony praw i wolności innych osób w walce z przestępstwami terrorystycznymi i poważną przestępczością. Stosowanie niniejszej dyrektywy powinno być należycie uzasadnione; należy wprowadzić niezbędne gwarancje, aby zapewnić zgodność z prawem przechowywania, analizowania, przekazywania lub wykorzystywania danych PNR.
- (23) Państwa członkowskie powinny wymieniać otrzymywane dane PNR między sobą oraz z Europolem, jeżeli zostanie to uznane za niezbędne do zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania. JIP powinny, w stosownych przypadkach, przekazywać bezzwłocznie JIP w innych państwach członkowskich wyniki przetwarzania danych PNR w celu prowadzenia dalszego postępowania przygotowawczego. Przepisy niniejszej dyrektywy nie powinny naruszać innych unijnych instrumentów dotyczących wymiany informacji między organami policyjnymi i innymi organami ścigania oraz organami wymiaru sprawiedliwości, w tym decyzji Rady 2009/371/WSiSW ⁽²⁾ oraz decyzji ramowej Rady 2006/960/WSiSW ⁽³⁾. Taka wymiana danych PNR powinna być regulowana przepisami o współpracy policyjnej i wymiarów sprawiedliwości i nie powinna zagrażać wysokiemu poziomowi ochrony prywatności i danych osobowych, zgodnie z wymogami określonymi w Karcie praw podstawowych, Konwencji nr 108 i Konwencji praw człowieka.
- (24) Należy zapewnić bezpieczną wymianę informacji dotyczącą danych PNR między państwami członkowskimi za pomocą wszelkich istniejących kanałów współpracy między właściwymi organami państw członkowskich, oraz w szczególności z Europolem za pomocą jego aplikacji sieci bezpiecznej wymiany informacji (SIENA).

⁽¹⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

⁽²⁾ Decyzja Rady 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol) (Dz.U. L 121 z 15.5.2009, s. 37).

⁽³⁾ Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz.U. L 386 z 29.12.2006, s. 89).

- (25) Dane PNR powinny być zatrzymywane na okres niezbędny i proporcjonalny do celów, jakimi są zapobieganie przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie. Ze względu na charakter danych i ich wykorzystanie niezbędne jest zatrzymywanie danych PNR przez wystarczająco długi okres, aby możliwe było ich analizowanie i wykorzystywanie w postępowaniach przygotowawczych. Po upływie początkowego okresu zatrzymania dane PNR powinny zostać poddane depersonalizacji poprzez maskowanie elementów danych, aby zapobiec ich nieproporcjonalnemu wykorzystywaniu. Po upływie początkowego okresu zatrzymania dostęp do pełnych danych PNR, które umożliwiają bezpośrednie zidentyfikowanie osoby, której dane dotyczą, powinien być możliwy wyłącznie po spełnieniu bardzo restrykcyjnych i ściśle określonych warunków, aby zapewnić jak najwyższy poziom ochrony danych.
- (26) Jeżeli właściwemu organowi przekazano konkretne dane PNR i są one wykorzystywane w ramach konkretnego postępowania przygotowawczego lub ścigania w sprawie karnej, ich zatrzymanie przez właściwy organ powinno być uregulowane w prawie krajowym, niezależnie od określonych w niniejszej dyrektywie okresów zatrzymania danych.
- (27) Przetwarzanie danych PNR w każdym państwie członkowskim przez JIP oraz przez właściwe organy powinno podlegać standardom ochrony danych osobowych wynikającym z prawa krajowego, zgodnym z decyzją ramową Rady 2008/977/WSiSW⁽¹⁾ oraz ze szczególnymi wymogami w zakresie ochrony danych określonymi w niniejszej dyrektywie. Odesłania do decyzji ramowej 2008/977/WSiSW należy rozumieć jako odesłania do przepisów obecnie obowiązujących, jak i do przepisów, które je zastąpią.
- (28) Mając na uwadze prawo do ochrony danych osobowych, prawa osób, których dane dotyczą, odnoszące się do przetwarzania ich danych PNR, takie jak prawo dostępu do tych danych, ich poprawiania, usunięcia i ograniczania oraz prawo do odszkodowania i prawo do sądowych środków ochrony prawnej, powinny być zgodne zarówno z decyzją ramową 2008/977/WSiSW, jak również z wysokim poziomem ochrony przewidzianym w Karcie praw podstawowych i Konwencji praw człowieka.
- (29) Uwzględniając prawo pasażerów do uzyskania informacji o przetwarzaniu ich danych osobowych, państwa członkowskie powinny zapewnić, by pasażerowie otrzymywali w sposób łatwo dostępny i zrozumiały dokładne informacje na temat zbierania danych PNR, przekazywania ich do JIP oraz o prawach przysługujących im jako osobom, których dane dotyczą.
- (30) Niniejsza dyrektywa nie narusza przepisów unijnych ani krajowych dotyczących zasady publicznego dostępu do dokumentów urzędowych.
- (31) Przekazywanie danych PNR przez państwa członkowskie państwu trzecim powinno być dopuszczalne wyłącznie na podstawie oceny każdego indywidualnego przypadku i powinno odbywać się w pełnej zgodzie z przepisami ustanowionymi przez państwa członkowskie na podstawie decyzji ramowej 2008/977/WSiSW. Aby zapewnić ochronę danych osobowych, takie przekazywanie danych powinno podlegać dodatkowym wymogom dotyczącym celu przekazywania. Powinno ono także podlegać zasadom konieczności i proporcjonalności oraz wysokiemu poziomowi ochrony zapewnianemu przez Kartę praw podstawowych i Konwencję praw człowieka.
- (32) Krajowy organ nadzorczy ustanowiony w ramach wdrażania decyzji ramowej 2008/977/WSiSW powinien odpowiadać również za doradztwo i monitorowanie w zakresie stosowania przepisów przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy.
- (33) Niniejsza dyrektywa nie wpływa na możliwość ustanowienia przez państwa członkowskie, na mocy przepisów krajowych, systemu zbierania i przetwarzania danych PNR przekazywanych przez podmioty gospodarcze niebędące przewoźnikami, takie jak biura podróży i organizatorzy wycieczek świadczący usługi związane z podróżowaniem, w tym rezerwację lotów, na potrzeby których zbierają i przetwarzają dane PNR, lub przez dostawców usług transportowych innych niż dostawcy określeni w niniejszej dyrektywie, pod warunkiem że takie przepisy krajowe są zgodne z prawem Unii.
- (34) Niniejsza dyrektywa nie narusza obecnych przepisów Unii o trybie prowadzenia kontroli granicznych ani przepisów Unii regulujących wjazd na terytorium Unii i wyjazd z tego terytorium.
- (35) W związku z prawnymi i technicznymi różnicami w przepisach krajowych dotyczących przetwarzania danych osobowych, w tym danych PNR, przewoźnicy lotniczy spotykają się i będą się spotykać ze zróżnicowanymi wymogami co do rodzaju informacji, które należy przekazać, oraz co do warunków, zgodnie z którymi należy je dostarczać właściwym organom krajowym. Różnice te mogą utrudnić skuteczną współpracę między właściwymi organami krajowymi mającą na celu zapobieganie przestępstwom terrorystycznym lub poważnej przestępczości,

⁽¹⁾ Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350 z 30.12.2008, s. 60).

ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie. Niezbędnym jest zatem ustanowienie na poziomie unijnym wspólnych ram prawnych określających przekazywanie i przetwarzanie danych PNR.

- (36) Niniejsza dyrektywa jest zgodna z prawami podstawowymi i zasadami uznanymi w Karcie praw podstawowych, w szczególności z prawem do ochrony danych osobowych, prawem do prywatności i prawem do niedyskryminacji, chronionymi na mocy art. 8, 7 i 21 Karty praw podstawowych; powinna zatem zostać odpowiednio wdrożona. Niniejsza dyrektywa jest zgodna z zasadami ochrony danych, a jej przepisy pozostają w zgodzie z decyzją ramową 2008/977/WSiSW. Ponadto, aby uczynić zadość zasadzie proporcjonalności, w odniesieniu do niektórych kwestii niniejsza dyrektywa przewiduje bardziej rygorystyczne przepisy dotyczące ochrony danych niż decyzja ramowa 2008/977/WSiSW.
- (37) Zakres stosowania niniejszej dyrektywy jest maksymalnie ograniczony, ponieważ: przewiduje ona zatrzymanie danych PNR w JIP przez okres nieprzekraczający pięciu lat, po upływie którego dane powinny zostać usunięte; przewiduje poddanie danych depersonalizacji poprzez maskowanie elementów danych po upływie początkowego okresu sześciu miesięcy; oraz zakazuje zbierania i wykorzystywania danych szczególnie chronionych. W celu zapewnienia skuteczności i wysokiego poziomu ochrony danych państwa członkowskie są zobowiązane do zapewnienia, by za doradztwo i monitorowanie w zakresie sposobu przetwarzania danych PNR odpowiadał niezależny krajowy organ nadzorczy oraz, w szczególności, inspektor ochrony danych. Wszelkie operacje przetwarzania danych PNR powinny być ewidencjonowane lub dokumentowane na potrzeby weryfikacji zgodności z prawem tych operacji, monitorowania własnej działalności oraz zapewnienia odpowiedniej integralności danych i bezpiecznego przetwarzania. Ponadto państwa członkowskie powinny zapewnić, by pasażerowie byli informowani w sposób jasny i dokładny o zbieraniu danych PNR i o przysługujących im prawach.
- (38) Ponieważ cele niniejszej dyrektywy, a mianowicie przekazywanie danych PNR przez przewoźników lotniczych i przetwarzanie tych danych w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ściganie, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest niezbędne do osiągnięcia tych celów.
- (39) Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, te dwa państwa członkowskie powiadomiły o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej dyrektywy.
- (40) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu niniejszej dyrektywy i nie jest nią związana ani jej nie stosuje.
- (41) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ⁽¹⁾ zasięgnięto opinii Europejskiego Inspektora Ochrony Danych, który wydał ją dnia 25 marca 2011 r.,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot i zakres stosowania

1. Niniejsza dyrektywa określa:
- przekazywanie przez przewoźników lotniczych danych dotyczących przelotu pasażera (zwanymi dalej „danymi PNR”), które dotyczą pasażerów lotów pozaunijnych;
 - przetwarzanie danych, o których mowa w lit. a), w tym ich zbieranie, wykorzystywanie i zatrzymywanie przez państwa członkowskie oraz wymianę tych danych między państwami członkowskimi.

⁽¹⁾ Rozporządzenie (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 (Dz.U. L 8 z 12.1.2001, s. 1).

2. Dane PNR zebrane zgodnie z niniejszą dyrektywą mogą być przetwarzane wyłącznie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, jak przewidziano w art. 6 ust. 2 lit. a), b) i c).

Artykuł 2

Stosowanie niniejszej dyrektywy do lotów wewnątrzunijnych

1. Jeżeli państwo członkowskie podejmie decyzję o stosowaniu niniejszej dyrektywy do lotów wewnątrzunijnych, powiadamia o tym Komisję na piśmie. Państwo członkowskie może złożyć lub cofnąć takie powiadomienie w każdym czasie. Komisja publikuje takie powiadomienia oraz wszelkie ich cofnięcia w *Dzienniku Urzędowym Unii Europejskiej*.
2. Po złożeniu powiadomienia, o którym mowa w ust. 1, wszystkie przepisy niniejszej dyrektywy stosuje się do lotów wewnątrzunijnych, tak jakby były one lotami pozaunijnymi, oraz do danych PNR dotyczących lotów wewnątrzunijnych, tak jakby były one danymi PNR dotyczącymi lotów pozaunijnych.
3. Państwo członkowskie może podjąć decyzję o stosowaniu niniejszej dyrektywy wyłącznie do wybranych lotów wewnątrzunijnych. Podejmując taką decyzję, państwo członkowskie dokonuje wyboru lotów, które uważa za niezbędne z punktu widzenia realizacji celów niniejszej dyrektywy. Państwo członkowskie może w każdym czasie podjąć decyzję o zmianie wyboru lotów wewnątrzunijnych.

Artykuł 3

Definicje

Na potrzeby niniejszej dyrektywy stosuje się następujące definicje:

- 1) „przewoźnik lotniczy” oznacza przedsiębiorstwo transportu lotniczego posiadające ważną koncesję lub równorzędne zezwolenie uprawniające do lotniczego przewozu pasażerów;
- 2) „lot pozaunijny” oznacza regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z państwa trzeciego, z zaplanowanym lądowaniem na terytorium państwa członkowskiego albo odbywający się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem w państwie trzecim, w tym – w obu przypadkach – loty z postojami na terytorium państw członkowskich lub państw trzecich;
- 3) „lot wewnątrzunijny” oznacza regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem na terytorium co najmniej jednego innego państwa członkowskiego, bez postojów na terytorium państwa trzeciego;
- 4) „pasażer” oznacza osobę, w tym pasażera transferowego lub tranzytowego, z wyjątkiem członków załogi, która jest przewożona lub ma być przewieziona na pokładzie samolotu za zgodą przewoźnika lotniczego wyrażoną w formie wpisu tej osoby na listę pasażerów;
- 5) „dane dotyczące przelotu pasażera” lub „dane PNR” oznaczają zbiór danych o podróży każdego pasażera, który zawiera informacje niezbędne, aby umożliwić przetwarzanie i weryfikowanie rezerwacji przez przewoźników lotniczych obsługujących rezerwację i lot w odniesieniu do każdego przelotu zarezerwowanego przez jakąkolwiek osobę lub w jej imieniu, bez względu na to, czy zbiór ten znajduje się w systemach rezerwacji, systemach odpraw pasażerskich lub równorzędnych systemach pełniących te same funkcje;
- 6) „system rezerwacji” oznacza wewnętrzny system przewoźnika lotniczego, w którym zbierane są dane PNR w celu obsługi rezerwacji;
- 7) „metoda dostarczania” („metoda push”) oznacza metodę polegającą na przekazywaniu przez przewoźników lotniczych danych PNR, wymienionych w załączniku I, do bazy danych organów, które się o nie zwróciły;

- 8) „przestępstwa terrorystyczne” oznaczają przestępstwa w rozumieniu prawa krajowego, o których mowa w art. 1–4 decyzji ramowej 2002/475/WSiSW;
- 9) „poważna przestępczość” oznacza przestępstwa wymienione w załączniku II, które na mocy prawa krajowego państwa członkowskiego podlegają karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat;
- 10) „depersonalizacja poprzez maskowanie elementów danych” oznacza uczynienie niewidocznymi dla użytkownika takich elementów danych, które mogłyby posłużyć do bezpośredniego zidentyfikowania osoby, której dane dotyczą.

ROZDZIAŁ II

Obowiązki państw członkowskich

Artykuł 4

Jednostka do spraw informacji o pasażerach

1. Każde państwo członkowskie ustanawia lub wyznacza organ właściwy do zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania albo dział takiego organu do pełnienia roli jednostki do spraw informacji o pasażerach (zwanej dalej „JIP”).
2. JIP odpowiada za:
 - a) zbieranie od przewoźników lotniczych danych PNR, ich przechowywanie i przetwarzanie oraz za przekazywanie tych danych lub wyników ich przetwarzania właściwym organom, o których mowa w art. 7;
 - b) wymianę zarówno danych PNR, jak i wyników ich przetwarzania z JIP w innych państwach członkowskich i z Europolem zgodnie z art. 9 i 10.
3. Pracownicy JIP mogą być oddelegowani z właściwych organów. Państwa członkowskie zapewniają JIP odpowiednie zasoby umożliwiające im realizację ich zadań.
4. Dwa państwa członkowskie lub większa ich liczba (zwane dalej „uczestniczącymi państwami członkowskimi”) mogą ustanowić lub wyznaczyć jeden organ jako swoją JIP. Taka JIP jest ustanawiana w jednym z uczestniczących państw członkowskich i uznawana za krajową JIP wszystkich uczestniczących państw członkowskich. Uczestniczące państwa członkowskie uzgadniają wspólnie szczegółowe zasady funkcjonowania JIP oraz przestrzegają wymogów określonych w niniejszej dyrektywie.
5. W terminie jednego miesiąca od ustanowienia własnej JIP każde państwo członkowskie powiadamia o tym Komisję; może ono w każdym czasie dokonać zmiany swojego powiadomienia. Komisja publikuje to powiadomienie oraz wszelkie jego zmiany w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 5

Inspektor ochrony danych w JIP

1. JIP powołuje inspektora ochrony danych, który odpowiada za monitorowanie przetwarzania danych PNR i stosowanie odpowiednich gwarancji.
2. Państwa członkowskie udostępniają inspektorom ochrony danych środki umożliwiające im wykonywanie w sposób skuteczny i niezależny obowiązków i zadań określonych w niniejszym artykule.
3. Państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do kontaktowania się z inspektorem ochrony danych, jako pojedynczym punktem kontaktowym, we wszystkich sprawach związanych z przetwarzaniem danych PNR tej osoby.

Artykuł 6

Przetwarzanie danych PNR

1. Dane PNR przekazane przez przewoźników lotniczych są zbierane przez JIP we właściwym państwie członkowskim w sposób określony w art. 8. Jeżeli wśród danych PNR przekazanych przez przewoźników lotniczych znajdują się dane inne niż wymienione w załączniku I, JIP usuwa takie dane w sposób trwały niezwłocznie po ich otrzymaniu.
2. JIP przetwarza dane PNR wyłącznie w następujących celach:
 - a) dokonania sprawdzenia pasażerów przed ich planowanym przylotem do lub odlotem z państwa członkowskiego w celu identyfikacji osób, które wymagają dalszego sprawdzenia przez właściwe organy, o których mowa w art. 7, oraz – w stosownych przypadkach – przez Europol zgodnie z art. 10, ze względu na możliwość udziału takich osób w przestępstwach terrorystycznych lub w poważnej przestępczości;
 - b) odpowiadania, na podstawie oceny każdego indywidualnego przypadku, na należycie uzasadniony i oparty na wystarczających podstawach wniosek właściwych organów o przekazanie i przetwarzanie danych PNR w określonych przypadkach w celach zapobiegania przestępstwu terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, oraz o przekazanie właściwym organom lub – w stosownych przypadkach – Europolowi wyników takiego przetwarzania; oraz
 - c) analizowania danych PNR do celów aktualizacji lub tworzenia nowych kryteriów stosowanych przy sprawdzaniach dokonywanych na podstawie ust. 3 lit. b) w celu identyfikacji wszystkich osób, które mogą brać udział w przestępstwach terrorystycznych lub w poważnej przestępczości.
3. Dokonując sprawdzenia, o którym mowa w ust. 2 lit. a), JIP może:
 - a) porównywać dane PNR z bazami danych, które mają znaczenie dla zapobiegania przestępstwu terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, w tym z bazami danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem, zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych; lub
 - b) przetwarzać dane PNR według wcześniej ustalonych kryteriów.
4. Sprawdzenie pasażerów przed ich planowym przylotem do lub odlotem z państwa członkowskiego dokonywane na podstawie ust. 3 lit. b) według wcześniej ustalonych kryteriów odbywa się w sposób niedyskryminacyjny. Te ustalone wcześniej kryteria muszą być ukierunkowane, proporcjonalne i szczegółowe. Państwa członkowskie zapewniają, by kryteria te były ustanawiane i poddawane regularnym przeglądom przez JIP we współpracy z właściwymi organami, o których mowa w art. 7. Kryteria te w żadnym przypadku nie mogą opierać się na rasie ani pochodzeniu etnicznym, na poglądach politycznych, przekonaniach religijnych lub światopoglądowych, przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby.
5. Państwa członkowskie zapewniają, by każdy pozytywny wynik automatycznego przetwarzania danych PNR dokonanego na podstawie ust. 2 lit. a) był indywidualnie oceniany w sposób niezautomatyzowany w celu ustalenia, czy właściwy organ, o którym mowa w art. 7, powinien podjąć działania zgodnie z prawem krajowym.
6. JIP w państwie członkowskim przekazuje do dalszego sprawdzenia dane PNR osób zidentyfikowanych zgodnie z ust. 2 lit. a) lub wyniki przetwarzania tych danych właściwym organom, o których mowa w art. 7, w tym samym państwie członkowskim. Przekazywanie to odbywa się wyłącznie na podstawie oceny każdego indywidualnego przypadku, a w przypadku automatycznego przetwarzania danych PNR – po indywidualnej ocenie przeprowadzonej w sposób niezautomatyzowany.
7. Państwa członkowskie zapewniają, by inspektor ochrony danych miał dostęp do wszystkich danych przetwarzanych przez JIP. Jeżeli inspektor ochrony danych uzna, że przetwarzanie jakichkolwiek danych było niezgodne z prawem, może przekazać sprawę do krajowego organu nadzorczego.
8. Przechowywanie, przetwarzanie i analiza danych PNR przez JIP odbywa się wyłącznie w bezpiecznym miejscu lub bezpiecznych miejscach na terytorium państw członkowskich.

9. Skutki sprawdzenia pasażerów, o którym mowa w ust. 2 lit. a) niniejszego artykułu, nie naruszają prawa osób, którym przysługuje unijne prawo do swobodnego przemieszczania się, do wjazdu na terytorium danego państwa członkowskiego, zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2004/38/WE⁽¹⁾. Ponadto, jeżeli sprawdzenie jest dokonywane w odniesieniu do lotów wewnątrzunijnych pomiędzy państwami członkowskimi, do których stosuje się rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 562/2006⁽²⁾, skutki takiego sprawdzenia nie naruszają tego rozporządzenia.

Artykuł 7

Właściwe organy

1. Każde państwo członkowskie sporządza wykaz właściwych organów uprawnionych do występowania do JIP o dane PNR lub o wyniki przetwarzania tych danych lub do otrzymywania takich danych i wyników ich przetwarzania od JIP na potrzeby dalszego sprawdzenia tych informacji lub podjęcia odpowiednich czynności w celu zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.
2. Organy, o których mowa w ust. 1, są organami właściwymi do zapobiegania przestępstwom terrorystycznym lub poważnym przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.
3. Na potrzeby art. 9 ust. 3 każde państwo członkowskie powiadamia Komisję o wykazie swoich właściwych organów do dnia 25 maja 2017 r. oraz może w każdym czasie dokonać zmiany swojego powiadomienia. Komisja publikuje to powiadomienie oraz jego zmiany w *Dzienniku Urzędowym Unii Europejskiej*.
4. Dane PNR oraz wyniki przetwarzania tych danych, otrzymane od JIP, mogą być poddane dalszemu przetwarzaniu przez właściwe organy państw członkowskich wyłącznie do określonych celów, jakimi są zapobieganie przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie lub ich ściganie.
5. Ust. 4 nie narusza określonych prawem krajowym uprawnień organów ścigania i organów wymiaru sprawiedliwości, w przypadku gdy w toku czynności podejmowanych w ramach ścigania przestępstw wykryte zostaną, na podstawie wyników takiego przetwarzania, inne przestępstwa lub okoliczności na nie wskazujące.
6. Właściwe organy nie podejmują żadnych decyzji, które miałyby negatywne skutki prawne dla danej osoby lub znacząco wpływałyby na jej sytuację, wyłącznie na podstawie automatycznego przetwarzania danych PNR. Takie decyzje nie mogą zostać podjęte w oparciu o rasę ani pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne ani orientację seksualną danej osoby.

Artykuł 8

Obowiązki przewoźników lotniczych dotyczące przekazywania danych

1. Państwa członkowskie przyjmują środki niezbędne do zapewnienia, by przewoźnicy lotniczy przekazywali, za pomocą „metody push”, dane PNR wymienione w załączniku I – w zakresie, w jakim już zbierają takie dane w ramach swojej normalnej działalności – do bazy danych JIP w państwie członkowskim, na którego terytorium nastąpi przyloc lub z którego terytorium nastąpi odlot. W przypadku gdy lot odbywa się pod wspólnym kodem jednego lub większej liczby przewoźników lotniczych, obowiązek przekazania danych PNR wszystkich pasażerów uczestniczących w tym locie spoczywa na przewoźniku lotniczym obsługującym lot. Jeżeli lot pozaunijny odbywa się z jednym lub kilkoma postojami na lotniskach państw członkowskich, przewoźnicy lotniczy przekazują dane PNR dotyczące wszystkich pasażerów do JIP we wszystkich odpowiednich państwach członkowskich. Dotyczy to również lotów wewnątrzunijnych z jednym lub kilkoma postojami na lotniskach różnych państw członkowskich, ale wyłącznie w przypadku państw członkowskich, które zbierają dane PNR dotyczące lotów wewnątrzunijnych.

⁽¹⁾ Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium państw członkowskich, zmieniająca rozporządzenie (EWG) nr 1612/68 i uchylająca dyrektywy 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG i 93/96/EWG (Dz.U. L 158 z 30.4.2004, s. 77).

⁽²⁾ Rozporządzenie (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.U. L 105 z 13.4.2006, s. 1).

2. Jeżeli przewoźnicy lotniczy zebrali jakiegokolwiek dane pasażera przekazane przed podróżą (zwane dalej „danymi API”) wymienione w pkt 18 załącznika I, ale nie zatrzymują tych danych za pomocą takich samych technicznych środków jak w przypadku innych danych PNR, państwa członkowskie przyjmują środki niezbędne do zapewnienia, by przewoźnicy lotniczy przekazywali, za pomocą „metody push”, także te dane do JIP w państwach członkowskich, o których mowa w ust. 1. W przypadku takiego przekazania stosuje się do tych danych API wszystkie przepisy niniejszej dyrektywy.
3. Przewoźnicy lotniczy przekazują dane PNR za pomocą środków elektronicznych z wykorzystaniem wspólnych protokołów i obsługiwanych formatów danych, które to protokoły i formaty zostaną określone zgodnie z procedurą sprawdzającą, o której mowa w art. 17 ust. 2, a w przypadku awarii technicznej – innymi właściwymi sposobami zapewniającymi odpowiedni poziom bezpieczeństwa danych:
 - a) 24 do 48 godzin przed planowym odlotem; oraz
 - b) niezwłocznie po zakończeniu odprawy, czyli bezpośrednio po wejściu pasażerów na pokład samolotu przygotowującego się do odlotu, kiedy to pasażerowie nie mogą już wejść na pokład ani go opuścić.
4. Państwa członkowskie zezwalają przewoźnikom lotniczym na ograniczenie przekazywania danych, o którym mowa w ust. 3 lit. b), do aktualizacji przekazania, o którym mowa w lit. a) tego ustępu.
5. Jeżeli dostęp do danych PNR jest niezbędny, by zareagować na konkretne i rzeczywiste zagrożenie związane z przestępstwami terrorystycznymi lub poważną przestępczością, przewoźnicy lotniczy – na podstawie oceny każdego indywidualnego przypadku – przekazują dane PNR w innych terminach niż te, o których mowa w ust. 3, na wniosek JIP zgodny z prawem krajowym.

Artykuł 9

Wymiana informacji między państwami członkowskimi

1. Państwa członkowskie zapewniają, by w odniesieniu do osób zidentyfikowanych przez JIP zgodnie z art. 6 ust. 2 ta JIP przekazywała wszystkie istotne i niezbędne dane PNR lub wyniki przetwarzania tych danych odpowiednim JIP w innych państwach członkowskich. JIP w państwach członkowskich, które otrzymują dane, przekazują otrzymane informacje, zgodnie z art. 6 ust. 6, swoim właściwym organom.
2. JIP w danym państwie członkowskim ma prawo, w razie potrzeby, zwrócić się do JIP w dowolnym państwie członkowskim z wnioskiem o przekazanie jej danych PNR, które są przechowywane w bazie danych tej JIP, a które nie zostały jeszcze poddane depersonalizacji poprzez maskowanie elementów danych na podstawie art. 12 ust. 2, jak również – w razie potrzeby – o przekazanie wyników przetwarzania tych danych, jeżeli już go dokonano zgodnie z art. 6 ust. 2 lit. a). Taki wniosek zawiera należyte uzasadnienie. Może on dotyczyć jednego elementu danych lub kombinacji takich elementów, w zależności od tego, co wnioskująca JIP uważa w konkretnym przypadku za niezbędne do celów zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania. JIP przekazuje wnioskowane informacje tak szybko, jak to wykonalne. Jeżeli wnioskowane dane zostały poddane depersonalizacji poprzez maskowanie elementów danych zgodnie z art. 12 ust. 2, JIP przekazuje pełne dane PNR wyłącznie wtedy, gdy istnieje uzasadnienie, by uznać, że jest to niezbędne do celów określonych w art. 6 ust. 2 lit. b), oraz wyłącznie po otrzymaniu zgody organu, o którym mowa w art. 12 ust. 3 lit. b).
3. Właściwe organy państwa członkowskiego mogą zwrócić się bezpośrednio do JIP w dowolnym państwie członkowskim z wnioskiem o przekazanie im danych PNR przechowywanych w bazie danych tej JIP wyłącznie wtedy, gdy jest to niezbędne w nagłych przypadkach i na warunkach określonych w ust. 2. Wnioski właściwych organów zawierają uzasadnienie. Kopie tych wniosków są zawsze przekazywane do JIP we wnioskującym państwie członkowskim. We wszystkich innych przypadkach właściwe organy składają wnioski za pośrednictwem JIP we własnym państwie członkowskim.
4. W wyjątkowych przypadkach, jeżeli dostęp do danych PNR jest niezbędny, by zareagować na konkretne i rzeczywiste zagrożenie związane z przestępstwami terrorystycznymi lub poważną przestępczością, JIP w danym państwie członkowskim ma prawo zwrócić się do JIP w innym państwie członkowskim z wnioskiem o uzyskanie danych PNR zgodnie z art. 8 ust. 5 i o dostarczenie ich wnioskującej JIP.
5. Do wymiany informacji na podstawie niniejszego artykułu można zastosować dowolny istniejący kanał współpracy między właściwymi organami państw członkowskich. W przypadku wniosków i wymiany informacji używa

się języka, który ma zastosowanie do wybranego kanału współpracy. Państwa członkowskie, dokonując powiadomień zgodnie z art. 4 ust. 5, przekazują Komisji także szczegółowe informacje o punktach kontaktowych, do których można kierować wnioski w nagłych przypadkach. Komisja przekazuje takie szczegółowe informacje państwom członkowskim.

Artykuł 10

Warunki dostępu Europolu do danych PNR

1. Europol jest uprawniony – w granicach swojej właściwości i na potrzeby realizowanych zadań – do zwracania się z wnioskiem o przekazanie danych PNR lub wyników ich przetwarzania od JIP w państwach członkowskich.
2. W indywidualnych przypadkach Europol może, za pośrednictwem jednostki krajowej, zwrócić się drogą elektroniczną do JIP w dowolnym państwie członkowskim z należycie uzasadnionym wnioskiem o przekazanie określonych danych PNR lub wyników przetwarzania tych danych. Europol może zwrócić się z takim wnioskiem, gdy jest to absolutnie niezbędne do wsparcia i wzmocnienia działań państw członkowskich mających na celu zapobieżenie konkretnemu przestępstwu terrorystycznemu lub poważnemu przestępstwu, ich wykrycie, prowadzenie postępowań przygotowawczych w ich sprawie lub ich ściganie, w zakresie, w jakim dane przestępstwo pozostaje w zakresie właściwości Europolu na mocy decyzji 2009/371/WSiSW. Wniosek taki zawiera uzasadnione przesłanki, na podstawie których Europol uważa, że przekazanie danych PNR lub wyników przetwarzania tych danych w istotny sposób przyczyni się do zapobieżenia danemu przestępstwu, wykrycia go lub prowadzenia postępowania przygotowawczego w jego sprawie.
3. Europol informuje inspektora ochrony danych, powołanego zgodnie z art. 28 decyzji 2009/371/WSiSW, o każdej wymianie informacji na podstawie niniejszego artykułu.
4. Wymiana informacji na podstawie niniejszego artykułu odbywa się za pomocą aplikacji sieci bezpiecznej wymiany informacji (SIENA) i zgodnie z decyzją 2009/371/WSiSW. W przypadku wniosków i wymiany informacji używa się języka stosowanego w aplikacji sieci bezpiecznej wymiany informacji (SIENA).

Artykuł 11

Przekazywanie danych do państw trzecich

1. Państwo członkowskie może przekazać państwu trzeciemu dane PNR oraz wyniki przetwarzania takich danych, które są przechowywane przez JIP zgodnie z art. 12, wyłącznie na podstawie oceny każdego indywidualnego przypadku i jeżeli:
 - a) spełnione zostały warunki określone w art. 13 decyzji ramowej 2008/977/WSiSW;
 - b) przekazanie jest niezbędne do celów niniejszej dyrektywy określonych w art. 1 ust. 2;
 - c) państwo trzecie zgadza się, że dane te mogą być przekazane innemu państwu trzeciemu wyłącznie wtedy, gdy jest to absolutnie niezbędne do celów niniejszej dyrektywy określonych w art. 1 ust. 2 oraz wyłącznie za wyraźną zgodą tego państwa członkowskiego; oraz
 - d) spełnione zostały takie same warunki, jak te określone w art. 9 ust. 2.
2. Niezależnie od art. 13 ust. 2 decyzji ramowej 2008/977/WSiSW przekazywanie danych PNR bez uprzedniej zgody państwa członkowskiego, od którego uzyskano te dane, jest dopuszczalne w wyjątkowych okolicznościach, wyłącznie wtedy gdy:
 - a) przekazywanie takie jest istotne, by zareagować na konkretne i rzeczywiste zagrożenie związane z przestępstwami terrorystycznymi lub poważną przestępczością w państwie członkowskim lub państwie trzecim; oraz
 - b) uprzedniej zgody nie można uzyskać na czas.Organ odpowiedzialny za wydanie zgody musi zostać bezzwłocznie poinformowany, a przekazanie danych należycie odnotowane w ewidencji, z zastrzeżeniem możliwości dokonania weryfikacji *ex post*.
3. Państwa członkowskie przekazują dane PNR właściwym organom państw trzecich wyłącznie na warunkach zgodnych z niniejszą dyrektywą i wyłącznie po upewnieniu się, że cel, w jakim odbierający dane mają zamiar wykorzystać dane PNR, jest zgodny z tymi warunkami i gwarancjami.
4. Inspektor ochrony danych w JIP działającej w państwie członkowskim, które przekazało dane PNR, jest powiadamiany za każdym razem, gdy państwo członkowskie przekazuje dane PNR na podstawie niniejszego artykułu.

Artykuł 12

Okres zatrzymania danych i depersonalizacja

1. Państwa członkowskie zapewniają, by dane PNR dostarczone przez przewoźników lotniczych JIP były zatrzymywane w bazie danych JIP przez okres pięciu lat od przekazania ich do JIP w państwie członkowskim, na którego terytorium ma miejsce przylot lub z którego terytorium ma miejsce odlot.
2. Po upływie okresu sześciu miesięcy od przekazania danych PNR, o którym mowa w ust. 1, wszystkie dane PNR zostają poddane depersonalizacji poprzez maskowanie następujących ich elementów mogących posłużyć do bezpośredniej identyfikacji pasażera, którego dotyczą dane:
 - a) imię i nazwisko (imiona i nazwiska), w tym imię i nazwisko innych pasażerów wymienionych w danych PNR oraz liczba pasażerów wymienionych w danych PNR podróżujących razem;
 - b) adres i dane kontaktowe;
 - c) wszystkie informacje o formie płatności, w tym adres na fakturze, o ile zawierają one jakiegokolwiek informacje mogące posłużyć do bezpośredniej identyfikacji pasażera, którego dotyczą dane PNR, lub wszelkich innych osób;
 - d) informacje dotyczące programów lojalnościowych;
 - e) ogólne uwagi, o ile zawierają one informacje mogące posłużyć do bezpośredniej identyfikacji pasażera, którego dotyczą dane PNR; oraz
 - f) wszelkie zebrane dane API.
3. Po upływie okresu sześciu miesięcy, o którym mowa w ust. 2, ujawnienie pełnych danych PNR jest dopuszczalne wyłącznie wtedy, gdy:
 - a) istnieje uzasadnienie, by uznać, że jest to niezbędne do celów określonych w art. 6 ust. 2 lit. b); oraz
 - b) uzyskano zgodę:
 - (i) organu wymiaru sprawiedliwości; lub
 - (ii) innego organu krajowego, który zgodnie z prawem krajowym jest właściwy do ustalenia, czy warunki ujawnienia zostały spełnione, z zastrzeżeniem poinformowania inspektora ochrony danych w JIP oraz dokonania przez tego inspektora ochrony danych weryfikacji *ex post*.
4. Państwa członkowskie zapewniają, by po upływie okresu, o którym mowa w ust. 1, dane PNR zostały usunięte w sposób trwały. Obowiązek ten nie ma wpływu na przypadki, w których określone dane PNR zostały przekazane właściwemu organowi i są wykorzystywane w konkretnej sprawie w celu zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania; w takim przypadku zatrzymanie takich danych przez właściwy organ regulowane jest prawem krajowym.
5. Wyniki przetwarzania, o którym mowa w art. 6 ust. 2 lit. a), są przechowywane przez JIP wyłącznie przez okres niezbędny do poinformowania o pozytywnym wyniku właściwych organów oraz – zgodnie z art. 9 ust. 1 – JIP w pozostałych państwach członkowskich. Jeżeli wynik automatycznego przetwarzania, po indywidualnej ocenie przeprowadzonej w sposób niezautomatyzowany, o której mowa w art. 6 ust. 5, okaże się negatywny, może on mimo to być przechowywany, by zapobiec przyszłym wynikom fałszywie pozytywnym, dopóki dane bazowe nie zostaną usunięte zgodnie z ust. 4 niniejszego artykułu.

Artykuł 13

Ochrona danych osobowych

1. Każde państwo członkowskie zapewnia, by w odniesieniu do wszelkich operacji przetwarzania danych osobowych na podstawie niniejszej dyrektywy, każdemu pasażerowi przysługiwało prawo do ochrony jego danych osobowych, prawo dostępu do tych danych, ich poprawiania, usunięcia i ograniczania oraz prawo do odszkodowania i prawo do sądowych środków ochrony prawnej, odpowiadające prawom ustanowionym w prawie Unii i w prawie krajowym oraz w ramach wdrożenia art. 17, 18, 19 i 20 decyzji ramowej 2008/977/WSiSW. Artykuły te zatem stosuje się.

2. Każde państwo członkowskie stanowi, że przepisy przyjęte w prawie krajowym w ramach wdrożenia art. 21 i 22 decyzji ramowej 2008/977/WSiSW w odniesieniu do poufności przetwarzania oraz bezpieczeństwa danych stosuje się także do wszelkich operacji przetwarzania danych osobowych na podstawie niniejszej dyrektywy.

3. Niniejsza dyrektywa nie ma wpływu na możliwość stosowania dyrektywy Parlamentu Europejskiego i Rady 95/46/WE⁽¹⁾ do przetwarzania danych osobowych przez przewoźników lotniczych, w szczególności w zakresie ich obowiązku podjęcia odpowiednich środków technicznych i organizacyjnych w celu ochrony bezpieczeństwa i poufności danych osobowych.

4. Państwa członkowskie zakazują przetwarzania danych PNR ujawniających rasę lub pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną danej osoby. W przypadku otrzymania przez JIP danych PNR ujawniających takie informacje, dane takie są niezwłocznie usuwane.

5. Państwa członkowskie zapewniają, by JIP prowadziły dokumentację dotyczącą wszystkich systemów i procedur przetwarzania, za które są odpowiedzialne. Dokumentacja ta zawiera co najmniej:

- a) nazwę i dane kontaktowe organizacji oraz imiona i nazwiska i dane kontaktowe personelu JIP, którym powierzono przetwarzanie danych PNR wraz z poszczególnymi poziomami prawa dostępu;
- b) wnioski złożone przez właściwe organy i JIP w innych państwach członkowskich;
- c) wszystkie wnioski o przekazanie i przypadki przekazania danych PNR do państwa trzeciego.

JIP na wniosek krajowego organu nadzorczego udostępnia mu całą dokumentację.

6. Państwa członkowskie zapewniają, by JIP prowadziła ewidencję co najmniej następujących operacji przetwarzania: zbieranie, przeglądanie, ujawnianie i usuwanie. W ewidencji przeglądania i ujawniania podaje się w szczególności cel, datę i godzinę takich operacji oraz, w miarę możliwości, tożsamość osoby, która przeglądała lub ujawniała dane PNR, a także tożsamość odbiorców tych danych. Ewidencja jest wykorzystywana wyłącznie w celu: weryfikacji, monitorowania własnej działalności, zapewnienia integralności i bezpieczeństwa danych lub audytu. JIP, na wniosek krajowego organu nadzorczego, udostępnia mu tę ewidencję.

Ewidencję tę przechowuje się przez okres pięciu lat.

7. Państwa członkowskie zapewniają, by ich JIP wdrożyła odpowiednie środki techniczne i organizacyjne oraz procedury techniczne i organizacyjne, by zapewnić wysoki poziom bezpieczeństwa odpowiedni do zagrożenia związanego z przetwarzaniem danych PNR oraz do charakteru tych danych.

8. Jeżeli naruszenie ochrony danych osobowych może nieść duże zagrożenie dla ochrony danych osobowych lub naruszać prywatność osoby, której dane dotyczą, państwa członkowskie zapewniają, by JIP bez zbędnej zwłoki poinformowała o takim naruszeniu osobę, której dane dotyczą, oraz krajowy organ nadzorczy.

Artykuł 14

Sankcje

Państwa członkowskie ustanawiają przepisy dotyczące sankcji za naruszenie przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszelkie środki niezbędne do zapewnienia ich egzekwowania.

W szczególności państwa członkowskie ustanawiają przepisy dotyczące sankcji, w tym kar finansowych, w stosunku do przewoźników, którzy nie przekazują danych zgodnie z art. 8, lub nie przekazują ich w wymaganym formacie.

Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstrasżające.

⁽¹⁾ Dyrektywa 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 (Dz.U. L 281 z 23.11.1995, s. 31).

*Artykuł 15***Krajowy organ nadzorczy**

1. Każde państwo członkowskie stanowi, że krajowy organ nadzorczy, o którym mowa w art. 25 decyzji ramowej 2008/977/WSiSW, odpowiada za doradztwo i monitorowanie w zakresie stosowania na jego terytorium przepisów przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy. Art. 25 decyzji ramowej 2008/977/WSiSW stosuje się.
2. Te krajowe organy nadzorcze realizują swoje zadania, o których mowa w ust. 1, w celu ochrony praw podstawowych w związku z przetwarzaniem danych osobowych.
3. Każdy krajowy organ nadzorczy:
 - a) rozpatruje skargi złożone przez osoby, których dane dotyczą, bada daną sprawę oraz w rozsądnym terminie informuje osoby, których dane dotyczą, o postępach i wyniku rozpatrzenia ich skarg;
 - b) sprawdza zgodność z prawem przetwarzania danych, prowadzi postępowania, inspekcje i audyty zgodnie z prawem krajowym, z własnej inicjatywy lub na podstawie skargi, o której mowa w lit. a).
4. Każdy krajowy organ nadzorczy doradza, na wniosek, osobie, której dane dotyczą, w sprawie wykonywania praw określonych w przepisach przyjętych na podstawie niniejszej dyrektywy.

ROZDZIAŁ III

Środki wykonawcze*Artykuł 16***Wspólne protokoły i obsługiwane formaty danych**

1. Każde przekazanie danych PNR przez przewoźników lotniczych do JIP do celów niniejszej dyrektywy odbywa się za pomocą środków elektronicznych, które dają wystarczające gwarancje pod względem technicznych środków bezpieczeństwa i środków organizacyjnych regulujących dokonywane przetwarzanie danych. W przypadku awarii technicznej dane PNR mogą być przekazywane wszelkimi innymi odpowiednimi sposobami, pod warunkiem zachowania tego samego poziomu bezpieczeństwa i pełnego poszanowania unijnych przepisów o ochronie danych.
2. Po upływie jednego roku od daty określenia po raz pierwszy przez Komisję zgodnie z ust. 3 wspólnych protokołów i obsługiwanych formatów danych, każde przekazanie danych PNR przez przewoźników lotniczych do JIP do celów niniejszej dyrektywy odbywa się drogą elektroniczną z wykorzystaniem bezpiecznych metod zgodnych z tymi wspólnymi protokołami. Protokoły te są identyczne w przypadku każdego przekazania danych, po to by zapewnić bezpieczeństwo danych PNR podczas ich przekazywania. Dane PNR są przekazywane w obsługiwanej formie danych, po to by zapewnić możliwość ich odczytania przez wszystkie uczestniczące strony. Wszyscy przewoźnicy lotniczy zobowiązani są do wyboru i wskazania JIP wspólnego protokołu i formatu danych, które zamierzają wykorzystywać do przekazywania danych.
3. Komisja, w drodze aktów wykonawczych, sporządza wykaz wspólnych protokołów i obsługiwanych formatów danych oraz w razie potrzeby dostosowuje ten wykaz. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 17 ust. 2.
4. Ust. 1 stosuje się, dopóki nie będą dostępne wspólne protokoły i obsługiwane formaty danych, o których mowa w ust. 2 i 3.
5. W okresie jednego roku od daty określenia wspólnych protokołów i obsługiwanych formatów danych, o których mowa w ust. 2, każde państwo członkowskie zapewnia przyjęcie niezbędnych środków technicznych, by móc korzystać z tych wspólnych protokołów i formatów danych.

*Artykuł 17***Procedura komitetowa**

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.
2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

W przypadku gdy komitet nie wyda żadnej opinii, Komisja nie przyjmuje projektu aktu wykonawczego i stosuje się art. 5 ust. 4 akapit trzeci rozporządzenia (UE) nr 182/2011.

ROZDZIAŁ IV

Przepisy końcowe*Artykuł 18***Transpozycja**

1. Państwa członkowskie wprowadzają w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy do dnia 25 maja 2018 r. Niezwłocznie powiadamiają o tym Komisję.

Przepisy przyjęte przez państwa członkowskie zawierają odesłanie do niniejszej dyrektywy lub odesłanie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odesłania określane są przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji teksty najważniejszych przepisów prawa krajowego z dziedziny objętej niniejszą dyrektywą.

*Artykuł 19***Przegląd**

1. Na podstawie informacji dostarczonych przez państwa członkowskie, w tym informacji statystycznych, o których mowa w art. 20 ust. 2, Komisja w terminie do dnia 25 maja 2020 r. dokonuje przeglądu wszystkich elementów niniejszej dyrektywy oraz przedkłada i przedstawia sprawozdanie Parlamentowi Europejskiemu i Radzie.

2. Dokonując tego przeglądu, Komisja zwraca szczególną uwagę na:

- a) przestrzeganie mających zastosowanie standardów ochrony danych osobowych;
- b) konieczność i proporcjonalność zbierania i przetwarzania danych PNR w odniesieniu do każdego celu określonego w niniejszej dyrektywie;
- c) długość okresu zatrzymania danych;
- d) skuteczność wymiany informacji między państwami członkowskimi; oraz
- e) jakość sprawdzeń, w tym w odniesieniu do informacji statystycznych zgromadzonych na podstawie art. 20.

3. Sprawozdanie, o którym mowa w ust. 1, zawiera również przegląd konieczności, proporcjonalności i skuteczności włączenia do zakresu stosowania niniejszej dyrektywy obowiązkowego zbierania i przekazywania danych PNR w odniesieniu do wszystkich lub wybranych lotów wewnątrzunijnych. Komisja uwzględnia doświadczenia państw członkowskich, zwłaszcza tych, które stosują niniejszą dyrektywę do lotów wewnątrzunijnych zgodnie z art. 2. W sprawozdaniu rozważa się także konieczność włączenia do zakresu stosowania niniejszej dyrektywy podmiotów gospodarczych niebędących przewoźnikami, takich jak biura podróży i organizatorzy wycieczek świadczący usługi turystyczne związane z podróżowaniem, w tym rezerwację lotów.

4. W stosownym przypadku, w świetle przeglądu, dokonanego na podstawie niniejszego artykułu, Komisja przedkłada Parlamentowi Europejskiemu i Radzie wniosek ustawodawczy mający na celu zmianę niniejszej dyrektywy.

Artykuł 20

Dane statystyczne

1. Państwa członkowskie co roku dostarczają Komisji zestaw informacji statystycznych o danych PNR dostarczonych JIP. Statystyki te nie zawierają żadnych danych osobowych.
2. Statystyki te obejmują co najmniej:
 - a) łączną liczbę pasażerów, których dane PNR zostały zebrane i wymienione;
 - b) liczbę pasażerów wytypowanych do dalszego sprawdzenia.

Artykuł 21

Stosunek do innych instrumentów prawnych

1. Państwa członkowskie mogą w dalszym ciągu stosować dwustronne lub wielostronne umowy lub uzgodnienia między nimi dotyczące wymiany informacji między właściwymi organami, które pozostają w mocy w dniu 24 maja 2016 r., o ile takie umowy lub uzgodnienia są zgodne z niniejszą dyrektywą.
2. Niniejsza dyrektywa nie ma wpływu na możliwość stosowania dyrektywy 95/46/WE do przetwarzania danych osobowych przez przewoźników lotniczych.
3. Niniejsza dyrektywa nie ma wpływu na obowiązki i zobowiązania państw członkowskich lub Unii wynikające z dwustronnych lub wielostronnych umów z państwami trzecimi.

Artykuł 22

Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsza dyrektywa skierowana jest do państw członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia 27 kwietnia 2016 r.

W imieniu Parlamentu Europejskiego

M. SCHULZ
Przewodniczący

W imieniu Rady

J.A. HENNIS-PLASSCHAERT
Przewodniczący

ZAŁĄCZNIK I

Dane dotyczące przelotu pasażera zbierane przez przewoźników lotniczych

1. Kod identyfikacyjny danych PNR
 2. Data rezerwacji/wystawienia biletu
 3. Data(-y) planowanej podróży
 4. Imię i nazwisko (imiona i nazwiska)
 5. Adres i dane kontaktowe (numer telefonu, adres e-mail)
 6. Wszystkie informacje o formie płatności, w tym adres na fakturze
 7. Kompletna trasa podróży dla konkretnych danych PNR
 8. Informacje o programach lojalnościowych
 9. Biuro podróży/agencja turystyczna
 10. Dane o statusie podróży pasażera, w tym potwierdzenia, stan odprawy biletowo-bagażowej, dane typu: pasażer nie stawił się lub pasażer nabył bilet w czasie odprawy bez wcześniejszej rezerwacji
 11. Informacje o podzieleniu/rozdzieleniu danych PNR
 12. Uwagi ogólne (w tym wszelkie dostępne informacje o osobach małoletnich bez opieki w wieku poniżej 18 lat, takie jak: imię i nazwisko, płeć, wiek, języki, którymi włada, imię i nazwisko oraz dane kontaktowe opiekuna w momencie odlotu i rodzaj więzi łączącej go z osobą małoletnią, imię i nazwisko oraz dane kontaktowe opiekuna w momencie lądowania i rodzaj więzi łączącej go z osobą małoletnią, przedstawiciel obecny przy odlocie i przylocie)
 13. Informacje o wystawieniu biletu, w tym numer biletu, data wystawienia biletu i bilety w jedną stronę, informacja o automatycznie skalkulowanej taryfie
 14. Numer miejsca na pokładzie i inne informacje o miejscu
 15. Informacje o wspólnej obsłudze połączeń
 16. Wszystkie informacje o bagażu
 17. Liczba oraz imiona i nazwiska innych podróżnych wymienionych w PNR
 18. Wszelkie zebrane dane pasażera przekazane przed podróżą (dane API) (w tym rodzaj, numer, kraj wydania i data ważności dokumentu tożsamości, obywatelstwo, nazwisko, imię, płeć, data urodzenia, linia lotnicza, numer lotu, data odlotu, data przylotu, port lotniczy odlotu, port lotniczy przylotu, godzina odlotu i godzina przylotu)
 19. Wszystkie dotychczasowe zmiany danych PNR wymienionych w pkt 1–18.
-

ZAŁĄCZNIK II

Wykaz przestępstw, o których mowa w art. 3 pkt 9

1. Udział w organizacji przestępczej
 2. Handel ludźmi
 3. Wykorzystywanie seksualne dzieci i pornografia dziecięca
 4. Nielegalny handel narkotykami i substancjami psychotropowymi
 5. Nielegalny handel bronią, amunicją i materiałami wybuchowymi
 6. Korupcja
 7. Oszustwo, w tym oszustwo przeciwko interesom finansowym Unii
 8. Pranie dochodów z przestępstwa i fałszowanie pieniędzy, w tym euro
 9. Przestępczość komputerowa i cyberprzestępczość
 10. Przestępstwa przeciwko środowisku, w tym nielegalny handel zagrożonymi gatunkami zwierząt oraz zagrożonymi gatunkami i odmianami roślin
 11. Ułatwianie bezprawnego wjazdu i pobytu
 12. Zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu
 13. Nielegalny obrót organami i tkankami ludzkimi
 14. Uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładników
 15. Kradzież zorganizowana i rozbój przy użyciu broni
 16. Nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki
 17. Podrabianie i piractwo produktów
 18. Fałszowanie dokumentów urzędowych i handel nimi
 19. Nielegalny handel substancjami hormonalnymi i innymi środkami pobudzającymi wzrost
 20. Nielegalny handel materiałami jądrowymi lub promieniotwórczymi
 21. Zgwałcenie
 22. Przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego
 23. Bezprawne zawładnięcie statkiem powietrznym lub statkiem
 24. Sabotaż
 25. Handel skradzionymi pojazdami
 26. Szpiegostwo przemysłowe.
-