

Sprawa C-215/20

Streszczenie wniosku o wydanie orzeczenia w trybie prejudycjalnym zgodnie z art. 98 § 1 regulaminu postępowania przed Trybunałem Sprawiedliwości

Data wpływu:

19 maja 2020 r.

Oznaczenie sądu odsyłającego:

Verwaltungsgericht Wiesbaden (Niemcy)

Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym:

13 maja 2020 r.

Strona skarżąca:

JV

Strona przeciwna:

Bundesrepublik Deutschland

Przedmiot postępowania głównego

Dopuszczalność przekazywania danych dotyczących przelotu pasażera

Przedmiot i podstawa prawna wniosku o wydanie orzeczenia w trybie prejudycjalnym

Wykładnia prawa Unii, art. 267 Traktatu o funkcjonowaniu Unii Europejskiej (zwanego dalej „TFUE”)

Pytania prejudycjalne

1. Czy 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 przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.U. 2016,

L 119, s. 132; zwana dalej „dyrektywą 2016/681”), zgodnie z którą przewoźnicy lotniczy przekazują kompleksowe dane dotyczące bez wyjątku wszystkich pasażerów do ustanowionych lub wyznaczonych jednostek do spraw informacji o pasażerach (JIP), gdzie dane te bez konkretnej potrzeby są wykorzystywane do zautomatyzowanego porównania z bazami danych i wzorami, a następnie zatrzymywane przez okres 5 lat, jest – przy uwzględnieniu celu tej dyrektywy i wymogów określoności oraz proporcjonalności – zgodna z Kartą prawa podstawowych Unii Europejskiej (zwaną dalej „kartą praw podstawowych”), w szczególności art. 7, 8 i 52 tej karty?

2. W szczególności:

- a) Czy art. 3 pkt 9 dyrektywy 2016/681 w związku z załącznikiem II do tej dyrektywy w zakresie, w jakim regulują, iż pojęcie „poważnej przestępczości” w rozumieniu dyrektywy 2016/681 oznacza przestępstwa wymienione w załączniku II do tej dyrektywy, 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, jest z uwzględnieniem wymogów wystarczającej określoności i proporcjonalności zgodny z art. 7 i 8 karty?
- b) Czy podlegające przekazywaniu dane dotyczące przelotu pasażera (zwane dalej „danymi PNR”) w zakresie, w jakim dotyczą imienia i nazwiska (imion i nazwisk) (art. 8 ust. 1 zdanie pierwsze w związku z pkt 4 załącznika I do dyrektywy 2016/681), programów lojalnościowych (art. 8 ust. 1 zdanie pierwsze w związku z pkt 8 załącznika I do dyrektywy 2016/681) oraz wpisów uwag ogólnych w wolnym polu tekstowym (art. 8 ust. 1 zdanie pierwsze w związku z pkt 12 załącznika I do dyrektywy 2016/681), są na tyle wystarczająco określone, żeby usprawiedliwić ingerencję w prawa przewidziane w art. 7 i 8 karty praw podstawowych?
- c) Czy zgodne z art. 7 i 8 karty praw podstawowych oraz celem dyrektywy 2016/681 jest to, że poza danymi dotyczącymi pasażerów zbierane są także dane podmiotów trzecich, np. biur podróży/agencji turystycznych (pkt 9 załącznika I do dyrektywy 2016/681), opiekunów osób małoletnich (pkt 12 załącznika I do dyrektywy 2016/681) i innych podróżnych wymienionych w PNR (pkt 17 załącznika I do dyrektywy 2016/681)?
- d) Czy dyrektywa 2016/681 w zakresie, w jakim zgodnie z jej przepisami przekazywane, przetwarzane i zatrzymywane są dane PNR pasażerów małoletnich, jest zgodna z art. 7, 8 i 24 karty praw podstawowych?
- e) Czy art. 8 ust. 2 dyrektywy 2016/681 w związku z pkt 18 załącznika I do dyrektywy 2016/681, zgodnie z którym dane API podlegają przekazaniu przez przewoźnika lotniczego do JIP w państwie członkowskim także

wtedy, gdy są identyczne z danymi PNR, jest, przy uwzględnieniu zasady minimalizacji danych, zgodny z art. 8 i 52 karty praw podstawowych?

- f) Czy art. 6 ust. 4 dyrektywy 2016/681 jako podstawa prawna dla określenia kryteriów, według których porównywane są dane (tzw. wzorów), stanowi wystarczającą podstawę prawną przewidzianą ustawą w rozumieniu art. 8 ust. 2 i art. 52 karty praw podstawowych oraz art. 16 ust. 2 TFUE?
 - g) Czy art. 12 dyrektywy 2016/681 ogranicza ingerencję w art. 7 i 8 karty praw podstawowych do tego, co jest absolutnie konieczne, skoro przekazywane dane są przechowywane przez JIP w państwach członkowskich przez pięć lat?
 - h) Czy depersonalizacja na podstawie art. 12 ust. 2 dyrektywy 2016/681 prowadzi do zmniejszenia ilości danych osobowych do poziomu wymaganego na podstawie art. 8 i 52 karty praw podstawowych, skoro w jej przypadku chodzi o nic innego, jak tylko o możliwość do odwrócenia w każdym czasie pseudonimizację?
 - i) Czy art. 7, 8 i 47 karty praw podstawowych należy interpretować w ten sposób, że wymagają one, by pasażerowie, których dane zostały ponownie ujawnione w trakcie przetwarzania danych PNR (art. 12 ust. 3 dyrektywy 2016/681), zostali o tym poinformowani i w ten sposób uzyskali możliwość poddania ujawnienia danych kontroli sądowej?
3. Czy art. 11 dyrektywy 2016/681 w zakresie, w jakim pozwala na przekazywanie danych PNR państwom trzecim, które nie zapewniają odpowiedniego poziomu ochrony danych, jest zgodny z art. 7 i 8 karty praw podstawowych?
4. Czy art. 6 ust. 4 zdanie czwarte dyrektywy 2016/681 zapewnia wystarczającą ochronę przed przetwarzaniem szczególnych kategorii danych osobowych w rozumieniu art. 9 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1; zwanego dalej „RODO”) i art. 10 dyrektywy Parlamentu Europejskiego i Rady (UE) nr 2016/680 z dnia 27 czerwca 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 1; zwanej dalej „dyrektywą 2016/680”), w sytuacji gdy w wolnym polu tekstowym „Uwagi ogólne” (pkt 12 załącznika I do dyrektywy 2016/681) mogą zostać wpisane przykładowo informacje o preferencjach dotyczących

posiłków, które pozwalają na wyciągnięcie wniosków dotyczących takich szczególnych kategorii danych osobowych?

5. Czy w zgodzie z art. 13 RODO pozostaje sytuacja, w której pasażerowie są informowani przez przewoźnika lotniczego na jego stronie internetowej wyłącznie o krajowej ustawie transponującej dyrektywę {tu: Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) [ustawa o przetwarzaniu danych dotyczących przelotu pasażera w celu transpozycji dyrektywy (UE) 2016/681 (ustawa o danych dotyczących przelotu pasażera)] z dnia 6 czerwca 2017 r., BGBl. I s. 1484, zwana dalej „FlugDaG”}?

Właściwe przepisy prawa Unii

Karta praw podstawowych Unii Europejskiej (zwana dalej „kartą praw podstawowych”), art. 7, 8, 24, 47 i 52

Artykuł 16 TFUE

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 przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.U. 2016, L 119, s. 132; zwana dalej „dyrektywą 2016/681”)

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 89; zwana dalej „dyrektywą 2016/680”)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1; zwane dalej „RODO”)

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. 1995, L 283, s. 31; zwana dalej „dyrektywą 95/46”)

Właściwe przepisy prawa krajowego

Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 [ustawa o przetwarzaniu danych dotyczących przelotu pasażera w celu transpozycji dyrektywy (UE) 2016/681, zwana dalej „FlugDaG”]

Zwięzły opis stanu faktycznego i przebiegu postępowania

- 1 W dniu 10 czerwca 2017 r. weszła w życie FlugDaG, mocą której transponowano do prawa niemieckiego dyrektywę 2016/681. Dyrektywa ta reguluje przekazywanie danych PNR w przypadku lotów z państw członkowskich Unii do państw trzecich i z państw trzecich do państw członkowskich Unii, jak również przetwarzanie takich danych.
- 2 Zgodnie z jej art. 1 ust. 2, celem dyrektywy 2016/681 jest zapobieganie przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie. Na podstawie art. 4 dyrektywy państwa członkowskie są zobowiązane do ustanowienia lub wyznaczenia tzw. jednostek do spraw informacji o pasażerach (zwanej dalej „JIP”), odpowiedzialnych za zbieranie od przewoźników lotniczych danych PNR, ich przechowywanie i przetwarzanie oraz za przekazywanie tych danych lub wyników ich przetwarzania właściwym organom, jak również za wymianę zarówno danych PNR, jak i wyników ich przetwarzania. Zgodnie z art. 8 w związku z załącznikiem I do dyrektywy 2016/681 państwa członkowskie zobowiązują przewoźników lotniczych do przekazywania określonych danych PNR do JIP w państwie członkowskim, na którego terytorium nastąpi przylot lub z którego terytorium nastąpi odlot. Zgodnie z art. 9 dyrektywy 2016/681 państwa członkowskie mogą żądać danych PNR od siebie nawzajem i nawzajem przekazywać sobie takie dane. W razie spełnienia przesłanek z art. 11 dyrektywy 2016/681 dopuszczalne jest również przekazywanie danych do państw trzecich. Zgodnie z art. 12 ust. 2 dyrektywy 2016/681 zatrzymane dane dotyczące pasażerów, które podlegają zatrzymaniu na okres 5 lat, zostają poddane „depersonalizacji” po upływie 6 miesięcy, co oznacza, że elementy danych, mogące posłużyć do bezpośredniej identyfikacji pasażera, zostają zamaskowane. Jednakże możliwe jest również ujawnienie tych zdepersonalizowanych elementów danych w razie spełnienia przesłanek z art. 12 ust. 3 dyrektywy 2016/681. Artykuł 6 dyrektywy reguluje przetwarzanie danych, w szczególności w drodze zautomatyzowanego porównania ich z bazami danych i przetwarzania według wcześniej ustalonych kryteriów (FlugDaG posługuje się w odniesieniu do tych kryteriów pojęciem „Muster” – „wzór”).
- 3 W dniu 28 kwietnia 2019 r. skarżący poleciał z przewoźnikiem lotniczym Lufthansa z Frankfurtu nad Menem (Niemcy) do Bogoty (Kolumbia), a w dniu 7 maja 2019 r. z Rio de Janeiro (Brazylia) z powrotem do Frankfurtu nad Menem. W odniesieniu do tych lotów skarżący domaga się usunięcia swoich danych przez stronę przeciwną.

Zwięzłe wskazanie przyczyn wystąpienia z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym

- 4 Rozstrzygnięcie sprawy w postępowaniu głównym zależy od ustalenia, czy dyrektywa 2016/681 w całości lub w części jest sprzeczna z postanowieniami karty praw podstawowych. Gdyby tak było, FlugDaG jako ustawa transponująca dyrektywę nie znajdowałaby zastosowania, a w konsekwencji sporne przetwarzanie danych byłoby niedopuszczalne i skarżącemu przysługiwałoby roszczenie o usunięcie danych.

W przedmiocie pytania pierwszego: Czy dyrektywa 2016/681 jest generalnie zgodna z kartą?

- 5 Różne sposoby przetwarzania danych PNR przewidziane w dyrektywie 2016/681 i FlugDaG naruszają zakres ochrony podstawowego prawa do poszanowania życia prywatnego zagwarantowanego w art. 7 karty praw podstawowych. Prawo to rozciąga się bowiem na każdą informację, która dotyczy zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (zob. wyrok z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, pkt 52), a więc również na wymienione w załączniku I do dyrektywy 2016/681 informacje o osobach, których dotyczy przetwarzanie danych PNR. Ponadto sposoby przetwarzania danych osobowych, o których mowa w dyrektywie 2016/681, wchodzą w zakres zastosowania art. 8 karty praw podstawowych z tego powodu, że chodzi o przetwarzanie danych osobowych w rozumieniu tego artykułu, a w związku z tym konieczne jest spełnienie wynikających z tego artykułu wymogów w zakresie ochrony danych (zob. opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 123).
- 6 Zgodnie z orzecznictwem Trybunału udostępnianie danych osobowych podmiotowi trzeciemu takiemu jak organ rządowy stanowi ingerencję w prawo podstawowe gwarantowane w art. 7 karty praw podstawowych, niezależnie od tego, w jaki sposób dane te zostaną później wykorzystane. To samo dotyczy zatrzymania danych osobowych, jak również dostępu do tych danych w celu ich wykorzystania przez organy rządowe. W tym względzie nie ma znaczenia okoliczność, czy informacje związane z życiem prywatnym mają charakter szczególnie chroniony, ani też to, czy też ze względu na tę ingerencję zainteresowane osoby doświadczyły ewentualnych niedogodności (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124). Sytuacja ma się analogicznie w odniesieniu do art. 8 karty praw podstawowych w zakresie, w jakim mamy do czynienia z przetwarzaniem danych osobowych (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 126).
- 7 Prawdą jest, że prawa gwarantowane w art. 7 i 8 karty praw podstawowych nie stanowią prerogatyw o charakterze absolutnym, lecz powinny być oceniane w świetle ich funkcji społecznej (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 136). Ograniczenie tych praw w pełni uzasadnia realizacja celów interesu ogólnego Unii, w tym w postaci zwalczania terroryzmu oraz

poważnej przestępczości międzynarodowej (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 149). Ingerencje w prawa podstawowe muszą być jednak odpowiednie i konieczne do osiągnięcia tych celów i nie mogą okazać się nieproporcjonalne sensu stricto. Ponadto zgodnie z art. 52 ust. 1 karty praw podstawowych wszelkie ograniczenia w korzystaniu z uznanych w niej praw i wolności muszą być przewidziane ustawą i szanować ich istotę. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 138).

- 8 Zgodnie z utrwalonym orzecznictwem Trybunału zasada proporcjonalności wymaga, by akty prawne instytucji Unii były odpowiednie do realizacji uzasadnionych celów, którym akty te służą, i nie wykroczyły poza to, co jest konieczne do ich osiągnięcia (wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 46). Co się tyczy prawa do poszanowania życia prywatnego, zgodnie z orzecznictwem Trybunału ochrona tego prawa wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne (wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 52).
- 9 Żeby zadośćuczynić przywołanym wymogom przepisy, które przewidują ingerencję, muszą zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania przewidywanych środków, a także ustanawiać wymogi minimalne. Osoby, których dane zostały przekazane, muszą mieć wystarczające gwarancje rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć. Przepisy takie muszą w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać użyty środek, który przewiduje przetwarzanie takich danych, a to celem zagwarantowania, że ingerencja ogranicza się do tego, co absolutnie konieczne. Konieczność zapewnienia takich gwarancji ma znaczenie tym większe, gdy dane osobowe przetwarzane są w sposób zautomatyzowany. Jest tak w szczególności wtedy, gdy chodzi o ochronę szczególnej kategorii danych osobowych wrażliwych (wyrok z dnia 8 kwietnia 2014 r. w sprawach połączonych Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 54 i nast.).
- 10 Istnieją poważne wątpliwości co do tego, czy dyrektywa 2016/681 spełnia wszystkie te wymogi.
- 11 Zgodnie z przepisami dyrektywy 2016/681 przewoźnicy lotniczy są zobowiązani do przekazywania danych PNR wszystkich pasażerów, bez wyjątku, dla każdego lotu, do JIP w państwach członkowskich, gdzie dane te są przetwarzane w sposób zautomatyzowany i na stałe zatrzymywane. Nie jest konieczne istnienie szczególnej potrzeby, np. konkretnych poszlak związku z międzynarodowym terroryzmem lub zorganizowaną przestępczością. Prowadzi to do tego, że w krótkich okresach czasu setki miliardów danych są przetwarzane

i zatrzymywane. „Zatrzymywanie na zapas danych” dotyczących przelotu pasażera dotyczy zatem w oczywisty sposób praw podstawowych bardzo dużej części całego społeczeństwa europejskiego.

- 12 Dane, które podlegają przekazywaniu, określone w art. 8 ust. 1 zdanie pierwsze w związku z załącznikiem I do dyrektywy 2016/681, są bardzo obszerne i obejmują nie tylko nazwiska i adresy pasażerów oraz całą trasę podróży, ale także informacje o ich bagażu, współpodróżnych, wszelkiego rodzaju informacje o płatnościach i bliżej nieokreślone „uwagi ogólne”. Na podstawie tych wszystkich danych można wyciągnąć bardzo dokładne wnioski na temat życia prywatnego i zawodowego osób, których dane dotyczą. Wynika z nich bowiem, kto, kiedy, z kim i dokąd podróżował, jakich środków płatności przy tym używał, jakie dane kontaktowe zostały podane i czy konkretna osoba podróżowała z lekkim czy ciężkim bagażem. Wolne pole tekstowe „uwagi ogólne” może być wykorzystane do uzyskania dalszych danych, których zakres jest zupełnie niejasny (patrz poniżej).
- 13 Sąd odsyłający dostrzega porównywalność przetwarzania i zatrzymywania danych PNR z zatrzymywaniem (retencją) danych w sektorze telekomunikacyjnym. Co do tego drugiego Trybunał wyjaśnił, że zatrzymywanie (retencja) danych stanowi szczególnie daleko posuniętą ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty praw podstawowych. Zatrzymywanie w ogromnym zakresie i bez konkretnej potrzeby obszernych danych, które pozwalają na poczynienie wniosków co do życia prywatnego i zawodowego osób, których te dane dotyczą, może bowiem wywołać u tych osób poczucie, że podlegają stałemu nadzorowi (wyrok z dnia 8 kwietnia 2014 r., *Digital Rights Ireland i in.*, C-293/12 i C-594/12, EU:C:2014:238, pkt 37).
- 14 W swoim pierwszym wyroku dotyczącym zatrzymywania (retencji) danych Trybunał uznał je za sprzeczne z prawami podstawowymi m.in. z tej przyczyny, że dane zatrzymywane są niejako „na zapas” nawet wtedy, gdy wobec danej osoby nie ma żadnych podstaw mogących sugerować, że jej zachowanie może mieć związek, nawet pośredni i daleki, z poważnymi przestępstwami (wyrok z dnia 8 kwietnia 2014 r., *Digital Rights Ireland i in.*, C-293/12 i C-594/12, EU:C:2014:238, pkt 58). Dotyczy to również przetwarzania i przechowywania danych PNR, co pokazuje, że przepisy dyrektywy 2016/681 wykraczają poza granice tego, co jest konieczne do osiągnięcia celów tej dyrektywy, a zatem są nieproporcjonalne w rozumieniu orzecznictwa Trybunału. Ponadto, w przeciwieństwie do danych o ruchu telekomunikacyjnym w kontekście zatrzymywania (retencji) danych, dane PNR nie tylko są przechowywane bez konkretnej potrzeby, ale są również dalej przetwarzane, to znaczy w sposób zautomatyzowany porównywane z bazami danych i tzw. „wzorami”.

W przedmiocie pytania drugiego lit. a): pojęcie „poważnej przestępczości”

- 15 Wątpliwości istnieją również co do określoności i proporcjonalności zbierania i przetwarzania danych PNR w odniesieniu do czynów zabronionych, które w ten

sposób mają być zwalczane. Deklarowanym celem dyrektywy 2016/681 jest zapobieganie, wykrywanie, prowadzenie postępowań przygotowawczych i ściganie przestępstw terrorystycznych i poważnej przestępczości. Artykuł 3 pkt 9 dyrektywy definiuje „poważną przestępczość” jako 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. Załącznik II do dyrektywy 2016/681 zawiera wykaz 26 czynów zabronionych zgodnie z art. 3 pkt 9, w tym np. korupcję (nr 6), oszustwo (nr 7), przestępczość komputerową i cyberprzestępczość (nr 9) i przestępstwa przeciwko środowisku (nr 10).

- 16 Po pierwsze, wątpliwa jest określoność tych przepisów. Przykładowo niemieckie prawo karne nie zna przestępstwa „korupcji”, ale raczej jest to ogólny termin określający wiele różnych przestępstw. To samo dotyczy terminów „oszustwo”, „przestępczość komputerowa” i „przestępstwa przeciwko środowisku”.
- 17 Okoliczność ta wraz z odniesieniem w art. 3 pkt 9 dyrektywy 2016/681 do wymiaru kar stosowanych w każdym państwie członkowskim prowadzi do sytuacji, w której dane PNR są wykorzystywane w różny sposób w różnych państwach członkowskich Unii. Pozostawia się bowiem w gestii poszczególnych państw członkowskich to, czy na skutek przyjęcia konkretnego zagrożenia karą w krajowych kodeksach karnych pewne czyny zabronione będą kwalifikowane jako „poważna przestępczość” w rozumieniu dyrektywy czy też nie.
- 18 Ponadto wątpliwości z perspektywy odpowiedniości przepisów budzi ustalona w art. 3 pkt 9 dyrektywy 2016/681 granica zagrożenia karą w maksymalnej wysokości co najmniej trzech lat pozbawienia wolności. Zgodnie z niemieckim prawem karnym przepis w tym kształcie obejmuje ogromną liczbę czynów zabronionych, których zakwalifikowanie jako „poważnej przestępczości” wydaje się bardzo wątpliwe. Przykładowo zgodnie z § 263 Strafgesetzbuch (niemieckiego kodeksu karnego, zwanego dalej „StGB”), zagrożenie karą w przypadku zwykłego oszustwa sięga do pięciu lat pozbawienia wolności. To samo dotyczy na przykład paserstwa (§ 259 StGB), oszustwa komputerowego (§ 263a StGB) lub sprzeniewierzenia (§ 266 StGB). Wszystkie te czyny zabronione można zaliczyć do kategorii przestępstw wymienionych w załączniku II do dyrektywy 2016/681 (w szczególności jako „oszustwa” zgodnie z pkt 7). Tego rodzaju czyny zabronione należą jednak do często występujących „przestępstw pospolitych” i mogą występować również w przypadkach mniejszej wagi. W takim zaś wypadku objęcie ich zakresem zastosowania dyrektywy 2016/681 nie ma nic wspólnego z zapobieganiem i ściganem poważnej przestępczości.

W przedmiocie pytania drugiego lit. b): określoność danych PNR

- 19 Z uwzględnieniem okoliczności, że Trybunał wymaga jasnych i precyzyjnych reguł dotyczących zakresu i sposobu stosowania konkretnych środków [mogących powodować ingerencję w prawa podstawowe] (zob. opinia 1/15 z dnia 26 lipca

2017 r., EU:C:2017:592, pkt 141), wskazać należy, że niektóre dane PNR, które mają być przekazywane przez przewoźników lotniczych do JIP w państwach członkowskich, nie zostały wystarczająco dokładnie określone w załączniku I do dyrektywy 2016/681.

- 20 Nie jest jasne, co należy rozumieć pod pojęciem „Imię i nazwisko (imiona i nazwiska)” [w niemieckiej wersji językowej wyłącznie „Name(n)”], które mają być podane zgodnie z pkt 4 załącznika I do dyrektywy 2016/681. Problem ilustruje wynik niemieckiej transpozycji dyrektywy, gdzie w § 2 pkt 1 i 9 FlugDaG zapytuje się o nazwisko [rodowe albo przyjęte wskutek zmiany nazwiska], nazwisko panińskie, imiona oraz ewentualny stopień naukowy doktora i inne dane dotyczące nazwiska. W codziennej praktyce na pytanie o nazwisko zwykle nie podaje się również nazwiska panińskiego. W związku z tym nie jest jasne, czy nazwisko panińskie wchodzi w zakres pojęcia „Imię i nazwisko (imiona i nazwiska)” zgodnie z pkt 4 załącznika I do dyrektywy 2016/681. Wątpliwe jest również, czy stopień naukowy należy uznać za element imienia i nazwiska w rozumieniu dyrektywy.
- 21 Niewystarczająco określona jest również regulacja co do przekazywania i przetwarzania danych dotyczących programów lojalnościowych (pkt 8 załącznika I do dyrektywy 2016/681). W szczególności nie jest jasne, czy chodzi tylko o udział w programach lojalnościowych dla często podróżujących pasażerów, czy też o konkretne informacje o lotach i rezerwacjach osoby uczestniczącej w takim programie.
- 22 Sformułowanie „Uwagi ogólne [w tym (...)]” w pkt 12 załącznika I do dyrektywy 2016/681 jest bardzo szerokie i nieprecyzyjne. Użycie sformułowania „w tym” wskazuje na to, że jest to tylko przykładowe, niewyczerpujące wyliczenie. Ponadto wskutek wypełnienia tego wolnego pola tekstowego może dojść do przekazania informacji, które nie pozostają w żadnym związku z celem przekazywania danych PNR (tak już w opinii 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 160). Użycie tego sformułowania mogłoby w szczególności doprowadzić do przekazania informacji, na które nie ma pozwolenia w dyrektywie 2016/681, a mianowicie danych wrażliwych, które zgodnie z motywem 15 dyrektywy 2016/681 nie powinny być gromadzone (zobacz w tym kontekście również pytanie czwarte).

W przedmiocie pytania drugiego lit. c): osoby trzecie, których dane dotyczą

- 23 Zgodnie z art. 1 ust. 1 dyrektywy 2016/681 reguluje ona przekazywanie przez przewoźników lotniczych danych PNR dotyczących pasażerów lotów pozaunijnych oraz przetwarzanie tych danych przez państwa członkowskie. Zgodnie z art. 3 pkt 4 dyrektywy 2016/681 „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. W załączniku I do dyrektywy 2016/681 wskazuje się jednak wiele danych

podlegających przekazaniu, które nie dotyczą tak zdefiniowanych „pasażerów”. W tym zakresie przepisy dyrektywy są wewnętrznym sprzeczne.

- 24 I tak sprzeczne z art. 3 pkt 4 dyrektywy 2016/681 jest wyrażone w pkt 9 załącznika I do dyrektywy 2016/681 wymaganie, żeby w ramach przetwarzania danych dotyczących pasażera zebrano także dane dotyczące biura podróży lub agencji turystycznej. Zgodnie z pkt 12 załącznika I do dyrektywy 2016/681 w wolnym polu tekstowym „Uwagi ogólne” wskazać należy natomiast w szczególności informacje o opiece osoby małoletniej w momencie odlotu i przyłotu oraz towarzyszącym przedstawicieli lotniska.
- 25 Jasne jest, że wszystkie te przywołane dane nie dotyczą grupy pasażerów w rozumieniu art. 3 pkt 4 dyrektywy 2016/681. Mimo to muszą być przekazywane przez przewoźników lotniczych do JIP w państwach członkowskich i tam zatrzymywane. Mając to na uwadze, sąd odsyłający uważa, że omawiane przepisy nie ograniczają się do tego, co jest absolutnie konieczne w rozumieniu orzecznictwa Trybunału (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 141). Dodatkowo w przypadku wszystkich osób trzecich, których dotyczą dane, pojawia się pytanie o to, w jaki sposób powinny być one informowane o przetwarzaniu ich danych osobowych zgodnie z art. 14 RODO.
- 26 Zgodnie z pkt 17 załącznika I do dyrektywy 2016/681 przekazaniu i przetwarzaniu podlegać powinny także dane PNR innych podróżnych wymienionych w danych PNR dotyczących pasażera. W przypadku współpodróżujących prowadzi to do podwójnego zebrania danych, ponieważ jako pasażerowie i tak są oni poddani przetwarzaniu danych dotyczących przelotu pasażera. W ten sposób dochodzi do rażącego naruszenia nakazu minimalizacji danych [zobacz art. 5 ust. 1 lit. c) RODO].

W przedmiocie pytania drugiego lit. d): osoby małoletnie

- 27 Zgodnie z dyrektywą 2016/681 przewoźnicy lotniczy przekazują poszczególnym JIP w państwach członkowskich dane PNR odnoszące się do wszystkich pasażerów, bez wyjątku. Dotyczy to zatem również pasażerów będących osobami małoletnimi.
- 28 Dane dotyczące osób małoletnich mogą być przetwarzane z jednej strony w celu zastosowania środków zapobiegawczych lub represyjnych wobec osób małoletnich, które (hipotetycznie) są zaangażowane w działalność terrorystyczną lub poważną przestępczość, a z drugiej strony ze względów związanych z ochroną osób małoletnich, na przykład w celu wykrywania lub ścigania handlu dziećmi. Te dwa różne cele wymagają zróżnicowanych regulacji prawnych. Pogląd ten znajduje dodatkowe potwierdzenie w art. 6 dyrektywy 2016/680, który stanowi, że w miarę możliwości należy dokonać wyraźnego rozróżnienia między danymi osobowymi poszczególnych kategorii osób, których dane dotyczą. Te podlegające rozróżnieniu kategorie obejmują w szczególności osoby, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają

popęlnić czyn zabroniony [art. 6 lit. a) dyrektywy 2016/680] oraz pokrzywdzeni czynem zabronionym lub osoby, w przypadku których określone fakty wskazują, że mogą stać się ofiarą czynu zabronionego [art. 6 lit. c) dyrektywy 2016/680].

- 29 W przypadku gdy dane są zbierane i przetwarzane w celu podjęcia działań represyjnych lub zapobiegawczych wobec osób małoletnich, należy nadto zauważyć, że ściganie oparte na ustaleniach z przetwarzania danych pasażerów jest możliwe jedynie w przypadku osób małoletnich, które osiągnęły już wiek, w którym możliwie jest przypisanie odpowiedzialności karnej. W tym kontekście dyrektywa 2016/681 wykracza poza to, co jest absolutnie konieczne, ponieważ nie zawiera ograniczenia do danych osób małoletnich, które ze względu na wiek mogą ponosić odpowiedzialność karną.
- 30 W odniesieniu do zbierania i przetwarzania danych PNR do celów ochrony osób małoletnich należy zauważyć, że dzieci i młodzież potrzebują szczególnej ochrony. Zostało to jasno wyrażone w art. 24 karty praw podstawowych, który przyznaje im na gruncie prawa Unii własne prawa podstawowe właśnie w celu zapewnienia im szczególnej ochrony. Ta szczególna potrzeba ochrony dotyczy również przetwarzania danych osobowych. W zakresie, w jakim zbieranie i przetwarzanie danych PNR dotyczących osób małoletnich ma na celu zapobieganie przestępstwom przeciwko dzieciom lub ich ściganie, przepisy dyrektywy 2016/681 nie wydają się odpowiednie. Celem przetwarzania danych PNR jest wykrycie lub identyfikacja osób podejrzanych. Dlatego dane PNR są w sposób zautomatyzowany porównywane z bazami danych i wzorami, co ma doprowadzić do identyfikacji osób podejrzanych (zobacz art. 6 ust. 2 dyrektywy 2016/681). W kontekście ochrony osób małoletnich przed handlem dziećmi wskazać jednak należy, że dane tych osób nie są przecież danymi osób podejrzanych, lecz przeciwnie, osób potrzebujących ochrony. Dlatego też powinny być one traktowane inaczej. Nie ma w takiej sytuacji w ogóle potrzeby dopasowywania tych danych do wzorów. W tym względzie oczywiste jest, że w dyrektywie 2016/681 brakuje wystarczająco zróżnicowanych przepisów w odniesieniu do przetwarzania danych PNR osób małoletnich.

W przedmiocie pytania drugiego lit. e): dane API

- 31 Artykuł 8 ust. 2 dyrektywy 2016/681 stanowi, że państwa członkowskie przyjmują środki niezbędne do zapewnienia, żeby wszelkie zebrane dane pasażera przekazane przed podróżą w rozumieniu pkt 18 załącznika I do tej dyrektywy (zwane dalej „danymi 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, były przekazywane do JIP. W tym zakresie wielokrotnie dochodzi do nakładania się danych API oraz i tak podlegających przekazaniu danych PNR, w tym co do dat planowanej podróży (pkt 3 załącznika I do dyrektywy 2016/681), imion i nazwisk (pkt 4 załącznika I do dyrektywy 2016/681) oraz kompletnej trasy podróży (pkt 7 załącznika I do dyrektywy 2016/681).

- 32 Takie podwójne przetwarzanie danych dotyczących lotów pasażerów stoi w sprzeczności m.in. z wyrażoną w dyrektywie 2016/680 zasadą minimalizacji danych. Zasadę tę można wyprowadzić, po pierwsze, z art. 4 ust. 1 lit. c) dyrektywy 2016/680, który stanowi, że dane osobowe nie powinny być nienadmierne do celów, dla których są przetwarzane. Artykuł 20 ust. 1 dyrektywy 2016/680 konkretyzuje tę zasadę w ten sposób, że państwa członkowskie mają obowiązek zapewnienia, by administrator wdrożył odpowiednie środki celem skutecznej realizacji zasad ochrony danych, w tym zasady minimalizacji danych. Ponadto art. 20 ust. 2 dyrektywy 2016/680 stanowi, że przetwarzane powinny być wyłącznie te dane osobowe, których przetwarzanie jest niezbędne dla każdego konkretnego celu przetwarzania.

W przedmiocie pytania drugiego lit. f): podstawa prawna dla wzorów

- 33 Zgodnie z art. 6 ust. 3 lit. b) dyrektywy 2016/681 dane przekazywane przez przewoźników lotniczych do JIP w państwach członkowskich powinny być porównywane według wcześniej ustalonych kryteriów (na gruncie FlugDaG określanych mianem wzorów). Z art. 6 ust. 4 zdania drugie i czwarte dyrektywy 2016/681 wynika, że te wcześniej ustalone kryteria muszą być ukierunkowane, proporcjonalne i szczegółowe i 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. Zgodnie z art. 6 ust. 4 zdanie trzecie dyrektywy 2016/681 ustanawianie kryteriów należy do zadań poszczególnych JIP w państwach członkowskich.
- 34 Ukształtowanie systemu porównywania danych przy pomocy wzorów jest tym samym całkowicie pozostawione w gestii władz wykonawczych poszczególnych państw członkowskich. Musi to skutkować tym, że państwa członkowskie Unii stosują różne wzory, a tym samym w zależności od celu podróży dane pasażerów są poddawane porównaniom na podstawie różnych wzorów, co może prowadzić do całkowicie odmiennych rezultatów.
- 35 Należy zadać pytanie, czy jest to zgodne z art. 8 ust. 2 i art. 52 karty praw podstawowych oraz art. 16 ust. 2 TFUE. Zgodnie z art. 8 ust. 2 karty praw podstawowych dane osobowe muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Stosownie do art. 52 ust. 1 zdanie pierwsze karty praw podstawowych wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w karcie muszą być przewidziane ustawą. W myśl art. 16 ust. 2 TFUE Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii.

- 36 Usprawiedliwienie ingerencji w gwarantowane prawem Unii prawa podstawowe wymaga nie tylko istnienia jakiegokolwiek podstawy ustawowej, ale podstawa ta musi być wystarczająco określona (zobacz wyrok z dnia 21 grudnia 2016 r., AGET Iraklis, C-201/15, EU:C:2016:972, pkt 99). Adresat ustawy musi być w stanie przewidzieć jej skutki, przy czym regulacja o charakterze ogólnym jest dopuszczalna, jeżeli nie jest możliwe bardziej precyzyjne uregulowanie danego zagadnienia ustawowego (wyrok z dnia 20 maja 2003 r., Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 77).
- 37 Tych wymogów nie spełnia art. 6 ust. 4 dyrektywy 2016/681. Artykuł 6 ust. 4 zdanie drugie tej dyrektywy jest niejasny i na jego podstawie tworzone jest jedynie wrażenie istnienia skonkretyzowanych kryteriów, które jednak w rzeczywistości nie istnieją. Artykuł 6 ust. 4 zdanie trzecie dyrektywy pozostawia zasadniczą i fundamentalnie istotną decyzję co do tego, które dane mają być wykorzystane do ustalenia kryteriów lub wzorów zautomatyzowanego porównywania danych, w całości poszczególnym państwowi członkowskim. Nie jest to bezwzględnie konieczne ze względu na przedmiot regulacji. Prawodawca europejski mógłby z łatwością określić pewne dane lub kryteria, które powinny lub nie powinny być wykorzystywane przy tworzeniu wzorów. W tym względzie ani przestępstwa czy terroryzm mające miejsce w poszczególnych państwach członkowskich, ani też kryteria identyfikacji podejrzanych nie różnią się w poszczególnych państwach członkowskich.
- 38 Jako jedyny mechanizm kontroli proporcjonalności wzorów opracowywanych przez państwa członkowskie art. 6 ust. 7 w związku z art. 5 dyrektywy 2016/681 przewiduje dla inspektora ochrony danych w JIP uprawnienie do dostępu do tych wzorów. Jednakże zgodnie z art. 5 ust. 1 tej dyrektywy inspektor ochrony danych jest powoływany przez samą JIP i zazwyczaj przez nią zatrudniany, tak więc już z góry brakuje gwarancji jego niezależności (w sprawie niezależności organu nadzorczego ochrony danych zobacz wyroki z dnia 9 marca 2010 r., Komisja/Niemcy, C-518/07, EU:C:2010:125; z dnia 16 października 2012 r., Komisja/Austria, C-614/10, EU:C:2012:631).

W przedmiocie pytania drugiego lit. g): okres zatrzymywania danych

- 39 Zgodnie z art. 12 ust. 1 dyrektywy 2016/681 dane PNR są zatrzymywane przez okres pięciu lat. Zgodnie z motywem 25 zdanie drugie dyrektywy 2016/681 ze względu na charakter danych i ich wykorzystanie niezbędne jest zatrzymywanie danych PNR przez wystarczająco długi okres. Nie zostało przy tym wyjaśnione, dlaczego powinien to być okres pięciu lat.
- 40 Dla sądu odsyłającego nie jest jasne, dlaczego konieczny ma być tak długi okres zatrzymania. Po poddaniu pasażerów kontroli przed planowanym wjazdem do państwa członkowskiego lub wylotem z państwa członkowskiego zgodnie z art. 6 ust. 4 zdanie pierwsze dyrektywy 2016/681, o ile nie wystąpiły przy tym żadne nieprawidłowości, nie ma obiektywnych wskazań co do tego, że mogliby oni być powiązani, nawet pośrednio, z przestępstwami terrorystycznymi lub poważną

przestępczością. W związku z tym nie istnieje wystarczające powiązanie między zatrzymaniem danych a celami dyrektywy 2016/681. Jedynie w przypadku konkretnych oznak istnienia zagrożenia ze strony konkretnych pasażerów linii lotniczych odpowiednie wydaje się zatrzymanie danych na stałe (zob. opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 204 i nast.). Jednocześnie sama teoretyczna możliwość, że dane mogłyby w pewnym momencie stać się istotne z perspektywy bezpieczeństwa, nie jest wystarczająca, aby uzasadnić głębokie naruszenie praw podstawowych polegające na zatrzymaniu danych osobowych na lata.

- 41 Trybunał wyjaśnił już w odniesieniu do zatrzymania (retencji) danych – innej formy pozbawionego konkretnej przyczyny, masowego zatrzymywania danych osobowych – że dyrektywa, która przewiduje maksymalny okres zatrzymania danych do dwudziestu czterech miesięcy, nie ogranicza ingerencji do tego, co ściśle niezbędne (wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 64). Skoro już dwadzieścia cztery miesiące zatrzymywania danych to okres zbyt długi, to tym bardziej ma to miejsce w przypadku pięciu lat, jak w niniejszej sprawie.

W przedmiocie pytania drugiego lit. h): depersonalizacja

- 42 Zgodnie z motywem 25 dyrektywy 2016/681 tzw. depersonalizacja ma zapewnić wysoki poziom ochrony danych. Wydaje się to bardzo wątpliwe. „Depersonalizacja” danych zgodnie z art. 12 ust. 2 tej dyrektywy, która powinna nastąpić po upływie sześciu miesięcy, nie zmienia nic w odniesieniu do nieproporcjonalności okresu zatrzymania danych.
- 43 W pierwszej kolejności należy zauważyć, że termin „depersonalizacja” jest obcy systemowo i wprowadza w błąd. W istocie chodzi tu po prostu o pseudonimizację danych w rozumieniu art. 3 pkt 5 dyrektywy 2016/680. Różni się ona od anonimizacji tym, że w odróżnieniu od anonimizacji nie uniemożliwia w sposób trwały i ostateczny przyporządkowania danych do konkretnej osoby, lecz pozwala na ponowne ujawnienie danych osobowych (zobacz art. 12 ust. 3 dyrektywy 2016/681), a więc bez trudu możliwe jest przywrócenie bezpośredniego związku danych z osobą, której dane te dotyczą. Nie jest zatem jasne, dlaczego nie został zastosowany, tak jak w dyrektywie 2016/680, termin pseudonimizacja. Jednocześnie pseudonimizacja ze względu na jej odwracalność zmniejsza intensywność ingerencji w prawa podstawowe w znacznie mniejszym stopniu niż prawdziwa anonimizacja.
- 44 Ponadto zważyć należy na art. 4 ust. 1 lit. e) dyrektywy 2016/680. Zgodnie z tym przepisem dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania. W przypadku depersonalizacji, o której mowa w art. 12 ust. 2 dyrektywy 2016/681, identyfikacja osoby, której dane dotyczą, jest możliwa przez cały pięcioletni okres przechowywania, co potwierdza art. 12 ust. 3 dyrektywy 2016/681 pozwalający na (ponowne) ujawnienie pełnych

danych PNR po upływie sześciu miesięcy. Nie jest jednak oczywiste ani też nie zostało uzasadnione przez prawodawcę, że jest to niezbędnie konieczne do osiągnięcia celów dyrektywy 2016/681.

W przedmiocie pytania drugiego lit. i): powiadomienie po ujawnieniu danych

- 45 W dyrektywie 2016/681 brakuje przepisu, który wymagałby informowania osób, których dane dotyczą, w sytuacji gdy dotyczące ich dane przechowywane przez JIP w państwach członkowskich zostały ujawnione zgodnie z art. 12 ust. 3 tej dyrektywy. Uregulowane zostało jedynie, że ujawnienie musi zostać zatwierdzone przez „organ wymiaru sprawiedliwości” lub inny organ krajowy [art. 12 ust. 3 lit. b) dyrektywy 2016/681].
- 46 Trybunał wyjaśnił już w swojej opinii dotyczącej umowy między Kanadą a Unią Europejską, że zgodnie z projektowaną umową pasażerowie lotniczy mieli być wprowadzeni ogólnie informowani za pośrednictwem strony internetowej o przetwarzaniu dotyczących ich danych do celów kontroli bezpieczeństwa i kontroli granicznych, jednakże w oparciu o tę ogólną informację nie byli w stanie ustalić, czy ich dane zostały wykorzystane przez właściwe organy także poza tymi kontrolami (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 223). Dalej w opinii Trybunału wskazano wyraźnie: „Tak więc w sytuacjach [...], w których obecne są obiektywne elementy uzasadniające takie wykorzystanie i wymagające uprzedniego zezwolenia wydanego przez sąd lub niezależny organ administracyjny, indywidualne informowanie pasażerów lotniczych okazuje się konieczne. Dotyczy to również wypadków, gdy dane PNR pasażerów lotniczych są udostępniane innym organom rządowym lub osobom fizycznym” (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 223).
- 47 Sąd odsyłający przyjmuje, że ta ocena Trybunału może zostać przeniesiona na grunt dyrektywy 2016/681 i w związku z tym uważa, że osoby, których dane dotyczą, powinny być indywidualnie informowane o ujawnieniu ich danych osobowych. Gdyby Trybunał uznał, że niezwłoczne poinformowanie osób, których dane dotyczą, o ujawnieniu ich danych osobowych mogłoby nadmiernie zaszkodzić realizacji zamierzonego celu, jakim jest zapobieganie przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywanie, prowadzenie dochodzeń w ich sprawie i ich ściganie, sąd odsyłający uważa, że poinformowanie osób, których dane dotyczą, powinno koniecznie nastąpić najpóźniej w momencie, w którym realizacja celu ujawnienia danych osobowych nie jest już zagrożona, na przykład ze względu na zakończenie postępowania przygotowawczego.
- 48 Osoba, której dane dotyczą, ma również na podstawie art. 47 karty praw podstawowych prawo do tego, by kontrola została przeprowadzona przez niezawisły i bezstronny sąd ustanowiony uprzednio na mocy ustawy, a nie przez „organ wymiaru sprawiedliwości”. W niniejszej sprawie tego rodzaju środek prawny jest jednak niedostępny.

W przedmiocie pytania trzeciego: przekazanie państwom trzecim

- 49 Zgodnie z art. 11 ust. 1 dyrektywy 2016/681 dane PNR oraz wyniki przetwarzania takich danych mogą zostać przekazane państwu trzeciemu w konkretnym przypadku, jeżeli spełnione zostały warunki określone w art. 13 decyzji ramowej 2008/977/WSiSW, przekazanie jest niezbędne do celów dyrektywy 2016/681, państwo trzecie zgadza się, że dane te mogą być przekazane innemu państwu trzeciemu wyłącznie wtedy, gdy jest to absolutnie niezbędne do celów tej dyrektywy oraz wyłącznie za wyraźną zgodą tego państwa członkowskiego, oraz spełnione zostały takie same warunki określone w art. 9 ust. 2 dyrektywy 2016/681.
- 50 Artykuł 11 ust. 2 dyrektywy 2016/681 przewiduje wyjątek od przywołanych wyżej wymogów, stanowiąc, że niezależnie od art. 13 ust. 2 decyzji ramowej 2008/977/WSiSW (obecnie art. 38 dyrektywy 2016/680) przekazywanie danych PNR bez uprzedniej zgody państwa członkowskiego, od którego uzyskano te dane, jest dopuszczalne w wyjątkowych okolicznościach, tj. wyłącznie wtedy, gdy 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 gdy uprzedniej zgody nie można uzyskać na czas.
- 51 Wobec tego, że organy państw trzecich uzyskują dostęp do danych PNR wskutek ich przekazania, również w stosunku do tych państw trzecich muszą znajdować zastosowanie wszystkie zasady dotyczące wykorzystywania danych, mające na celu zagwarantowanie proporcjonalności związanych z tym ingerencji w prawa podstawowe oraz odpowiedniego poziomu ochrony. W tym zakresie Trybunał wyjaśnił w swojej opinii dotyczącej umowy między Unią Europejską a Kanadą, że przekazywanie danych osobowych z Unii do państwa trzeciego może mieć miejsce wyłącznie wówczas, gdy państwo to zapewnia poziom ochrony podstawowych praw i wolności zasadniczo równoważny poziomowi gwarantowanemu w Unii. Dzięki temu możliwe ma być zapobieżenie obejściu poziomu ochrony przewidzianego w tej umowie poprzez przekazywanie danych osobowych do innych państw trzecich, jak również zapewnienie ciągłości poziomu ochrony przyznanego prawem Unii (opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 214). Na tej podstawie Trybunał wysnuł wniosek, że udostępnienie danych osobowych państwu trzeciemu wymaga istnienia bądź umowy między Unią a danym państwem trzecim równoważnej umowie między Unią a Kanadą, bądź decyzji Komisji przyjętej na podstawie art. 25 ust. 6 dyrektywy 95/46 (obecnie art. 45 ust. 3 RODO) stwierdzającej, że rzeczne państwo trzecie zapewnia odpowiedni poziom ochrony, i obejmującej organy, którym zamierza się przekazywać dane PNR (opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 214).
- 52 Artykuł 11 dyrektywy 2016/681 nie gwarantuje realizacji tak określonych warunków. Artykuł 11 ust. 1 lit. a) dyrektywy 2016/681 odsyła do art. 13 decyzji ramowej 2008/977/WSiSW. Rieczona decyzja ramowa została uchylona na mocy

dyrektywy 2016/680. Odesłania do decyzji ramowej oznaczają obecnie odesłania do dyrektywy 2016/680 (zobacz art. 59 dyrektywy 2016/680). Artykułowi 13 uchylonej decyzji ramowej 2008/977/WSiSW odpowiadają co do zasady art. 35–38 dyrektywy 2016/680.

- 53 Zgodnie z art. 35 ust. 1 lit. d) dyrektywy 2016/680 przekazanie danych państwu trzeciemu może nastąpić, pod warunkiem że Komisja wydała decyzję w przedmiocie zgodności na podstawie art. 36 tej dyrektywy, lub w razie braku takiej decyzji zapewnione zostały lub istnieją odpowiednie zabezpieczenia zgodnie z art. 37 tej dyrektywy, lub w razie braku decyzji w przedmiocie zgodności wydanej na podstawie art. 36 tej dyrektywy lub zabezpieczeń zgodnie z art. 37 tej dyrektywy, zastosowanie mają wyjątki w szczególnych sytuacjach zgodnie z art. 38 tej dyrektywy. Tym samym odesłanie z art. 11 ust. 1 lit. a) dyrektywy 2016/681 do art. 13 decyzji ramowej 2008/977/WSiSW i w ten sposób do art. 35 dyrektywy 2016/680 nie gwarantuje odpowiedniego poziomu ochrony danych po stronie państw trzecich, albowiem przepis ten wskutek odesłania do art. 38 dyrektywy 2016/680 pozwala na to, żeby dane PNR były przekazywane państwom trzecim także mimo braku decyzji w przedmiocie zgodności i braku odpowiednich zabezpieczeń po stronie państwa trzeciego. Jest tak w szczególności dlatego, że pojęcie wyjątku w rozumieniu art. 38 dyrektywy 2016/680 zostało ujęte bardzo szeroko. Przepis ten umożliwia bowiem przekazanie danych osobowych do państwa trzeciego mimo niezapewnienia odpowiedniego poziomu ochrony, jeżeli w indywidualnym przypadku służy to celom wyrażonym w art. 1 ust. 1 dyrektywy 2016/680 (zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych i wykonywanie kar, w tym ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom) albo pozostając w związku z tymi celami jest niezbędne dla ustalenia, dochodzenia lub obrony roszczeń (zobacz art. 38 ust. 1 lit. d) i e) dyrektywy 2016/680).

W przedmiocie pytania czwartego: preferencje dotyczące posiłków w wolnym polu tekstowym

- 54 Zgodnie z art. 6 ust. 4 zdanie czwarte dyrektywy 2016/681 kryteria, w oparciu o które JIP w państwach członkowskich porównują dane w sposób zautomatyzowany, 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.
- 55 Jednakże przepis ten zawiera jedynie deklarację zamiaru prawodawcy, który zostaje udaremniony w szczególności na skutek pkt 12 załącznika I do dyrektywy 2016/681. W związku z wypełnieniem wolnego pola tekstowego „Uwagi ogólne”, skąd dane są przekazywane do JIP obowiązkowo w każdym przypadku i bez wyjątków, może bowiem dojść do przekazania JIP, a następnie wykorzystania przez JIP szeregu przeróżnych informacji, w tym danych wrażliwych.

Przykładowo wskutek wypełnienia tego wolnego pola tekstowego może zostać przekazana informacja, że pasażer poprosił o jedzenie koszerne lub halal. Informacje te mogą zaś zostać wykorzystane do wyciągnięcia wniosków na temat przekonań religijnych danej osoby, a więc może chodzić o dane szczególnie wrażliwe w rozumieniu opisanym wyżej.

W przedmiocie pytania piątego: informacje udzielane przez przewoźnika lotniczego

- 56 Zgodnie z art. 13 ust. 3 dyrektywy 2016/681 dyrektywa ta nie ma wpływu na możliwość stosowania dyrektywy Parlamentu Europejskiego i Rady 95/46/WE 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. Również art. 21 ust. 2 dyrektywy 2016/681 stanowi wyraźnie, że dyrektywa 2016/681 nie ma wpływu na możliwość stosowania dyrektywy 95/46 do przetwarzania danych osobowych przez przewoźników lotniczych.
- 57 Dyrektywa 95/46 została zastąpiona przez RODO (zobacz art. 94 ust. 2 RODO, zgodnie z którym odesłania do dyrektywy 95/46 należy traktować jako odesłania do RODO).
- 58 Zgodnie z art. 13 RODO w przypadku zbierania danych osobowych osobie, której dane te dotyczą, udziela się informacji wskazanych w tym artykule. Pojęcie „danych osobowych” zostało zdefiniowane w art. 4 pkt 1 RODO. Zbieranie danych PNR dotyczących pasażerów i osób trzecich przez przewoźników lotniczych stanowi zbieranie danych osobowych w rozumieniu tej definicji, a w konsekwencji w tym przypadku do przewoźników lotniczych znajduje zastosowanie art. 13 RODO.
- 59 Zdaniem sądu odsyłającego względ na przedstawioną wyżej wagę ingerencji w prawa podstawowe związanej z przetwarzaniem danych PNR powoduje, że wymogi informacyjne muszą być restrykcyjnie egzekwowane.
- 60 W ocenie sądu odsyłającego na przewoźnikach lotniczych spoczywa obowiązek informacyjny w stosunku do osób, których dane dotyczą, zgodnie z art. 13 i 14 RODO, albowiem w przeciwnym razie istniałaby luka, która byłaby nie do pogodzenia z treścią art. 7 i 8 karty praw podstawowych. W związku z tym niezbędne jawi się, żeby przewoźnicy lotniczy wyraźnie informowali pasażerów o wszystkich gromadzonych przez nich danych PNR, planowanym przekazaniu tych danych do JIP w państwach członkowskich oraz dalszym przetwarzaniu tam rzeczonych danych, w tym o pięcioletnim okresie zatrzymania, a także o szczególnych prawach, które przysługują pasażerom jako osobom, których dane dotyczą. Bez tej informacji pasażerowie nie będą bowiem w stanie korzystać z praw, które przysługują im jako osobom, których dane dotyczą. Dyrektywa 2016/681 nie zawiera jednak żadnych przepisów w tym zakresie.

- 61 Trybunał wyjaśnił już w swojej opinii dotyczącej umowy między Unią Europejską i Kanadą, że dla zapewnienia przestrzegania tych praw istotne jest, by pasażerowie lotniczy byli informowani o przekazywaniu ich danych PNR do Kanady oraz o wykorzystywaniu tych danych od chwili, gdy to udostępnienie nie może zagrozić dochodzeniom prowadzonym przez organy rządowe, o których mowa w rzeczonej umowie. Informowanie takie okazuje się de facto konieczne, by umożliwić pasażerom lotniczym skorzystanie z prawa do domagania się dostępu do dotyczących ich danych PNR oraz ewentualnie ich sprostowania, jak również, zgodnie z art. 47 akapit pierwszy karty praw podstawowych, wniesienia skutecznego środka prawnego do sądu (zobacz opinia 1/15 z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 220).
- 62 Jako przykład niewystarczających informacji przekazywanych pasażerom przez przewoźników lotniczych posłużyć mogą informacje udzielane przez przewoźnika, z którego usług skorzystał skarżący. Na stronie internetowej Lufthansa AG (<https://www.lufthansa.com/xx/de/informationen-zum-datenschutz>, ostatnio dostęp w dniu 11 maja 2020 r.) podano następujące informacje:

„Kto jest administratorem?”

Deutsche Lufthansa [...] niniejszym informuje Państwa o przetwarzaniu Państwa danych osobowych [...]

[...]

Do kogo mogę się zwrócić?

W razie [...] pytań dotyczących ochrony danych [...], prosimy o kontakt z naszym inspektorem danych osobowych:

[...]

Jakie obowiązki [...] realizujemy, przetwarzając Państwa dane?

Przetwarzamy dane dotyczące przelotu pasażera celem wypełnienia obowiązków prawnych zgodnie z art. 6 ust. 1 zdanie pierwsze lit. c) RODO:

O ile jesteśmy do tego prawnie zobowiązani, przetwarzamy dane osobowe w celu [...] spełnienia wymogów bezpieczeństwa [...]

Przekazywanie danych do organów imigracyjnych:

- *W oparciu o umowy w przedmiocie danych dotyczących przelotu pasażera zawartych między UE a USA lub Kanadą*
- *W oparciu o Fluggastdatengesetz (ustawę o danych dotyczących przelotu pasażera) w Niemczech*

- Przekazywanie API* (Advance Passenger Information), jeżeli jesteśmy zobowiązani do współpracy w działaniach kontrolnych dotyczących podróży międzynarodowych

*Dane części paszportu lub dowodu tożsamości nadających się do odczytu maszynowego

Dalsze informacje otrzymają Państwo we właściwych organach.

[...]

Kto otrzyma Państwa dane?

[...] Państwa dane [mogą] zostać przekazane następującym kategoriom odbiorców:

[...]

jednostki i organy państwowe, np. w związku z przepisami dotyczącymi wjazdu na terytorium państwa lub działaniami policji i innych organów ścigania.

Może się zdarzyć, że dane osobowe zostaną przekazane do państw trzecich lub organizacji międzynarodowych. W celu zapewnienia Państwu ochrony oraz ochrony dotyczących Państwa danych osobowych przewidziano odpowiednie gwarancje dotyczące takiego przekazywania danych na podstawie wymogów ustawowych i w zgodzie z nimi.

Jeżeli takie przekazanie danych nie ma podstawy ustawowej lub dokonywane jest do kraju, w odniesieniu do którego Komisja Europejska nie wydała decyzji stwierdzającej odpowiedni stopień ochrony, stosujemy standardowe klauzule umowne UE.

Jakie prawa w zakresie ochrony danych osobowych Państwu przysługują?

Dla Lufthansa istotne jest, aby nasze procedury przetwarzania danych były uczciwe i przejrzyste. Dlatego ważne jest dla nas, aby osoby, których dane dotyczą, mogły korzystać oprócz prawa do sprzeciwu także z następujących praw, jeżeli spełnione są warunki ustawowe:

Prawo dostępu do danych przysługujące osobie, której dane dotyczą, art. 15 RODO

Prawo do sprostowania danych, art. 16 RODO

Prawo do usunięcia danych („prawo do bycia zapomnianym”), art. 17 RODO

Prawo do ograniczenia przetwarzania danych, art. 18 RODO

Prawo do przenoszenia danych, art. 20 RODO

Prawo do sprzeciwu, art. 21 RODO

[...]”.

- 63 Informacje te mogą być niewystarczające i wprowadzać w błąd. W szczególności informacja, że w przypadku danych API chodzi jedynie o części paszportu lub dowodu tożsamości nadające się do odczytu maszynowego, jest oczywiście niepełna. Zgodnie z pkt 18 załącznika I do dyrektywy 2016/681 przekazaniu podlegają bowiem wszelkie zebrane dane API, w tym dotyczące linii lotniczej, numeru lotu oraz dat, godzin i miejsc odlotu i przylotu, a więc w żadnym razie nie są to jedynie części dokumentów tożsamości nadające się do odczytu maszynowego. Poza tym w żadnym miejscu nie ma odesłania do dyrektywy 2016/681, a jedynie do FlugDaG. Ponadto nie ma jakiegokolwiek odniesienia do treści dyrektywy 2016/681 ani FlugDaG. W związku z tym w okresie poprzedzającym rezerwację lotu nie jest jasne dla osób, których dane dotyczą, który organ kwalifikowany jest jako JIP w danym państwie członkowskim i w jaki sposób można się do niego zwrócić, jak dokładnie dane PNR są tam przetwarzane ani jak długo dane te mogą być przez tę JIP zatrzymane. W związku z tym informacje przekazywane pasażerom przez Lufthansa AG nie wydają się spełniać wymogów z art. 13 RODO w odniesieniu do tych pasażerów, nie wspominając już o całkowitym przemilczeniu innych osób, które również powinny być informowane.