



Rada
Unii Europejskiej

Bruksela, 14 grudnia 2022 r.
(OR. en)

Międzyinstytucjonalne numery
referencyjne:
2022/0425(COD)
2022/0424(COD)

15720/22
ADD 3

IXIM 293
ENFOPOL 638
FRONT 461
AVIATION 318
DATAPROTECT 362
JAI 1677
COMIX 615
CODEC 2011
IA 222

PISMO PRZEWODNIE

Od: Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)

Data otrzymania: 14 grudnia 2022 r.

Do: Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej

Nr dok. Kom.: SWD(2022) 423 final

Dotyczy: DOKUMENT ROBOCZY SŁUŻB KOMISJI - STRESZCZENIE
SPRAWOZDANIA Z OCENY SKUTKÓW - towarzyszący dokumentom:
wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady
w sprawie gromadzenia i przekazywania danych pasażera
przekazywanych przed podróżą (API) w celu usprawnienia i ułatwienia
kontroli na granicach zewnętrznych, zmieniające rozporządzenie (UE)
2019/817 i rozporządzenie (UE) 2018/1726 oraz uchylające dyrektywę
Rady 2004/82/WE wniosek dotyczący rozporządzenia Parlamentu
Europejskiego i Rady w sprawie gromadzenia i przekazywania danych
pasażera przekazywanych przed podróżą w celu zapobiegania
przestępstwom terrorystycznym i poważnej przestępczości, ich
wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie
i ich ścigania oraz zmieniające rozporządzenie (UE) 2019/818

Delegacje otrzymują w załączeniu dokument SWD(2022) 423 final.

Zał.: SWD(2022) 423 final

Strasburg, dnia 13.12.2022 r.
SWD(2022) 423 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI
STRESZCZENIE SPRAWOZDANIA Z OCENY SKUTKÓW

[...]

Towarzyszący dokumentom:

wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie gromadzenia i przekazywania danych pasażera przekazywanych przed podróżą (API) w celu usprawnienia i ułatwienia kontroli na granicach zewnętrznych, zmieniające rozporządzenie (UE) 2019/817 i rozporządzenie (UE) 2018/1726 oraz uchylające dyrektywę Rady 2004/82/WE

wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie gromadzenia i przekazywania danych pasażera przekazywanych przed podróżą w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania oraz zmieniające rozporządzenie (UE) 2019/818

{COM(2022) 729 final} - {SEC(2022) 444 final} - {SWD(2022) 421 final} -
{SWD(2022) 422 final}

Streszczenie oceny skutków

Ocena skutków zmiany dyrektywy w sprawie danych pasażera przekazywanych przed podróżą (API)

A. Zasadność działań

Dlaczego należy podjąć działania? Na czym polega problem?

W ciągu ostatnich dziesięcioleci nastąpił wzrost liczby osób podróżujących drogą powietrzną – w UE odnotowano 1 mld pasażerów (w 2019 r.), w tym pół miliarda pasażerów przybywających do UE lub opuszczających UE drogą powietrzną. Stanowi to obciążenie dla zewnętrznych granic powietrznych. W tym kontekście dane pasażera przekazywane przed podróżą (API) stanowią skuteczne narzędzie informowania służb granicznych z wyprzedzeniem o liczbie i tożsamości osób podróżujących drogą powietrzną, co umożliwia przeprowadzenie wstępnych kontroli przed przybyciem tych osób na granicę zewnętrzną. Pojawiają się jednak **dwa główne problemy**, które skutkują powstawianiem luk i niespójności, jeżeli chodzi o sposób przetwarzania danych API przez państwa członkowskie zarówno na potrzeby zarządzania granicami, jak i na potrzeby ochrony porządku publicznego.

- Po pierwsze, aby zarządzanie granicami było skuteczne, **wszystkie osoby podróżujące drogą powietrzną, przekraczające zewnętrzne granice strefy Schengen, muszą być poddawane skutecznym i systematycznym wstępnym kontrolom z wykorzystaniem danych API**. Nie wszystkie jednak państwa członkowskie wymagają od przewoźników lotniczych przekazywania danych API. Co więcej, w odniesieniu do państw członkowskich, które wprowadziły system API, w ocenie dyrektywy w sprawie API z 2020 r. stwierdzono, że w niewystarczającym stopniu korzystają one z możliwości przetwarzania danych API do celów usprawnienia zarządzania granicami. Skuteczne wykorzystanie danych API wymaga ponadto gromadzenia wiarygodnych i zweryfikowanych danych, co obecnie nie zawsze ma miejsce. W dyrektywie w sprawie API faktycznie nie przewidziano sposobów gromadzenia danych API od pasażerów, co w rezultacie może skutkować przekazywaniem organom krajowym niepełnych lub niepoprawnych danych. Z tych względów i dzięki elastyczności, jaką zapewniają wymogi określone w dyrektywie w sprawie API, występuje duża różnorodność w sposobie wdrażania dyrektywy w sprawie API przez państwa członkowskie. W rezultacie nie każda osoba podróżująca drogą powietrzną i przekraczająca zewnętrzną granicę strefy Schengen zostaje poddana wstępnej kontroli z wykorzystaniem danych API.
- Po drugie, **łączone przetwarzanie danych API i danych dotyczących przelotu pasażera (PNR) stanowi skuteczne narzędzie wykorzystywane przez organy ścigania do celów wykrywania terrorystów i innych osób dopuszczających się poważnych przestępstw**. Zwalczanie poważnej przestępczości i terroryzmu stanowi odrębny cel przetwarzania danych API, przy czym wykorzystywanie danych API w tym celu jest skuteczne wyłącznie wówczas, gdy są one przetwarzane w połączeniu z informacjami dotyczącymi rezerwacji zawartymi w danych PNR. Wskazane wyżej braki w przetwarzaniu danych API ograniczają skuteczność wykorzystania tych danych na potrzeby ochrony porządku publicznego. Co więcej, ponieważ w obecnie obowiązujących unijnych ramach przewidziano łączone przetwarzanie danych API i PNR wyłącznie w przypadku lotów do UE lub z UE, istnieje poważna luka w systemie bezpieczeństwa związana z przetwarzaniem przez władze państw członkowskich danych osób podróżujących drogą powietrzną w ramach lotów wewnątrzunijnych i krajowych. Aby wyeliminować tę lukę, w opracowanej przez Komisję Strategii na rzecz **w pełni funkcjonującej i odpornej strefy Schengen** z czerwca 2021 r., wezwano do większego wykorzystania danych API w połączeniu z danymi PNR w przypadku lotów wewnątrz strefy Schengen w celu znacznego zwiększenia bezpieczeństwa wewnętrznego, zgodnie z prawem podstawowym do **ochrony danych osobowych** i prawem podstawowym do **swobody przemieszczania się**¹.

Jaki jest cel inicjatywy?

Celem tej inicjatywy jest **usprawnienie zarządzania zewnętrzną granicą strefy Schengen** poprzez zapewnienie, aby każda osoba przylatująca do strefy Schengen lub opuszczająca strefę Schengen drogą powietrzną była poddawana wstępnej kontroli z wykorzystaniem danych API przed przybyciem na zewnętrzną granicę strefy Schengen. Inicjatywa ta służy również **zwiększeniu bezpieczeństwa wewnętrznego UE** poprzez zapewnienie, aby organy ścigania państw członkowskich miały dostęp do wiarygodnych danych dotyczących osób podróżujących drogą powietrzną na potrzeby skutecznego zapobiegania terroryzmowi i poważnej przestępczości i ich skutecznego zwalczania. Aby osiągnąć te ogólne cele, w ramach inicjatywy określono trzy cele szczegółowe:

- zapewnienie **wstępnych kontroli z wykorzystaniem danych API na zewnętrznych granicach strefy Schengen**: dzięki gromadzeniu danych API organy krajowe mogą systematycznie porównywać dane

¹ COM(2021) 277 final (2.6.2021).

dotyczące pasażerów z informacjami zawartymi w krajowych, unijnych i międzynarodowych bazach danych, jeszcze zanim dany pasażer faktycznie zjawi się na przejściu granicznym. Za sprawą danych API funkcjonariusze straży granicznych mają więcej czasu na przeanalizowanie informacji, dzięki czemu mogą lepiej zorganizować swoją pracę;

- **usprawnienie przepływu pasażerów podróżujących w dobrej wierze na zewnętrznych granicach strefy Schengen:** dane API ułatwiają odprawę pasażerów niskiego ryzyka. Lepsze przygotowanie do kontroli poszczególnych pasażerów, którzy są weryfikowani z wykorzystaniem danych API, jeszcze zanim dotrą na granicę, przyczynia się do przyspieszenia odpraw granicznych, ponieważ pasażerów wymagających dodatkowych kontroli można oddzielić od pozostałych pasażerów, którzy dzięki temu nie muszą stać w kolejce i czekać;
- **skuteczne zwalczanie poważnej przestępczości i terroryzmu za sprawą łącznego przetwarzania danych API i PNR:** dane API gromadzone w sposób zautomatyzowany umożliwią wiarygodną identyfikację pasażerów będących osobami szczególnego zainteresowania dla właściwych organów prowadzących dochodzenia w sprawie poważnej przestępczości i terroryzmu. Aby łączne przetwarzanie danych API i PNR było możliwe, wszystkie dane PNR otrzymane przez właściwe organy muszą być uzupełniane kompletnymi i prawidłowymi danymi API, z poszanowaniem prawa podstawowego do ochrony danych osobowych i prawa podstawowego do swobody przemieszczania się.

Na czym polega wartość dodana podjęcia działań na poziomie UE?

Stosowanie dyrektywy w sprawie API skutkuje przyjmowaniem niespójnych i zróżnicowanych praktyk, jak wynika z oceny tej dyrektywy z 2020 r., w związku z czym konieczne jest podjęcie dalszego działania w tym obszarze w celu zapewnienia, aby dane API wykorzystywano do wstępnych kontroli na zewnętrznych granicach strefy Schengen w sposób skuteczny i spójny. Interwencja na poziomie UE zapewniłaby również ogólnounijne kryteria w zakresie gromadzenia i przekazywania danych API na potrzeby ochrony porządku publicznego z myślą o zwiększeniu skuteczności przetwarzania danych PNR w celu zwalczania poważnej przestępczości i terroryzmu w UE.

Dzięki bardziej przejrzystym kryteriom dotyczącym gromadzenia danych API możliwe będzie zapewnienie większego wykorzystywania tych danych w branży lotniczej i skuteczniejszego przestrzegania tych kryteriów, a także zwiększenie wydajności, zwłaszcza dzięki wprowadzeniu obowiązku przekazywania danych API do jednego punktu wejścia (interfejs przewoźnika i router API), a nie – tak jak obecnie – do wielu organów krajowych. Organy krajowe i pozostałe zainteresowane strony, z którymi skonsultowano się podczas przygotowywania niniejszej oceny skutków, wezwały do zmiany dyrektywy w sprawie API w celu zapewnienia spójności i jasności prawa.

B. Rozwiązania

Jakie warianty legislacyjne i nielegislacyjne rozważono? Czy wskazano preferowany wariant? Dlaczego należy podjąć działania?

Rozważono szereg wariantów strategicznych o charakterze legislacyjnym, gdyż za pomocą wariantów nielegislacyjnych nie zdołano by skutecznie rozwiązać zidentyfikowanych problemów. Po dokonaniu wstępnej selekcji niektóre warianty zostały szybko odrzucone. Warianty strategiczne przeanalizowane w niniejszej ocenie skutków można podzielić na trzy zestawy, tj.:

- (1) **warianty dotyczące zakresu gromadzenia danych API na potrzeby zarządzania zewnętrznymi granicami strefy Schengen.** W tym przypadku można wyróżnić dwa zbiorcze warianty strategiczne:
 - wariant strategiczny 1.1: gromadzenie danych API w przypadku wszystkich lotów przychodzących spoza strefy Schengen;
 - wariant strategiczny 1.2: gromadzenie danych API w przypadku wszystkich lotów przychodzących spoza strefy Schengen i wszystkich lotów wychodzących poza strefę Schengen;
- (2) **warianty dotyczące zakresu gromadzenia danych API na potrzeby ochrony porządku publicznego** w celu zapewnienia możliwości łącznego przetwarzania danych API i PNR. W tym przypadku można wyróżnić dwa zbiorcze warianty strategiczne:
 - wariant strategiczny 2.1: gromadzenie danych API w przypadku wszystkich pozaunijnych lotów przychodzących i wychodzących;
 - wariant strategiczny 2.2: gromadzenie danych API w przypadku wszystkich lotów pozaunijnych (przychodzących i wychodzących), wszystkich lotów wewnątrzunijnych i wszystkich lotów krajowych, w odniesieniu do których gromadzone są dane PNR;
- (3) **warianty dotyczące jakości i pozyskiwania danych API,** zakładające przyjęcie podejścia horyzontalnego. Wiązałoby się to z gromadzeniem danych API w przypadku każdego odpowiedniego lotu i w dowolnym celu, tj. zarówno na potrzeby zarządzania zewnętrznymi granicami strefy Schengen, jak i na potrzeby ochrony porządku publicznego. Istnieją dwa alternatywne warianty strategiczne:

- wariant strategiczny 3.1: gromadzenie danych API w sposób zautomatyzowany albo ręczny;
- wariant strategiczny 3.2: gromadzenie danych API wyłącznie w sposób zautomatyzowany.

Preferowane warianty strategiczne obejmują gromadzenie danych API w przypadku lotów przychodzących spoza strefy Schengen na potrzeby zarządzania zewnętrznymi granicami strefy Schengen (wariant strategiczny 1.1), lotów pozaunijnych, wybranych lotów wewnątrzunijnych i krajowych, w odniesieniu do których gromadzone są dane PNR na potrzeby ochrony porządku publicznego (wariant strategiczny 2.2). Preferowane warianty strategiczne obejmują również obowiązek przekazywania pełnego zestawu danych API przez przewoźników lotniczych wyłącznie w sposób zautomatyzowany (wariant strategiczny 3.2) zarówno na potrzeby zarządzania zewnętrznymi granicami strefy Schengen, jak i na potrzeby ochrony porządku publicznego.

Jak kształtuje się poparcie dla poszczególnych wariantów?

Podczas przygotowywania niniejszej oceny skutków przeprowadzono konsultacje z szerokim gronem zainteresowanych stron, w tym z organami krajowymi państw członkowskich, agencjami UE, organizacjami społeczeństwa obywatelskiego, a także przedstawicielami sektora prywatnego i organizacji międzynarodowych. Konsultacje przeprowadzono w formie badań ankietowych, wywiadów i warsztatów z głównymi zainteresowanymi stronami. Większość zainteresowanych stron, które uczestniczyły w konsultacjach, poparła preferowany wariant strategiczny.

C. Skutki wdrożenia preferowanego wariantu

Jakie korzyści przyniesie wdrożenie preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

Instrument API na potrzeby zarządzania granicami zewnętrznymi przyczyni się do zwiększenia zdolności państw członkowskich w zakresie wykorzystywania danych API na potrzeby skutecznej i wydajnej wstępnej kontroli osób podróżujących drogą powietrzną przed ich przybyciem na zewnętrzną granicę strefy Schengen. Standaryzacja wymogów dotyczących gromadzenia i przekazywania danych API pozwoli zwiększyć stopień przestrzegania tych wymogów przez branżę lotniczą, ponieważ we wszystkich państwach członkowskich będą obowiązywać te same wymogi. Bardziej wiarygodne i zweryfikowane dane API zgromadzone w sposób zautomatyzowany pozwolą na identyfikację podróżnych wysokiego ryzyka i zapewnią przyspieszenie i ułatwienie odprawy na granicach zewnętrznych oraz odprawy celnej pasażerów po przyjeździe.

Odrębny **instrument API na potrzeby ochrony porządku publicznego** ureguluje gromadzenie danych API w przypadku wszystkich lotów do UE i poza UE, a także wybranych lotów wewnątrzunijnych i krajowych, w odniesieniu do których gromadzone są dane PNR. Łączne przetwarzanie danych API i PNR pozwoli zwiększyć skuteczność dyrektywy w sprawie danych PNR w zakresie zwalczania poważnej przestępczości i terroryzmu. Właściwe organy krajowe (jednostki do spraw informacji o pasażerach) będą dysponowały wyższej jakości, zweryfikowanymi danymi API na potrzeby prowadzenia postępowań przygotowawczych w sprawie poważnej przestępczości i terroryzmu oraz identyfikacji sprawców tych poważnych przestępstw.

Jakie są koszty wdrożenia preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

Preferowany wariant strategiczny będzie wymagał inwestycji zarówno po stronie organów krajowych, jak i przewoźników lotniczych. Koszty **instrumentu API na potrzeby zarządzania granicami zewnętrznymi** ponoszone przez organy państw członkowskich będą zależeć od wielkości państwa i całkowitej liczby lotów przychodzących. Krajowe systemy API będą musiały zostać zmodyfikowane, aby umożliwić odbiór i przetwarzanie strumieni dodatkowych danych, które wcześniej nie były gromadzone. Łącznie koszty te szacuje się na średnio **13,5 mln EUR**. W przypadku przewoźników lotniczych głównym elementem kosztów będą koszty związane z przekazywaniem danych API. Obowiązek systematycznego przekazywania danych API w przypadku wszystkich lotów przychodzących spowoduje wzrost ilości przekazywanych danych i tym samym będzie skutkował dodatkowymi kosztami przekazywania. W ramach tej inicjatywy dane API będą jednak przekazywane jedynie do jednego punktu, tj. do interfejsu przewoźnika podłączonego do routera API, co pozwoli znacznie ograniczyć koszty przekazywania. Szacuje się, że osiągnięte w ten sposób oszczędności netto wyniosą **2,53 mln EUR** rocznie. Linie lotnicze, które nie stosują automatyzacji w procesach odprawy, będą również musiały dokonać inwestycji albo modyfikacji systemów, aby gromadzić dane API w sposób zautomatyzowany, co będzie wiązało się z jednorazowym szacunkowym kosztem rzędu **50 mln EUR**.

Instrument API na potrzeby ochrony porządku publicznego spowoduje również wzrost liczby pasażerów, których dane będą przekazywane organom przez linie lotnicze, przy czym związane z tym koszty będą ograniczone ze względu na fakt, iż dane te będą przekazywane tylko raz do interfejsu przewoźnika podłączonego do routera API. Szacuje się, że łącznie będzie się to wiązało z kosztami jednorazowymi na poziomie **75 mln EUR** i z powtarzającymi się kosztami przekazywania danych API w przypadku lotów wewnątrzunijnych na poziomie **16,13 mln EUR** oraz z powtarzającymi się kosztami w przypadku lotów wychodzących na poziomie **4,21 mln EUR**. Oczekuje się, że państwa członkowskie nie poniosą żadnych

kosztów, ponieważ istniejące zdolności są wystarczające do przetwarzania dodatkowych danych API.
Jakie będą skutki dla przedsiębiorstw, MŚP i mikroprzedsiębiorstw?
Oczekuje się, że proponowane środki nie będą miały istotnego wpływu na małe i średnie przedsiębiorstwa.
Czy przewiduje się znaczące skutki dla budżetów i administracji krajowych?
Szacunkowa suma oczekiwanych kosztów inwestycji na poziomie krajowym wynosi średnio 13,5 mln EUR .
Czy wystąpią inne znaczące skutki?
Wszystkie preferowane warianty strategiczne odnoszą się do przetwarzania danych osobowych. W związku z tym te warianty strategiczne mają wpływ na prawa podstawowe, a w szczególności na prawo do ochrony danych osobowych (art. 8 Karty praw podstawowych Unii Europejskiej) i prawo do poszanowania życia prywatnego i rodzinnego (art. 7 Karty). Gromadzenie danych API w przypadku wybranych lotów wewnątrzunijnych i krajowych może zniechęcać do korzystania ze swobody przemieszczania się zagwarantowanej w art. 45 Karty. Aby zapewnić pełną zgodność z prawami podstawowymi, w ocenie skutków w sposób kompleksowy uwzględniono prawa podstawowe w całej analizie oraz wskazano szereg koniecznych skutecznych gwarancji. W szczególności gromadzenie danych API w przypadku lotów wewnątrzunijnych i krajowych na potrzeby ochrony porządku publicznego nie będzie prowadzone systematycznie i będzie ograniczać się do lotów, w przypadku których gromadzone są dane PNR. Gromadzenie danych API będzie podlegało wymogom i gwarancjom określonym w wyroku Trybunału Sprawiedliwości w sprawie <i>Ligue des droits humains</i> . Wszystkie preferowane warianty strategiczne będą odpowiadać celowi leżącemu w interesie ogólnym – jakim jest skuteczne zarządzanie zewnętrznymi granicami strefy Schengen oraz zwalczanie poważnej przestępczości i terroryzmu – i będą ograniczać się ściśle do tego, co jest konieczne i proporcjonalne do osiągnięcia tego celu.
D. Działania następcze
Kiedy nastąpi przegląd przyjętej polityki?
Komisja zapewni wprowadzenie niezbędnych ustaleń dotyczących monitorowania funkcjonowania proponowanych środków i ich oceny w odniesieniu do głównych celów polityki. Po rozpoczęciu stosowania nowych instrumentów API Komisja przedłoży Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające wdrożenie tych instrumentów i ich wartość dodaną. Sprawozdanie to będzie zawierać również informacje o wszelkich bezpośrednich lub pośrednich skutkach dla praw podstawowych. Będzie ono zawierać analizę osiągniętych rezultatów pod kątem wyznaczonych celów i ocenę aktualności przesłanek dla wprowadzenia tych komponentów oraz wszelkich konsekwencji w kontekście przyszłych wariantów. W tym celu Komisja uwzględni informacje przekazane przez państwa członkowskie oraz wszelkie inne istotne informacje związane z wykonaniem tych dwóch instrumentów. Co więcej, przekazywanie danych API do interfejsu przewoźnika i ich przesłanie do właściwych organów krajowych za pomocą routera API ułatwi Komisji wykonywanie jej zadań związanych z oceną i egzekwowaniem prawa przez dostarczenie jej wiarygodnych statystyk dotyczących ilości przekazywanych danych oraz lotów, w odniesieniu do których dane API będą wymagane.