Rada
Unii Europejskiej

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

15719/22

Międzyinstytucjonalny numer referencyjny:
2022/0425 (COD)

IXIM 292
ENFOPOL 639
AVIATION 319
DATAPROTECT 363
JAI 1678
CODEC 2012
IA 223

WNIOSEK

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.:	COM(2022) 731 final
Dotyczy:	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 COM(2022) 731 final.

Zał.: COM(2022) 731 final

KOMISJA
EUROPEJSKA

Strasburg, dnia 13.12.2022 r.
COM(2022) 731 final

2022/0425 (COD)

Wniosek

ROZPORZĄDZENIE 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

{SWD(2022) 424 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W ostatnim dziesięcioleciu w UE i innych częściach świata odnotowano wzrost poważnej i zorganizowanej przestępczości. Zgodnie z przeprowadzoną przez Europol oceną zagrożenia poważną i zorganizowaną przestępczością w UE większość przestępczości zorganizowanej wiąże się z podróżami międzynarodowymi, które zazwyczaj mają na celu przemyt ludzi, narkotyków lub innych nielegalnych towarów do UE. W szczególności przestępcy często korzystają z głównych portów lotniczych w UE oraz z mniejszych regionalnych portów lotniczych obsługujących tanie linie lotnicze[1]. Również w sprawozdaniu Europolu dotyczącym sytuacji i tendencji w dziedzinie terroryzmu stwierdzono, że zagrożenie terrorystyczne w UE jest nadal realne i poważne[2], i wskazano, że większość operacji terrorystycznych ma charakter międzynarodowy i obejmuje kontakty transgraniczne lub podróże poza UE. W tym kontekście informacje o osobach podróżujących drogą lotniczą są dla organów ścigania ważnym narzędziem zwalczania poważnej przestępczości i terroryzmu w UE.

Dane osób podróżujących drogą lotniczą obejmują dane pasażera przekazywane przed podróżą (API) oraz dane dotyczące przelotu pasażera (PNR), które – gdy są wykorzystywane łącznie – są szczególnie skuteczne w identyfikacji osób podróżujących stanowiących zagrożenie i w potwierdzaniu schematu podróży osób podejrzanych. Gdy pasażer kupuje bilet u przewoźnika lotniczego, system rezerwacji przewoźnika generuje dane PNR do celów normalnej działalności przewoźnika. Obejmuje to dane dotyczące kompletnej trasy podróży, dane dotyczące płatności, dane kontaktowe i specjalne wnioski pasażera. W przypadku gdy taki obowiązek ma zastosowanie, dane PNR są przesyłane do jednostki do spraw informacji o pasażerach (JIP) kraju docelowego i często kraju wyjazdu.

W UE w 2016 r. przyjęto dyrektywę w sprawie danych PNR[3], aby zagwarantować, by wszystkie państwa członkowskie wdrożyły przepisy dotyczące gromadzenia danych PNR od przewoźników lotniczych w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, bez uszczerbku dla obowiązujących przepisów UE dotyczących obowiązku gromadzenia przez przewoźników lotniczych zbioru danych API zgodnie z dyrektywą w sprawie danych API[4]. Zgodnie z dyrektywą w sprawie danych PNR państwa członkowskie muszą przyjąć środki niezbędne do zapewnienia, by przewoźnicy lotniczy przekazywali dane PNR w zakresie, w jakim już zbierają takie dane w ramach swojej normalnej działalności.

---

1 Europol, Ocena zagrożenia poważną i zorganizowaną przestępczością w Unii Europejskiej (SOCTA), 2021. https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

2 Europol, Sprawozdanie dotyczące sytuacji i tendencji w dziedzinie terroryzmu, 2021. https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf

3 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.

4 Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów.

Dyrektywa w sprawie danych PNR umożliwia wspólne przetwarzanie zarówno danych API, jak i danych PNR, ponieważ definicja danych PNR obejmuje „[w]szelkie zebrane dane pasażera przekazane przed podróżą (dane API)”[5]. Dyrektywa w sprawie danych PNR nie zobowiązuje jednak przewoźników lotniczych do gromadzenia jakichkolwiek danych poza zakresem ich normalnej działalności. W związku z tym dyrektywa w sprawie danych PNR nie prowadzi do gromadzenia pełnego zestawu danych API, ponieważ przewoźnicy lotniczy nie mają żadnego celu w ramach swojej normalnej działalności, aby gromadzić takie dane.

Tylko wtedy, gdy taki obowiązek ma zastosowanie, dane API są gromadzone przez przewoźnika lotniczego podczas odprawy pasażera (odprawa przez internet i na lotnisku). Są one następnie przesyłane właściwym służbom granicznym jako kompletny „wykaz pasażerów”, zawierający wszystkich pasażerów znajdujących się na pokładzie w momencie startu samolotu. Dane API uznaje się za informacje „zweryfikowane”, ponieważ dotyczą one osób podróżujących, które ostatecznie wsiadły na pokład statku powietrznego; dane te mogą być wykorzystywane również przez organy ścigania do identyfikacji podejrzanych i poszukiwanych osób. Dane PNR są natomiast „niezweryfikowanymi” informacjami dostarczanymi przez pasażerów. Dane PNR określonego pasażera zazwyczaj nie zawierają wszystkich potencjalnych elementów danych PNR, lecz jedynie elementy dostarczone przez pasażera lub niezbędne do rezerwacji, a tym samym do prowadzenia normalnej działalności przez przewoźnika lotniczego.

Od przyjęcia dyrektywy w sprawie danych API w 2004 r. panuje powszechna zgoda co do tego, że dane API są nie tylko kluczowym instrumentem zarządzania granicami, ale również ważnym narzędziem ochrony porządku publicznego, zwłaszcza w celu zwalczania poważnej przestępczości i terroryzmu. W związku z tym na szczeblu międzynarodowym od 2014 r. w rezolucjach Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych wielokrotnie wzywano do ustanowienia i globalnego wdrożenia systemów danych API i PNR do celów ochrony porządku publicznego[6]. Ponadto zobowiązanie państw uczestniczących Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE) do utworzenia systemu danych API potwierdza znaczenie wykorzystania tych danych w walce z terroryzmem i przestępczością międzynarodową. [7]

Jak wynika ze sprawozdania Komisji w sprawie przeglądu dyrektywy w sprawie danych PNR, wspólne przetwarzanie danych API i PNR przez właściwe organy ścigania – co oznacza, że dane PNR gromadzone przez przewoźników lotniczych do celów ich normalnej działalności i przekazywane właściwym organom ścigania są uzupełniane zobowiązaniem przewoźników lotniczych do gromadzenia i przekazywania danych API – znacznie zwiększa skuteczność walki z poważną przestępczością i terroryzmem w UE[8]. Łączne wykorzystanie danych API i danych PNR umożliwia właściwym organom krajowym potwierdzenie tożsamości pasażerów i znacznie zwiększa wiarygodność danych PNR. Takie połączone wykorzystanie danych przed przybyciem osób podróżujących umożliwia również organom ścigania dokonanie oceny i przeprowadzenie dokładniejszej kontroli jedynie tych osób, które

---

5 Zob. pkt 18 załącznika 1 do dyrektywy (UE) 2016/681.

6 Rezolucje Rady Bezpieczeństwa ONZ nr 2178(2014), 2309(2016), 2396(2017), 2482(2019), a także decyzja Rady Ministerialnej OBWE nr 6/16 z dnia 9 grudnia 2016 r. w sprawie lepszego wykorzystywania danych pasażera przekazywanych przed podróżą.

7 Decyzja Rady Ministerialnej OBWE nr 6/16 z dnia 9 grudnia 2016 r. w sprawie lepszego wykorzystywania danych pasażera przekazywanych przed podróżą.

8 Komisja Europejska, dokument roboczy służb Komisji towarzyszący sprawozdaniu z przeglądu dyrektywy 2016/681, SWD(2020) 128 final.

w oparciu o obiektywne kryteria oceny i praktyki oraz zgodnie z mającym zastosowanie prawem najprawdopodobniej stanowią zagrożenie dla bezpieczeństwa. Ułatwia to podróżowanie wszystkim innym pasażerom i zmniejsza ryzyko poddania pasażerów kontroli po przybyciu przez właściwe organy w oparciu o elementy uznaniowe, takie jak pochodzenie rasowe lub etniczne, które mogą być przez organy ścigania niesłusznie wiązane z ryzykiem dla bezpieczeństwa.

Obecne ramy prawne UE regulują jednak jedynie wykorzystywanie danych PNR do zwalczania poważnej przestępczości i terroryzmu, nie regulują natomiast tego konkretnie w odniesieniu do danych API, o które można wystąpić wyłącznie w przypadku lotów z państw trzecich, co prowadzi do powstania luki w zakresie bezpieczeństwa, zwłaszcza w odniesieniu do lotów wewnątrzunijnych, w przypadku których państwa członkowskie zwracają się do przewoźników lotniczych o przekazywanie danych PNR. Jednostki do spraw informacji o pasażerach uzyskują najbardziej skuteczne wyniki operacyjne w odniesieniu do lotów, w przypadku których gromadzone są zarówno dane API, jak i dane PNR. Oznacza to, że właściwe organy ścigania nie mogą korzystać z wyników wspólnego przetwarzania danych API i danych PNR dotyczących lotów w obrębie UE, w odniesieniu do których przekazywane są wyłącznie dane PNR.

Aby wyeliminować tę lukę, w strategii Komisji z czerwca 2021 r. na rzecz w pełni funkcjonującej i odpornej strefy Schengen wezwano do szerszego wykorzystywania danych API w połączeniu z danymi PNR w odniesieniu do lotów wewnątrz strefy Schengen, aby znacznie zwiększyć bezpieczeństwo wewnętrzne, zgodnie z podstawowym prawem do ochrony danych osobowych i podstawowym prawem do swobodnego przemieszczania się[9].

Rozporządzenie, którego dotyczy wniosek, ma zatem na celu ustanowienie lepszych przepisów dotyczących gromadzenia i przekazywania danych API przez przewoźników lotniczych do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Aby zapewnić zgodność z odpowiednimi prawami podstawowymi zapisanymi w Karcie praw podstawowych Unii Europejskiej („Karta”), w szczególności z prawem do prywatności i prawem do ochrony danych osobowych, a także z wynikającymi z tego wymogami konieczności i proporcjonalności, wniosek jest – jak wyjaśniono poniżej – starannie zredukowany pod względem zakresu i zawiera ścisłe ograniczenia i zabezpieczenia w zakresie ochrony danych osobowych.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Proponowane przepisy dotyczące gromadzenia i przekazywania danych API do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania są dostosowane do mających zastosowanie przepisów dotyczących przetwarzania danych PNR, jak określono w dyrektywie w sprawie danych PNR[10]. Uwzględniają wykładnię Trybunału Sprawiedliwości Unii Europejskiej zawartą w jego niedawnym orzecznictwie, w szczególności to, co określono w tym orzecznictwie w sprawie przetwarzania danych PNR w odniesieniu do lotów wewnątrzunijnych, a mianowicie że przekazywanie danych PNR właściwym organom państw członkowskich w odniesieniu do lotów wewnątrzunijnych musi być selektywne i nie może

[9] COM(2021) 277 final z 2.6.2021.

[10] Dyrektywa w sprawie danych PNR określa warunki przetwarzania przedmiotowych danych, takie jak zaangażowane właściwe organy (art. 7), okres zatrzymywania danych (art. 12) i ochrona danych osobowych (art. 13).

być systematyczne, chyba że jest uzasadnione rzeczywistym i aktualnym lub możliwym do przewidzenia zagrożeniem terrorystycznym[11].

W zakresie, w jakim proponowane rozporządzenie i przepisy dyrektywy w sprawie danych PNR mogą się pokrywać, biorąc pod uwagę, że – jak wspomniano – na podstawie dyrektywy definicja „danych PNR" obejmuje „[w]szelkie zebrane dane pasażera przekazane przed podróżą (dane API)", przepisy proponowanego rozporządzenia mają pierwszeństwo, zważywszy, że są to zarówno *lex specialis*, jak i *lex posterior*. Na podstawie dyrektywy w sprawie danych PNR państwa członkowskie muszą przyjąć niezbędne środki w celu zapewnienia, by przewoźnicy lotniczy przekazywali dane PNR w zakresie, w jakim już zbierają takie dane w ramach swojej normalnej działalności; proponowane rozporządzenie nakłada natomiast na przewoźników lotniczych obowiązek gromadzenia danych API w określonych sytuacjach oraz przekazywania tych danych w określony sposób. Proponowane rozporządzenie uzupełnia zatem dyrektywę w sprawie danych PNR, ponieważ gwarantuje, że we wszystkich przypadkach, w których właściwe organy ścigania – tj. jednostki do spraw informacji o pasażerach – otrzymują dane PNR na podstawie dyrektywy w sprawie danych PNR, przewoźnicy lotniczy mają obowiązek gromadzenia i przekazywania tym właściwym organom również danych API.

Po przekazaniu danych API do jednostek do spraw informacji o pasażerach (JIP) ustanowionych dyrektywą w sprawie danych PNR, przepisy dotyczące późniejszego przetwarzania danych API przez JIP – poza ograniczonymi wymogami w tym zakresie określonymi w proponowanym rozporządzeniu – są określone w dyrektywie w sprawie danych PNR. Jak wspomniano, dyrektywa w sprawie danych PNR umożliwia wspólne przetwarzanie danych API i danych PNR, ponieważ definicja danych PNR w dyrektywie obejmuje „[w]szelkie zebrane dane pasażera przekazane przed podróżą (dane API)", a zatem również dane API otrzymane przez JIP zgodnie z proponowanym rozporządzeniem. W związku z tym zastosowanie mają przepisy art. 6 oraz art. 9 i nast. dyrektywy w sprawie danych PNR dotyczące kwestii takich jak dokładne cele przetwarzania, okresy zatrzymania danych, usuwanie, wymiana informacji, przekazywanie przez państwa członkowskie do państw trzecich oraz szczegółowe przepisy dotyczące ochrony takich danych osobowych.

Zastosowanie będą miały ponadto powszechnie obowiązujące akty prawa Unii zgodnie z określonymi w nich warunkami. Jeżeli chodzi o przetwarzanie danych osobowych, odnosi się to w szczególności do ogólnego rozporządzenia o ochronie danych (RODO)[12], dyrektywy o ochronie danych w sprawach karnych[13] i rozporządzenia o ochronie danych przetwarzanych przez organy UE[14]. Niniejszy wniosek nie ma wpływu na te akty.

---

11 Wyrok TSUE w sprawie C-817/19 *Ligue des droits humains*.

12 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.

13 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.

14 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

Zastosowanie wyżej wymienionych aktów prawa Unii do przetwarzania danych API otrzymanych na podstawie rozporządzenia, którego dotyczy niniejszy wniosek, oznacza, że państwa członkowskie stosują prawo Unii w rozumieniu art. 51 ust. 1 Karty, co z kolei oznacza, że zastosowanie mają również przepisy Karty. W szczególności przepisy tych aktów prawa UE należy interpretować w świetle Karty.

Zapewniając spójność z przepisami określonymi we wniosku dotyczącym rozporządzenia w sprawie gromadzenia i przekazywania danych API w celu usprawnienia kontroli granicznej oraz skuteczność przekazywania danych API, niniejszy wniosek nakłada na przewoźników lotniczych obowiązek gromadzenia tego samego zestawu danych API i przekazywania ich do tego samego routera ustanowionego na podstawie tego równolegle proponowanego rozporządzenia.

Gromadzenie danych API z dokumentów podróży jest również spójne z wytycznymi ICAO dotyczącymi dokumentów podróży odczytywanych maszynowo[15], które to wytyczne zostały transponowane do rozporządzenia 2019/1157 w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii, dyrektywy Rady 2019/997 ustanawiającej unijny tymczasowy dokument podróży oraz rozporządzenia 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży. To przyjęcie tych aktów umożliwiło automatyczne pobieranie kompletnych danych wysokiej jakości z dokumentów podróży.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Właściwą podstawą prawną niniejszego wniosku dotyczącego rozporządzenia w sprawie gromadzenia i przekazywania danych API w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, z uwzględnieniem jego celu i przewidzianych środków, są art. 82 ust. 1 lit. d) i art. 87 ust. 2 lit. a) Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

Na podstawie art. 82 ust. 1 lit. d) TFUE Unia jest uprawniona do przyjmowania środków mających na celu ułatwianie współpracy między organami sądowymi lub równoważnymi organami państw członkowskich w ramach ścigania karnego i wykonywania orzeczeń. Na podstawie art. 87 ust. 2 lit. a) TFUE Unia jest uprawniona do ustanowienia środków dotyczących gromadzenia, przechowywania, przetwarzania, analizowania i wymiany istotnych informacji do celów współpracy policyjnej w UE.

W związku z tym podstawa prawna wykorzystana w niniejszym wniosku jest taka sama jak podstawa prawna wykorzystana w przypadku dyrektywy w sprawie danych PNR, co jest właściwe, biorąc pod uwagę nie tylko, że proponowane rozporządzenie ma zasadniczo ten sam cel, ale również że ma ono na celu uzupełnienie dyrektywy w sprawie danych PNR.

---

[15] ICAO, dokument 9303, Machine Readable Travel Documents (Dokumenty podróży odczytywane maszynowo), wydanie ósme, 2021, dostępny pod adresem: https://www.icao.int/publications/documents/9303_p1_cons_en.pdf

- **Pomocniczość**

Organy ścigania muszą dysponować skutecznymi narzędziami do walki z terroryzmem i poważną przestępczością. Ponieważ najpoważniejsze przestępstwa i akty terroryzmu wiążą się z podróżami międzynarodowymi, często drogą lotniczą, dane PNR okazały się bardzo skuteczne pod względem ochrony bezpieczeństwa wewnętrznego UE. Ponadto dochodzenia prowadzone przez właściwe organy państw członkowskich w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania są w dużej mierze uzależnione od współpracy międzynarodowej i transgranicznej.

Na obszarze bez kontroli na granicach wewnętrznych gromadzenie, przetwarzanie i wymiana danych pasażerów, w tym danych PNR i API, przez państwa członkowskie są również skutecznymi środkami wyrównawczymi. Dzięki spójnym działaniom na szczeblu UE wniosek przyczyni się do zwiększenia bezpieczeństwa państw członkowskich, a tym samym całej UE.

Dyrektywa w sprawie danych API jest częścią dorobku Schengen związanego z przekraczaniem granic zewnętrznych. Nie reguluje ona zatem gromadzenia i przekazywania danych API w odniesieniu do lotów wewnątrzunijnych. Wobec braku danych API uzupełniających dane PNR w odniesieniu do tych lotów państwa członkowskie wdrożyły szereg różnych środków mających na celu zrekompensowanie braku danych dotyczących tożsamości pasażerów. Obejmuje to fizyczne kontrole zgodności w celu weryfikacji danych dotyczących tożsamości między dokumentem podróży a kartą pokładową, co generuje nowe problemy, nie rozwiązując problemu braku danych API.

Działania na szczeblu UE pomogą zapewnić stosowanie zharmonizowanych przepisów dotyczących ochrony praw podstawowych, w szczególności ochrony danych osobowych, w państwach członkowskich. Różne systemy państw członkowskich, które ustanowiły już podobne mechanizmy lub uczynią to w przyszłości, mogą mieć negatywny wpływ na przewoźników lotniczych, ponieważ mogą być oni zmuszeni do spełnienia szeregu rozbieżnych wymogów krajowych, na przykład w odniesieniu do rodzajów informacji, które mają być przekazywane, oraz warunków, na jakich informacje te muszą być przekazywane państwom członkowskim. Różnice te utrudnią skuteczną współpracę między państwami członkowskimi mającą na celu zapobieganie przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie. Takie zharmonizowane przepisy mogą zostać ustanowione jedynie na szczeblu UE.

Ponieważ cele wniosku nie mogą zostać w wystarczającym stopniu osiągnięte przez państwa członkowskie i mogą zostać lepiej osiągnięte na szczeblu UE, można stwierdzić, że UE jest zarówno uprawniona, jak i lepiej predestynowana do działania niż państwa członkowskie działające niezależnie. Wniosek jest zatem zgodny z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej.

- **Proporcjonalność**

Zgodnie z zasadą proporcjonalności określoną w art. 5 ust. 4 Traktatu UE konieczne jest dostosowanie charakteru i intensywności danego działania do zidentyfikowanego problemu. Wszystkie kwestie poruszone w tej inicjatywie ustawodawczej wymagają, w taki czy inny sposób, podjęcia działań ustawodawczych na szczeblu UE, które umożliwią państwom członkowskim skuteczne zajęcie się tymi kwestiami.

Proponowane przepisy dotyczące gromadzenia i przekazywania danych API, podlegających ścisłym ograniczeniom i zabezpieczeniom, przyczynią się do lepszego zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. W związku z tym proponowane przepisy odpowiadają stwierdzonej potrzebie zwiększenia bezpieczeństwa wewnętrznego, gdyż stanowią skuteczną odpowiedź na problem wynikający z braku wspólnego przetwarzania danych API i danych PNR, w tym w odniesieniu do lotów wewnątrzunijnych, w przypadku których państwa członkowskie otrzymują dane PNR.

Zakres wniosku ogranicza się do tego, co niezbędne, tj. ogranicza się do tych elementów, które wymagają zharmonizowanego podejścia na szczeblu UE, a mianowicie do celów, do których dane API mogą być wykorzystywane przez JIP, do elementów danych, które należy gromadzić, oraz do środków gromadzenia i przekazywania danych API od osób podróżujących. Dzięki przekazywaniu danych API do routera przewoźnicy lotniczy nie będą zmuszeni do utrzymania połączeń z jednostkami do spraw informacji o pasażerach; przyniesie to korzyści skali, a jednocześnie ograniczy zakres błędów i nadużyć. Cel wniosku obejmuje wyłącznie przestępstwa terrorystyczne i poważną przestępczość, zgodnie z zawartą w nim definicją, ze względu na ich poważny charakter i wymiar ponadnarodowy.

Aby ograniczyć ingerencję w prawa pasażerów do tego, co niezbędne, we wniosku określono szereg zabezpieczeń. Dokładniej rzecz ujmując, przetwarzanie danych API na podstawie proponowanego rozporządzenia ogranicza się do zamkniętego i okrojonego wykazu danych API. Poza tymi danymi nie należy gromadzić żadnych dodatkowych danych dotyczących tożsamości. Ponadto proponowane rozporządzenie przewiduje jedynie przepisy dotyczące gromadzenia i przekazywania danych API za pośrednictwem routera do JIP w ograniczonych celach określonych w tym rozporządzeniu i nie reguluje dalszego przetwarzania danych API przez JIP, biorąc pod uwagę, że – jak wyjaśniono powyżej – kwestia ta jest objęta innymi aktami prawa Unii (dyrektywa w sprawie danych PNR, prawo o ochronie danych osobowych, Karta). Funkcje routera, a w szczególności jego zdolność do gromadzenia i dostarczania wyczerpujących informacji statystycznych, zapewniają również wsparcie w monitorowaniu wdrażania niniejszego rozporządzenia przez przewoźników lotniczych i jednostki do spraw informacji o pasażerach. Przewidziano także pewne zabezpieczenia szczególne, takie jak przepisy dotyczące rejestrów oraz ochrony i bezpieczeństwa danych osobowych.

Aby zapewnić konieczność i proporcjonalność przetwarzania danych na podstawie proponowanego rozporządzenia, w szczególności w przypadku gromadzenia i przekazywania danych API w odniesieniu do lotów wewnątrzunijnych, państwa członkowskie będą otrzymywać dane API wyłącznie w odniesieniu do tych lotów wewnątrzunijnych, które wybrały zgodnie z wyżej wymienionym orzecznictwem TSUE. Dalsze przetwarzanie danych API przez JIP podlegałoby ponadto ograniczeniom i zabezpieczeniom ustanowionym w dyrektywie w sprawie danych PNR, zgodnie z wykładnią TSUE w sprawie *Ligue des droits humains*[16] w świetle Karty.

- **Wybór instrumentu**

Proponowanym instrumentem jest rozporządzenie. W związku z tym, że proponowane środki muszą być stosowane bezpośrednio i jednolicie we wszystkich państwach członkowskich, odpowiednim instrumentem prawnym jest rozporządzenie.

[16] TSUE, wyrok z dnia 21 czerwca 2022 r., sprawa C-817/19 *Ligue des droits humains*.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

• Ocena *ex post* obowiązującego prawodawstwa

Dyrektywa w sprawie danych API nie uniemożliwia przetwarzania danych API do celów ochrony porządku publicznego zgodnie z przepisami krajowymi i z zastrzeżeniem wymogów dotyczących ochrony danych osobowych. Jak jednak stwierdzono w ocenie dyrektywy w sprawie danych API, wdrożenie tej możliwości we wszystkich państwach członkowskich jest problematyczne, co prowadzi do luk w zakresie bezpieczeństwa ze względu na brak określonych przez UE kryteriów gromadzenia i przekazywania danych API do celów ochrony porządku publicznego[17]:

– Cel ochrony porządku publicznego jest szeroko rozumiany w prawie krajowym niektórych państw członkowskich, począwszy od przestępstw administracyjnych, poprawy bezpieczeństwa wewnętrznego i porządku publicznego, a skończywszy na walce z terroryzmem i ochronie bezpieczeństwa narodowego. W ocenie dyrektywy w sprawie danych API wskazano również, że skuteczne wykorzystywanie danych API do celów ochrony porządku publicznego wymagałoby specjalnego instrumentu prawnego służącego temu odrębnemu celowi[18].

– Różnorodność celów gromadzenia danych API zwiększa złożoność kwestii zapewniania zgodności z unijnymi ramami ochrony danych osobowych. Wymóg usunięcia danych API w ciągu 24 godzin ustanowiono jedynie w przypadku wykorzystywania danych API do głównego celu dyrektywy w sprawie danych API, a mianowicie do zarządzania granicami zewnętrznymi. Nie jest jasne, czy wymóg ten ma zastosowanie również do przetwarzania danych do celów ochrony porządku publicznego.

– Zbiór danych API, o który można zwrócić się do przewoźników do celów ochrony porządku publicznego, obok praktyki niektórych państw członkowskich polegającej na żądaniu danych API wykraczających poza niewyczerpujący wykaz zawarty w dyrektywie w sprawie danych API, stwarza dodatkowe przeszkody dla przewoźników lotniczych w spełnianiu różnych wymogów przy przewozie pasażerów do UE.

– Podobnie dyrektywa w sprawie danych API nie zawiera żadnych informacji na temat lotów, w odniesieniu do których można występować o dane API, ani na temat tego, któremu organowi dane API powinny być przekazywane, ani na temat warunków dostępu do takich danych do celów ochrony porządku publicznego.

• Konsultacje z zainteresowanymi stronami

Przygotowanie niniejszego wniosku obejmowało szeroki zakres konsultacji z zainteresowanymi stronami, w tym z organami państw członkowskich (właściwymi służbami granicznymi, jednostkami do spraw informacji o pasażerach), przedstawicielami

[17] Komisja Europejska, dokument roboczy służb Komisji, Ocena dyrektywy Rady 2004/82/WE w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (dyrektywa w sprawie danych API), Bruksela, 8.9.2020, SWD(2020) 174 final, s. 26 i 43.

[18] SWD(2020) 174, s. 57.

branży transportowej i poszczególnymi przewoźnikami. Wkład wniosły również agencje UE, na przykład Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex), Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) oraz Agencja Praw Podstawowych Unii Europejskiej (FRA). Uwzględniono również opinie i informacje zwrotne otrzymane podczas konsultacji publicznych przeprowadzonych pod koniec 2019 r. w ramach oceny dyrektywy w sprawie API[19].

W ramach konsultacji prowadzonych w kontekście przygotowania oceny skutków stanowiącej podstawę niniejszego wniosku zebrano informacje zwrotne od zainteresowanych stron za pomocą różnych metod. Działania te obejmowały w szczególności wstępną ocenę skutków, zewnętrzne badanie uzupełniające i cykl warsztatów technicznych.

W dniach od 5 czerwca 2020 r. do 14 sierpnia 2020 r. można było nadsyłać opinie w sprawie wstępnej oceny skutków; otrzymano łącznie siedem opinii na temat rozszerzenia zakresu przyszłej dyrektywy w sprawie API, jakości danych, kar, związku z danymi API i danych PNR oraz ochrony danych osobowych[20].

Zewnętrzne badanie uzupełniające przeprowadzono w oparciu o badanie źródeł wtórnych, wywiady i ankiety z ekspertami tematycznymi, którzy zbadali różne możliwe środki przetwarzania danych API na podstawie jasnych zasad ułatwiających legalne podróżowanie, spójnych z interoperacyjnością systemów informacyjnych UE, wymogami UE w zakresie ochrony danych osobowych oraz innymi istniejącymi instrumentami UE i normami międzynarodowymi.

Służby Komisji zorganizowały również cykl warsztatów technicznych z ekspertami z państw członkowskich i państw stowarzyszonych w ramach Schengen. Warsztaty te miały na celu zgromadzenie ekspertów w celu wymiany poglądów na temat możliwych wariantów, które przewidziano, aby wzmocnić przyszłe ramy danych API do celów zarządzania granicami, a także zwalczania przestępczości i terroryzmu.

Więcej szczegółowych informacji na temat konsultacji z zainteresowanymi stronami zamieszczono w załączonej ocenie skutków (załącznik 2).

- **Ocena skutków**

Zgodnie z wytycznymi dotyczącymi lepszego stanowienia prawa Komisja przeprowadziła ocenę skutków przedstawioną w towarzyszącym dokumencie roboczym służb Komisji [odniesienie]. Rada ds. Kontroli Regulacyjnej oceniła projekt oceny skutków podczas posiedzenia w dniu 28 września 2022 r., a w dniu 30 września 2022 r. wydała pozytywną opinię.

W świetle stwierdzonych problemów, związanych z gromadzeniem i przekazywaniem danych API, w ocenie skutków przeanalizowano warianty strategiczne dotyczące zakresu gromadzenia danych API do celów zarządzania granicami zewnętrznymi i do celów ochrony porządku publicznego oraz warianty dotyczące sposobów poprawy jakości danych API. Jeżeli chodzi o gromadzenie danych API do celów ochrony porządku publicznego, w ocenie

[19] SWD(2020) 174.

[20] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12434-Border-law-enforcement-advance-air-passenger-information-API-revised-rules_pl

skutków rozważono, z jednej strony, gromadzenie danych API w odniesieniu do wszystkich lotów pozaunijnych, a z drugiej – gromadzenie danych API w odniesieniu do wszystkich lotów pozaunijnych i wybranych lotów wewnątrzunijnych. W ocenie skutków przeanalizowano ponadto warianty poprawy jakości danych API – gromadzenie danych API w sposób zautomatyzowany i ręcznie albo gromadzenie danych API wyłącznie w sposób zautomatyzowany.

W oparciu o ustalenia zawarte w sprawozdaniu z oceny skutków preferowany wariant instrumentu API do celów ochrony porządku publicznego zakłada gromadzenie danych API w odniesieniu do wszystkich lotów do UE i poza UE, a także wybranych lotów wewnątrzunijnych, w przypadku których przekazywane są dane PNR. Zwiększy to w znacznym stopniu solidność niezbędnej analizy odpowiednich danych dotyczących osób podróżujących drogą lotniczą w walce z poważną przestępczością i terroryzmem, przy czym jednostki do spraw informacji o pasażerach skorzystają z dostępności danych API, weryfikowanych, a tym samym o wyższej jakości, w celu identyfikacji osób zaangażowanych w poważną przestępczość lub terroryzm. Gromadzenie i przekazywanie danych API do celów ochrony porządku publicznego opiera się na zdolnościach opracowanych w celu przekazywania danych API za pośrednictwem routera na potrzeby zarządzania granicami zewnętrznymi; oznacza to brak dodatkowych kosztów dla eu-LISA. Przewoźnicy lotniczy przekazują dane API wyłącznie do routera, który następnie przesyła te dane do jednostki do spraw informacji o pasażerach każdego odpowiedniego państwa członkowskiego. W ocenie skutków stwierdzono, że jest to rozwiązanie racjonalne pod względem kosztów dla przewoźników lotniczych, gdyż zmniejsza część kosztów transmisji ponoszoną przez przewoźników lotniczych, ograniczając jednocześnie możliwości wystąpienia błędów lub nadużyć. Niemniej jednak, inaczej niż ma to miejsce obecnie, zgodnie z proponowanym rozporządzeniem przewoźnicy lotniczy musieliby gromadzić i przekazywać dane API w odniesieniu do wszystkich lotów objętych rozporządzeniem, w tym również lotów wewnątrzunijnych, niezależnie od potrzeb wynikających z ich normalnej działalności. Wniosek jest spójny z celem neutralności klimatycznej określonym w Europejskim prawie o klimacie[21] oraz celami Unii na 2030 r. i 2040 r.

- **Prawa podstawowe**

Inicjatywa przewiduje przetwarzanie danych osobowych osób podróżujących, a zatem ogranicza korzystanie z podstawowego prawa do ochrony danych osobowych zagwarantowanego w art. 8 Karty i art. 16 TFUE. Jak podkreślił Trybunał Sprawiedliwości Unii Europejskiej (TSUE)[22], prawo do ochrony danych osobowych nie stanowi prerogatywy o charakterze absolutnym, ale wszelkie ograniczenia powinny być oceniane w świetle funkcji społecznej tego prawa i muszą być zgodne z kryteriami określonymi w art. 52 ust. 1 Karty[23]. Ochrona danych osobowych jest również ściśle związana z poszanowaniem prawa do prywatności w ramach prawa do poszanowania życia prywatnego i rodzinnego na mocy art. 7 Karty.

---

21 Art. 2 ust. 1 rozporządzenia (UE) 2021/1119 z dnia 30 czerwca 2021 r. ustanawiającego ramy na potrzeby osiągnięcia neutralności klimatycznej (Europejskie prawo o klimacie).

22 TSUE, wyrok z dnia 9 listopada 2010 r., sprawy połączone C-92/09 i C-93/09 *Volker und Markus Schecke* oraz *Eifert* [2010] ECR I-0000.

23 Zgodnie z art. 52 ust. 1 Karty, można ograniczyć korzystanie z prawa do ochrony danych, o ile takie ograniczenia są przewidziane ustawą i szanują istotę tych praw i wolności, i o ile, z zastrzeżeniem zasady proporcjonalności, są one konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób.

Jeżeli chodzi o gromadzenie i przekazywanie danych API w odniesieniu do wybranych lotów wewnątrzunijnych, niniejsza inicjatywa ma również wpływ na korzystanie z podstawowego prawa do swobodnego przemieszczania się przewidzianego w art. 45 Karty i art. 21 TFUE. Według TSUE takie ograniczenie swobody przemieszczania się osób może być uzasadnione jedynie wtedy, gdy opiera się na obiektywnych względach i jest proporcjonalne do uzasadnionego celu przepisów krajowych[24].

Na podstawie proponowanego rozporządzenia gromadzenie i przekazywanie danych API może odbywać się wyłącznie w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, zgodnie z definicją zawartą w dyrektywie w sprawie danych PNR. Przepisy zawarte w niniejszym wniosku przewidują jednolite kryteria gromadzenia i przekazywania danych API w odniesieniu do lotów pozaunijnych (przylotów i odlotów) z jednej strony oraz wybranych lotów wewnątrzunijnych z drugiej strony, w oparciu o ocenę przeprowadzoną przez państwa członkowskie i poddawaną regularnym przeglądom, zgodnie z wymogami określonymi przez Trybunał Sprawiedliwości w sprawie *Ligue des droits humains*. Spoczywający na przewoźnikach lotniczych obowiązek gromadzenia i przekazywania danych API do routera obejmuje wszystkie loty wewnątrzunijne. Przekazywanie danych API przez router do JIP jest rozwiązaniem technicznym, które ograniczy przekazywanie danych API do jednostek do spraw informacji o pasażerach wyłącznie w odniesieniu do wybranych lotów, bez ujawniania informacji poufnych na temat tego, które loty wewnątrzunijne wybrano. Takie informacje należy traktować jako poufne ze względu na ryzyko obejścia przepisów, które istniałoby w przypadku, gdyby informacje podano do wiadomości publicznej, a w szczególności gdyby poznały je osoby zaangażowane w poważną przestępczość lub działalność terrorystyczną.

Obowiązkowe stosowanie zautomatyzowanych środków przez przewoźników lotniczych w celu gromadzenia niektórych danych API od osób podróżujących może prowadzić do powstania ryzyka, w tym z punktu widzenia ochrony danych osobowych. Takie ryzyko zostało jednak ograniczone i złagodzone. Po pierwsze, wymóg ten ma zastosowanie jedynie w odniesieniu do niektórych danych API, w przypadku których środki zautomatyzowane mogą być wykorzystywane w sposób odpowiedzialny, tj. w przypadku danych nadających się do odczytu maszynowego zawartych w dokumentach osób podróżujących. Po drugie, proponowane rozporządzenie zawiera wymogi dotyczące zautomatyzowanych środków, jakie mają być zastosowane, które to wymogi mają zostać doprecyzowane w akcie delegowanym. Przewidziano również szereg zabezpieczeń, takich jak rejestry, szczegółowe przepisy dotyczące ochrony danych osobowych i skuteczny nadzór.

Ponadto, o ile – z wyjątkiem przepisu zapewniającego zgodność z zasadą ograniczenia celu – proponowane rozporządzenie nie reguluje wykorzystania przez właściwe służby graniczne danych API, które otrzymują na jego podstawie, biorąc pod uwagę, że – jak wyjaśniono powyżej – kwestia ta jest już objęta innymi przepisami, w celu zachowania jasności przypomina się w motywach, że takie wykorzystanie danych nie może prowadzić do jakiejkolwiek dyskryminacji zakazanej na podstawie art. 21 Karty.

[24] TSUE, wyrok z dnia 5 czerwca 2018 r., sprawa C-673/16 *Coman.*

4. WPŁYW NA BUDŻET

Inicjatywa ustawodawcza dotycząca gromadzenia i przekazywania danych API w celu ułatwienia kontroli granic zewnętrznych oraz w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania miałaby wpływ na budżet i potrzeby kadrowe eu-LISA i właściwych organów państw członkowskich.

W przypadku eu-LISA szacuje się, że potrzebne będą dodatkowe środki w wysokości około 45 mln EUR (33 mln EUR w obecnych WRF) na utworzenie routera i 9 mln EUR rocznie od 2029 r. na techniczne zarządzanie routerem oraz około 27 dodatkowych stanowisk do zapewnienia eu-LISA zasobów niezbędnych do wykonywania zadań powierzonych jej w niniejszym proponowanym rozporządzeniu i we wniosku dotyczącym rozporządzenia w sprawie gromadzenia i przekazywania danych API w celu usprawnienia i ułatwienia kontroli na granicach zewnętrznych.

W przypadku państw członkowskich szacuje się, że potrzebne będą środki w wysokości 11 mln EUR (3 mln EUR w ramach obecnych wieloletnich ram finansowych) na modernizację niezbędnych krajowych systemów i infrastruktury dla JIP, które mogą kwalifikować się do zwrotu z Funduszu Bezpieczeństwa Wewnętrznego[25], oraz stopniowo, począwszy od 2028 r., środki w wysokości do 2 mln EUR rocznie. Każde takie uprawnienie do zwrotu będzie musiało ostatecznie zostać określone zgodnie z przepisami regulującymi te fundusze, jak również z przepisami dotyczącymi kosztów zawartymi w proponowanym rozporządzeniu.

Ze względu na ścisły związek między rozporządzeniem, którego dotyczy niniejszy wniosek, oraz proponowanym rozporządzeniem w sprawie gromadzenia i przekazywania danych API w celu ułatwienia kontroli na granicach zewnętrznych, w szczególności w odniesieniu do przekazywania danych API do routera, ocena skutków finansowych regulacji zawarta w załączniku jest identyczna w przypadku tych dwóch wniosków.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Komisja zapewni wprowadzenie niezbędnych ustaleń dotyczących monitorowania funkcjonowania proponowanych środków i ich oceny w odniesieniu do głównych celów polityki. Cztery lata po rozpoczęciu stosowania proponowanego rozporządzenia w sprawie danych API, a następnie co cztery lata Komisja przedkładałaby Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające wykonanie rozporządzenia i jego wartość dodaną. Sprawozdanie zawierałoby również informacje na temat wszelkich bezpośrednich lub pośrednich skutków dotyczących praw podstawowych. Oceniono by osiągnięte rezultaty pod kątem przyjętych uprzednio celów, przeanalizowano, czy przesłanki dla wprowadzenia rozporządzenia pozostają aktualne, a także zbadano wszelkie konsekwencje dla przyszłych wariantów.

Nałożenie na przewoźników lotniczych obowiązku gromadzenia danych API w odniesieniu do lotów pozaunijnych i wybranych lotów wewnątrzunijnych oraz wprowadzenie routera danych API umożliwi uzyskanie jaśniejszego obrazu zarówno przekazywania danych API

[25] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1149 z dnia 7 lipca 2021 r. ustanawiające Fundusz Bezpieczeństwa Wewnętrznego.

przez przewoźników lotniczych, jak i wykorzystywania danych API przez państwa członkowskie zgodnie z obowiązującymi przepisami krajowymi i unijnymi. Pomoże to Komisji w jej zadaniach związanych z oceną i egzekwowaniem przepisów, dostarczając jej wiarygodnych danych statystycznych dotyczących ilości przekazywanych danych oraz lotów, w odniesieniu do których wystąpiono o przekazanie danych API.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

W rozdziale 1 zawarto przepisy ogólne rozporządzenia, począwszy od przepisów dotyczących jego przedmiotu i zakresu, a także wykaz definicji.

W rozdziale 2 zawarto przepisy dotyczące gromadzenia, przekazywania do routera i usuwania danych API przez przewoźników lotniczych oraz przepisy dotyczące przekazywania danych API z routera do jednostek do spraw informacji o pasażerach.

W rozdziale 3 zawarto przepisy szczegółowe dotyczące rejestrów, bezpieczeństwa i monitorowania własnej działalności przez przewoźników lotniczych i JIP oraz określono, kto jest administratorem danych osobowych w związku z przetwarzaniem na podstawie rozporządzenia danych API stanowiących dane osobowe.

W rozdziale 4 zawarto przepisy dotyczące połączeń i integracji z routerem przez jednostki do spraw informacji o pasażerach i przewoźników lotniczych, a także przepisy dotyczące związanych z tym kosztów ponoszonych przez państwa członkowskie. Rozdział ten obejmuje również przepisy regulujące sytuację częściowego lub całkowitego braku technicznej możliwości korzystania z routera oraz odpowiedzialność za szkody wyrządzone routerowi.

W rozdziale 5 zawarto przepisy dotyczące nadzoru, ewentualnych kar nakładanych na przewoźników lotniczych w przypadku nieprzestrzegania przez nich obowiązków określonych w rozporządzeniu oraz przygotowania praktycznego podręcznika przez Komisję.

W rozdziale 6 zawarto zmiany innych obowiązujących instrumentów, tj. rozporządzenia (UE) 2019/818.

W rozdziale 7 zawarto przepisy końcowe rozporządzenia, które dotyczą przyjmowania aktów delegowanych, monitorowania i oceny rozporządzenia oraz jego wejścia w życie i stosowania.

2022/0425 (COD)

Wniosek

ROZPORZĄDZENIE 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

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[26],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Międzynarodowy wymiar poważnej i zorganizowanej przestępczości oraz ciągłe zagrożenie atakami terrorystycznymi na terytorium Europy wymagają działań na szczeblu Unii w celu przyjęcia odpowiednich środków, aby zapewnić bezpieczeństwo w przestrzeni wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych. Informacje na temat osób podróżujących drogą lotniczą, takie jak dane dotyczące przelotu pasażera (PNR) i w szczególności dane pasażera przekazywane przed podróżą (API), są niezbędne do identyfikacji osób podróżujących stanowiących zagrożenie, w tym tych, które nie są w inny sposób znane organom ścigania, oraz do ustanowienia powiązań między członkami grup przestępczych i do przeciwdziałania działalności terrorystycznej.

(2) Dyrektywa Rady 2004/82/WE[27] ustanawia ramy prawne gromadzenia i przekazywania danych API przez przewoźników lotniczych w celu poprawy kontroli granicznych i zwalczania nielegalnej imigracji, ale stanowi ona również, że państwa członkowskie mogą wykorzystywać dane API do celów ochrony porządku publicznego. Jednak samo stworzenie takiej możliwości prowadzi do powstania szeregu luk i niedociągnięć. W szczególności oznacza to, że dane API – pomimo ich znaczenia dla celów ochrony porządku publicznego – nie są we wszystkich przypadkach

[26] Dz.U. C z, s. .

[27] 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).

gromadzone i przekazywane przez przewoźników lotniczych do tych celów. Oznacza to również, że w przypadkach, w których państwa członkowskie skorzystały z tej możliwości, przewoźnicy lotniczy mają do czynienia z rozbieżnymi wymogami prawa krajowego dotyczącymi tego, kiedy i w jaki sposób należy gromadzić i przekazywać dane API do tych celów. Rozbieżności te prowadzą nie tylko do niepotrzebnych kosztów i komplikacji dla przewoźników lotniczych, ale mogą również zaszkodzić bezpieczeństwu wewnętrznemu Unii i skutecznej współpracy między właściwymi krajowymi organami ścigania państw członkowskich. Ponadto, ze względu na odmienny charakter celów związanych z ułatwianiem kontroli granicznych i z ochroną porządku publicznego, należy ustanowić odrębne ramy prawne dotyczące gromadzenia i przekazywania danych API dla każdego z tych celów.

(3) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681[28] określa zasady wykorzystywania danych PNR w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Zgodnie z tą dyrektywą państwa członkowskie muszą przyjąć środki niezbędne do zapewnienia, by przewoźnicy lotniczy przekazywali dane PNR, w tym zgromadzone dane API, ustanowionej na podstawie dyrektywy jednostce do spraw informacji o pasażerach („JIP") w zakresie, w jakim już zbierają takie dane w ramach swojej normalnej działalności. W związku z tym dyrektywa ta nie gwarantuje gromadzenia i przekazywania danych API we wszystkich przypadkach, ponieważ przewoźnicy lotniczy nie mają żadnego celu w ramach swojej normalnej działalności, by gromadzić pełen zestaw takich danych. Zapewnienie, by JIP otrzymywały dane API wraz z danymi PNR, jest istotne, ponieważ wspólne przetwarzanie takich danych jest niezbędne, aby właściwe organy ścigania państw członkowskich mogły skutecznie zapobiegać przestępstwom terrorystycznym i poważnej przestępczości, wykrywać je, prowadzić postępowania przygotowawcze w ich sprawie i je ścigać. W szczególności takie wspólne przetwarzanie pozwala na dokładną identyfikację pasażerów, którzy mogą wymagać dalszego sprawdzenia przez te organy zgodnie z mającymi zastosowanie przepisami. Dyrektywa ta ponadto nie precyzuje szczegółowo, które informacje stanowią dane API. Z tych powodów należy ustanowić przepisy uzupełniające zobowiązujące przewoźników lotniczych do gromadzenia, a następnie przekazywania określonego zestawu danych API; wymogi te powinny mieć zastosowanie w zakresie, w jakim przewoźnicy lotniczy są na podstawie tej dyrektywy zobowiązani do gromadzenia i przekazywania danych PNR w odniesieniu do tego samego lotu.

(4) Konieczne jest zatem ustanowienie na szczeblu Unii jasnych, zharmonizowanych i skutecznych przepisów dotyczących gromadzenia i przekazywania danych API do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

(5) Biorąc pod uwagę ścisły związek między obydwoma aktami, niniejsze rozporządzenie należy rozpatrywać jako uzupełnienie przepisów przewidzianych w dyrektywie (UE) 2016/681. W związku z tym dane API należy gromadzić i przekazywać zgodnie ze

[28] 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. L 119 z 4.5.2016, s. 132).

szczegółowymi wymogami niniejszego rozporządzenia, w tym wymogami dotyczącymi sytuacji i sposobu, w jaki należy to robić. Przepisy powyższej dyrektywy mają jednak zastosowanie do kwestii nieobjętych konkretnie niniejszym rozporządzeniem – w szczególności przepisy dotyczące późniejszego przetwarzania danych API otrzymanych przez JIP, wymiany informacji między państwami członkowskimi, warunków dostępu Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) oraz przekazywania danych do państw trzecich, zatrzymywania i depersonalizacji, a także ochrony danych osobowych. W zakresie, w jakim przepisy te mają zastosowanie, zastosowanie mają również przepisy tej dyrektywy dotyczące sankcji i krajowych organów nadzorczych. Niniejsze rozporządzenie nie powinno naruszać tych przepisów.

(6) Gromadzenie i przekazywanie danych API ma wpływ na prywatność osób fizycznych i wiąże się z przetwarzaniem danych osobowych. Aby zagwarantować pełne poszanowanie praw podstawowych, w szczególności prawa do poszanowania życia prywatnego i prawa do ochrony danych osobowych, zgodnie z Kartą praw podstawowych Unii Europejskiej („Karta"), należy przewidzieć odpowiednie ograniczenia i zabezpieczenia. W szczególności wszelkie przetwarzanie danych API, zwłaszcza danych API stanowiących dane osobowe, powinno ograniczać się do tego, co jest konieczne i proporcjonalne do osiągnięcia celów niniejszego rozporządzenia. Należy ponadto zapewnić, by gromadzenie i przekazywanie danych API na podstawie niniejszego rozporządzenia nie prowadziło do żadnej formy dyskryminacji zakazanej na mocy Karty.

(7) Ze względu na uzupełniający charakter niniejszego rozporządzenia w stosunku do dyrektywy (UE) 2016/681 obowiązki przewoźników lotniczych wynikające z niniejszego rozporządzenia powinny mieć zastosowanie do wszystkich lotów, w odniesieniu do których państwa członkowskie mają wymagać od przewoźników lotniczych przekazywania danych PNR na podstawie dyrektywy (UE) 2016/681, a mianowicie lotów – zarówno regularnych, jak i nieregularnych – zarówno między państwami członkowskimi i państwami trzecimi (loty pozaunijne), jak i między państwami członkowskimi (loty wewnątrzunijne), o ile loty te zostały wybrane zgodnie z dyrektywą (UE) 2016/681, niezależnie od miejsca siedziby przewoźników lotniczych wykonujących te loty.

(8) W związku z tym, biorąc pod uwagę, że dyrektywa (UE) 2016/681 nie obejmuje lotów krajowych, tj. lotów, które rozpoczynają się i lądują na terytorium tego samego państwa członkowskiego bez przerwy w podróży na terytorium innego państwa członkowskiego lub państwa trzeciego, a także ze względu na ponadnarodowy wymiar przestępstw terrorystycznych i poważnej przestępczości objętych niniejszym rozporządzeniem, loty takie również nie powinny być objęte niniejszym rozporządzeniem. Niniejszego rozporządzenia nie należy rozumieć jako mającego wpływ na możliwość nałożenia przez państwa członkowskie, na podstawie ich prawa krajowego i zgodnie z prawem Unii, obowiązków na przewoźników lotniczych w zakresie gromadzenia i przekazywania danych API w odniesieniu do takich lotów krajowych.

(9) Ze względu na ścisły związek między odnośnymi aktami prawa Unii oraz w celu zapewnienia spójności i zgodności definicje zawarte w niniejszym rozporządzeniu powinny być w jak największym stopniu dostosowane do definicji określonych w dyrektywie (UE) 2016/681 i rozporządzeniu (UE) [w sprawie danych API

w obszarze zarządzania granicami][29] oraz powinny być interpretowane i stosowane w świetle tych definicji.

(10) W szczególności informacje łącznie stanowiące dane API, które mają być gromadzone, a następnie przekazywane na podstawie niniejszego rozporządzenia, powinny być informacjami wymienionymi w sposób jasny i wyczerpujący w rozporządzeniu (UE) [w sprawie danych pasażera przekazywanych przed podróżą w obszarze zarządzania granicami] i obejmować zarówno informacje dotyczące każdego pasażera, jak i informacje dotyczące lotu tej osoby podróżującej. Na podstawie niniejszego rozporządzenia takie informacje o locie powinny obejmować informacje na temat przejścia granicznego wjazdu na terytorium danego państwa członkowskiego wyłącznie w stosownych przypadkach, tj. nie w przypadku, gdy dane API odnoszą się do lotów wewnątrzunijnych.

(11) Aby zapewnić w jak największym stopniu spójne podejście do gromadzenia i przekazywania danych API przez przewoźników lotniczych, przepisy określone w niniejszym rozporządzeniu należy w stosownych przypadkach dostosować do przepisów określonych w rozporządzeniu (UE) [w sprawie danych API w obszarze zarządzania granicami]. Dotyczy to w szczególności przepisów odnoszących się do jakości danych, wykorzystania przez przewoźników lotniczych zautomatyzowanych środków do gromadzenia danych, dokładnego sposobu przekazywania zgromadzonych danych API do routera oraz usunięcia danych API.

(12) Aby zapewnić wspólne przetwarzanie danych API i danych PNR w celu skutecznej walki z terroryzmem i poważną przestępczością w Unii, a jednocześnie zminimalizować ingerencję w prawa podstawowe pasażerów chronione na podstawie Karty, JIP powinny być właściwymi organami w państwach członkowskich, którym powierzono przyjmowanie, a następnie dalsze przetwarzanie i ochronę danych API gromadzonych i przekazywanych na podstawie niniejszego rozporządzenia. W celu zapewnienia efektywności i zminimalizowania wszelkiego ryzyka dla bezpieczeństwa router, zaprojektowany, opracowany, obsługiwany i utrzymywany technicznie przez Agencję Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) zgodnie z rozporządzeniem (UE) [w sprawie danych API w obszarze zarządzania granicami], powinien przekazywać dane API zgromadzone i przekazane mu przez przewoźników lotniczych na podstawie niniejszego rozporządzenia do odpowiednich JIP. Biorąc pod uwagę niezbędny poziom ochrony danych API stanowiących dane osobowe, również w celu zapewnienia poufności odnośnych informacji, dane API powinny być przekazywane przez router do odpowiednich JIP w sposób zautomatyzowany.

(13) W przypadku lotów pozaunijnych JIP państwa członkowskiego, na którego terytorium lot ma wylądować lub z którego terytorium następuje odlot, powinna otrzymywać dane API od routera w odniesieniu do wszystkich tych lotów, biorąc pod uwagę, że dane PNR są gromadzone w odniesieniu do wszystkich tych lotów zgodnie z dyrektywą (UE) 2016/681. Router powinien identyfikować lot i odpowiadającą mu JIP, korzystając z informacji zawartych w kodzie identyfikacyjnym danych PNR –

[29] Dz.U. C z, s. .

elemencie danych wspólnym dla zbiorów danych API i PNR umożliwiającym wspólne przetwarzanie danych API i PNR przez JIP.

(14) W odniesieniu do lotów wewnątrzunijnych, zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (TSUE), aby uniknąć nieuzasadnionej ingerencji w odpowiednie prawa podstawowe chronione na podstawie Karty oraz zapewnić zgodność z wymogami prawa Unii dotyczącymi swobodnego przepływu osób i zniesienia kontroli na granicach wewnętrznych, należy przewidzieć podejście selektywne. Ze względu na znaczenie zapewnienia, by dane API mogły być przetwarzane wraz z danymi PNR, podejście to należy dostosować do podejścia określonego w dyrektywie (UE) 2016/681. Z tych powodów dane API w odniesieniu do tych lotów powinny być przekazywane z routera do odpowiednich JIP wyłącznie w przypadku, gdy państwa członkowskie dokonały wyboru lotów zgodnie z art. 2 dyrektywy (UE) 2016/681. Jak przypomniał TSUE, wybór odnośnych lotów wiąże się z ukierunkowaniem przez państwa członkowskie przedmiotowych obowiązków wyłącznie na m.in. określone trasy, wzorce podróżowania lub porty lotnicze, z zastrzeżeniem dokonywania regularnego przeglądu tego wyboru.

(15) Aby umożliwić stosowanie tego selektywnego podejścia na podstawie niniejszego rozporządzenia w odniesieniu do lotów wewnątrzunijnych, państwa członkowskie powinny być zobowiązane do sporządzenia i przedłożenia eu-LISA wykazów wybranych przez nie lotów, tak aby eu-LISA mogła zapewnić, aby tylko w odniesieniu do tych lotów dane API były przekazywane z routera do odpowiednich JIP oraz aby dane API w odniesieniu do innych lotów wewnątrzunijnych były natychmiast trwale usuwane.

(16) Aby – poprzez stworzenie ryzyka obchodzenia przepisów – nie zaszkodzić skuteczności systemu, który opiera się na gromadzeniu i przekazywaniu danych API, ustanowionego niniejszym rozporządzeniem, oraz danych PNR w ramach systemu ustanowionego dyrektywą (UE) 2016/681, do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, informacje na temat tego, które loty wewnątrzunijne zostały wybrane przez państwa członkowskie, powinny być traktowane w sposób poufny. Z tego powodu takie informacje nie powinny być udostępniane przewoźnikom lotniczym, a przewoźnicy lotniczy powinni być zobowiązani do gromadzenia danych API w odniesieniu do wszystkich lotów objętych niniejszym rozporządzeniem, w tym wszystkich lotów wewnątrzunijnych, a następnie do przekazywania tych danych do routera, gdzie należy dokonać koniecznego wyboru. Ponadto dzięki gromadzeniu danych API w odniesieniu do wszystkich lotów wewnątrzunijnych pasażerowie nie są informowani o tym, które loty wewnątrzunijne wybrano do przekazania danych API – a tym samym również danych PNR – do JIP zgodnie z oceną państw członkowskich. Podejście to gwarantuje również szybkie i skuteczne wdrożenie wszelkich zmian dotyczących tego wyboru, bez nakładania nadmiernych obciążeń ekonomicznych i operacyjnych na przewoźników lotniczych.

(17) W celu zapewnienia zgodności z podstawowym prawem do ochrony danych osobowych oraz zgodnie z rozporządzeniem (UE) [w sprawie danych API w obszarze zarządzania granicami] w niniejszym rozporządzeniu należy wskazać administratorów. W celu skutecznego monitorowania, zapewnienia odpowiedniej ochrony danych osobowych i zminimalizowania ryzyka dla bezpieczeństwa należy również ustanowić przepisy dotyczące rejestrów, bezpieczeństwa przetwarzania

danych i monitorowania własnej działalności. Jeżeli przepisy te odnoszą się do przetwarzania danych osobowych, należy je rozumieć jako uzupełniające mające ogólne zastosowanie akty prawa Unii dotyczące ochrony danych osobowych, w szczególności rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679[30], dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680[31] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725[32]. Niniejsze rozporządzenie nie powinno mieć wpływu na te akty, które mają również zastosowanie do przetwarzania danych osobowych na podstawie niniejszego rozporządzenia zgodnie z jego przepisami.

(18) Router, który ma zostać utworzony i być obsługiwany na podstawie rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami], powinien zminimalizować i uprościć połączenia techniczne niezbędne do przekazywania danych API, ograniczając je do jednego połączenia na jednego przewoźnika lotniczego i na jedną jednostkę do spraw informacji o pasażerach. W związku z tym niniejsze rozporządzenie nakłada na JIP i przewoźników lotniczych obowiązek ustanowienia takiego połączenia z routerem i osiągnięcia wymaganej integracji z routerem, tak aby zapewnić prawidłowe funkcjonowanie systemu przekazywania danych API ustanowionego niniejszym rozporządzeniem.

(19) Ze względu na interes Unii odpowiednie koszty ponoszone przez państwa członkowskie w związku z ich połączeniami z routerem i integracją z routerem, zgodnie z wymogami niniejszego rozporządzenia, powinny być pokrywane z budżetu Unii, zgodnie z mającymi zastosowanie przepisami, i powinny być objęte pewnymi wyjątkami. Koszty objęte tymi wyjątkami powinny być ponoszone przez każde odnośne państwo członkowskie.

(20) Zgodnie z rozporządzeniem (UE) 2018/1726 państwa członkowskie mogą powierzyć eu-LISA zadanie ułatwienia łączności z przewoźnikami lotniczymi, aby pomóc państwom członkowskim we wdrażaniu dyrektywy (UE) 2016/681, w szczególności poprzez gromadzenie i przekazywanie danych PNR za pośrednictwem routera.

(21) Nie można wykluczyć, że ze względu na wyjątkowe okoliczności i pomimo zastosowania wszelkich racjonalnych środków zgodnie z niniejszym rozporządzeniem oraz – w odniesieniu do routera – rozporządzeniem (UE) [w sprawie danych API w obszarze zarządzania granicami], router lub systemy lub infrastruktura łącząca JIP z przewoźnikami lotniczymi nie zadziałają prawidłowo, co doprowadzi do braku technicznej możności wykorzystania routera do przekazywania danych API. Biorąc

---

30 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. L 119 z 4.5.2016, s. 1).

31 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

32 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

pod uwagę niedostępność routera oraz fakt, że przewoźnicy lotniczy zasadniczo nie będą mogli przekazywać danych API, których dotyczy awaria, w sposób zgodny z prawem, bezpieczny, skuteczny i szybki za pomocą środków alternatywnych, obowiązek przekazania przez przewoźników lotniczych tych danych API do routera powinien przestać obowiązywać tak długo, jak długo utrzymuje się brak technicznej możliwości. W celu zminimalizowania czasu trwania i negatywnych skutków tej sytuacji zainteresowane strony powinny w takim przypadku niezwłocznie poinformować się nawzajem i niezwłocznie podjąć wszelkie niezbędne działania w celu rozwiązania problemu braku technicznej możliwości. Porozumienie to powinno pozostawać bez uszczerbku dla wynikających z niniejszego rozporządzenia obowiązków wszystkich zainteresowanych stron w zakresie zapewnienia prawidłowego funkcjonowania routera oraz odpowiednich systemów i infrastruktury, jak również bez uszczerbku dla faktu, że przewoźnicy lotniczy podlegają karom, jeżeli nie wywiązują się z tych obowiązków, w tym w przypadku gdy polegają oni na tym porozumieniu, jeżeli nie jest to uzasadnione. Aby zniechęcić do takich nadużyć oraz ułatwić nadzór i – w stosownych przypadkach – nakładanie kar, przewoźnicy lotniczy, którzy polegają na tym porozumieniu w związku z awarią własnego systemu i infrastruktury, powinni zgłosić to właściwemu organowi nadzorczemu.

(22) W celu zapewnienia skutecznego stosowania przepisów niniejszego rozporządzenia przez przewoźników lotniczych należy ustanowić przepis dotyczący wyznaczenia i upoważnienia organów krajowych odpowiedzialnych za nadzór nad tymi przepisami. Przepisy niniejszego rozporządzenia dotyczące takiego nadzoru, w tym w stosownych przypadkach w odniesieniu do nakładania kar, nie powinny wpływać na zadania i uprawnienia organów nadzorczych ustanowionych zgodnie z rozporządzeniem (UE) 2016/679 i dyrektywą (UE) 2016/680, w tym w odniesieniu do przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

(23) Wobec przewoźników lotniczych, którzy nie wypełniają obowiązków w zakresie gromadzenia i przekazywania danych API na podstawie niniejszego rozporządzenia, państwa członkowskie powinny przewidzieć skuteczne, proporcjonalne i odstraszające kary, w tym kary finansowe.

(24) W celu przyjęcia środków dotyczących wymogów technicznych i zasad operacyjnych dotyczących zautomatyzowanych środków gromadzenia danych API nadających się do odczytu maszynowego, wspólnych protokołów i formatów stosowanych do przekazywania danych API przez przewoźników lotniczych, przepisów technicznych i proceduralnych dotyczących przekazywania danych API z routera do JIP oraz połączeń JIP i przewoźników lotniczych z routerem i integracji z routerem, należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do – odpowiednio – art. 4, 5, 10 i 11. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[33]. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich,

[33] Dz.U. L 123 z 12.5.2016, s. 1.

a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(25) Wszystkim zainteresowanym stronom, a w szczególności przewoźnikom lotniczym i JIP, należy zapewnić wystarczająco dużo czasu na poczynienie niezbędnych przygotowań, aby mogli wypełniać swoje odpowiednie obowiązki wynikające z niniejszego rozporządzenia, biorąc pod uwagę, że niektóre z tych przygotowań, takie jak przygotowania dotyczące obowiązków w zakresie połączenia z routerem i integracji z routerem, mogą zostać zakończone dopiero po sfinalizowaniu faz projektowania i rozwoju routera i rozpoczęciu eksploatacji routera. Niniejsze rozporządzenie powinno zatem stosować się dopiero od odpowiedniego dnia po dacie rozpoczęcia eksploatacji routera, określonej przez Komisję zgodnie z rozporządzeniem (UE) [w sprawie danych API w obszarze zarządzania granicami]. Komisja powinna jednak mieć możliwość przyjmowania aktów delegowanych na podstawie niniejszego rozporządzenia już wcześniej, aby zapewnić jak najszybsze uruchomienie systemu ustanowionego niniejszym rozporządzeniem.

(26) Cele niniejszego rozporządzenia, a mianowicie przyczynianie się do zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, ze względu na ponadnarodowy wymiar tych przestępstw oraz potrzebę współpracy transgranicznej w celu skutecznego ich zwalczania, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie indywidualnie, natomiast możliwe jest ich lepsze osiągnięcie na poziomie Unii. Unia może zatem podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza zakres niezbędny do osiągnięcia tego celu.

(27) 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 niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje.

(28) [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 do Traktatu o funkcjonowaniu Unii Europejskiej, Irlandia powiadomiła o chęci uczestniczenia w przyjęciu i stosowaniu niniejszego rozporządzenia.] ALBO [Zgodnie z art. 1 i 2 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 do Traktatu o funkcjonowaniu Unii Europejskiej, bez uszczerbku dla art. 4 tego protokołu, Irlandia nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje.]

(29) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia [XX] r.[34],

[34] [Dz.U. C …].

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ 1

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

Do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania w niniejszym rozporządzeniu ustanawia się przepisy dotyczące:

a) gromadzenia przez przewoźników lotniczych danych pasażera przekazywanych przed podróżą („dane API") w odniesieniu do lotów pozaunijnych i wybranych lotów wewnątrzunijnych;

b) przekazywania przez przewoźników lotniczych danych API do routera;

c) przekazywania danych API z routera do jednostek do spraw informacji o pasażerach w odniesieniu do lotów pozaunijnych i wybranych lotów wewnątrzunijnych.

Artykuł 2

Zakres

Niniejsze rozporządzenie ma zastosowanie do przewoźników lotniczych wykonujących regularne lub nieregularne loty pozaunijne lub wewnątrzunijne.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

a) „przewoźnik lotniczy" oznacza przedsiębiorstwo transportu lotniczego określone w art. 3 pkt 1 dyrektywy (UE) 2016/681;

b) „lot pozaunijny" oznacza każdy lot określony w art. 3 pkt 2 dyrektywy (UE) 2016/681;

c) „lot wewnątrzunijny" oznacza każdy lot określony w art. 3 pkt 3 dyrektywy (UE) 2016/681;

d) „lot regularny" oznacza lot określony w art. 3 lit. e) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami];

e) „lot nieregularny” oznacza lot określony w art. 3 lit. f) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami];

f) „pasażer” oznacza każdą osobę określoną w art. 3 pkt 4 dyrektywy (UE) 2016/681;

g) „załoga” oznacza każdą osobę określoną w art. 3 lit. h) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami];

h) „osoba podróżująca” oznacza każdą osobę określoną w art. 3 lit. i) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami];

i) „dane pasażera przekazywane przed podróżą” lub „dane API” oznaczają dane określone w art. 3 lit. j) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami];

j) „dane dotyczące przelotu pasażera” lub „dane PNR” oznaczają zbiór danych o podróży każdego pasażera określony w art. 3 pkt 5 dyrektywy (UE) 2016/681;

k) „jednostka do spraw informacji o pasażerach” lub „JIP” oznacza właściwy organ ustanowiony przez państwo członkowskie, zawarty w powiadomieniach i zmianach opublikowanych przez Komisję zgodnie z – odpowiednio – art. 4 ust. 1 i 5 dyrektywy (UE) 2016/681;

l) „przestępstwo terrorystyczne” oznacza przestępstwo określone w art. 3–12 dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541[35];

m) „poważna przestępczość” oznacza przestępstwa określone w art. 3 pkt 9 dyrektywy (UE) 2016/681;

n) „router” oznacza router określony w art. 3 lit. k) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami];

o) „dane osobowe” oznaczają wszelkie informacje określone w art. 4 pkt 1 rozporządzenia (UE) 2016/679.

ROZDZIAŁ 2

PRZETWARZANIE DANYCH API

[35] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

Artykuł 4

Gromadzenie, przekazywanie i usuwanie danych API przez przewoźników lotniczych

1. Przewoźnicy lotniczy gromadzą dane API dotyczące osób podróżujących lotami, o których mowa w art. 2, w celu przekazania tych danych API do routera zgodnie z ust. 6. W przypadku gdy lot odbywa się pod wspólnym kodem jednego lub większej liczby przewoźników lotniczych, obowiązek przekazania danych API spoczywa na przewoźniku lotniczym obsługującym lot.

2. Przewoźnicy lotniczy gromadzą dane API w taki sposób, aby dane API, które przekazują zgodnie z ust. 6, były dokładne, kompletne i aktualne.

3. Przewoźnicy lotniczy gromadzą dane API, o których mowa w art. 4 ust. 2 lit. a)–d) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami], przy użyciu zautomatyzowanych środków do gromadzenia danych dokumentu podróży danej osoby podróżującej nadających się do odczytu maszynowego. Dokonują tego zgodnie ze szczegółowymi wymogami technicznymi i przepisami operacyjnymi, o których mowa w ust. 5, w przypadku gdy takie przepisy zostały przyjęte i mają zastosowanie.

   Jeżeli jednak takie wykorzystanie zautomatyzowanych środków nie jest możliwe ze względu na to, że dokument podróży nie zawiera danych nadających się do odczytu maszynowego, przewoźnicy lotniczy gromadzą te dane ręcznie, w sposób zapewniający zgodność z ust. 2.

4. Wszelkie zautomatyzowane środki stosowane przez przewoźników lotniczych do gromadzenia danych API na podstawie niniejszego rozporządzenia muszą być wiarygodne, bezpieczne i aktualne.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 19 w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie szczegółowych wymogów technicznych i przepisów operacyjnych dotyczących gromadzenia danych API, o których mowa w art. 4 ust. 2 lit. a)–d) rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami], przy użyciu zautomatyzowanych środków zgodnie z ust. 3 i 4 niniejszego artykułu.

6. Przewoźnicy lotniczy przekazują dane API zgromadzone zgodnie z ust. 1 do routera drogą elektroniczną. Dokonują tego zgodnie ze szczegółowymi przepisami, o których mowa w ust. 9, w przypadku gdy takie przepisy zostały przyjęte i mają zastosowanie.

7. Przewoźnicy lotniczy przekazują dane API zarówno w momencie odprawy, jak i bezpośrednio po zamknięciu lotu, tj. po wejściu osób podróżujących na pokład statku powietrznego przygotowującego się do odlotu, gdy osoby podróżujące nie mają już możliwości wejścia na pokład ani opuszczenia statku powietrznego.

8. Bez uszczerbku dla możliwości zatrzymywania i wykorzystywania przez przewoźników lotniczych danych API, jeżeli jest to konieczne do prowadzenia normalnej działalności zgodnie z mającymi zastosowanie przepisami, przewoźnicy lotniczy niezwłocznie poprawiają, uzupełniają lub aktualizują dane API lub trwale je usuwają w obu następujących sytuacjach:

a) gdy dowiedzą się, że zgromadzone dane API są niedokładne, niekompletne lub nieaktualne, lub że były przetwarzane niezgodnie z prawem, lub że przekazane dane nie stanowią danych API;

b) jeżeli przekazanie danych API zgodnie z ust. 3 zostało zakończone.

W przypadku gdy przewoźnicy lotniczy uzyskają wiedzę, o której mowa w akapicie pierwszym lit. a) niniejszego ustępu, po zakończeniu przekazywania danych zgodnie z ust. 6, niezwłocznie informują o tym Agencję Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA). Po otrzymaniu takich informacji eu-LISA niezwłocznie informuje JIP, które otrzymały dane API przekazane za pośrednictwem routera.

9. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 19 w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie niezbędnych szczegółowych przepisów dotyczących wspólnych protokołów i obsługiwanych formatów danych używanych do przekazywania danych do routera, o czym mowa w ust. 6.

Artykuł 5

Przekazywanie danych API z routera do JIP

1. Router niezwłocznie i w sposób zautomatyzowany przekazuje dane API przesłane mu przez przewoźników lotniczych na podstawie art. 4 do JIP państwa członkowskiego, na którego terytorium lot ma wylądować lub z którego terytorium następuje odlot, lub do obu tych jednostek w przypadku lotów wewnątrzunijnych. W przypadku gdy lot odbywa się z co najmniej jedną przerwą w podróży na terytorium innych państw członkowskich niż to, z którego nastąpił odlot, router przekazuje dane API do JIP wszystkich zainteresowanych państw członkowskich.

Do celów takiego przekazywania danych eu-LISA sporządza i aktualizuje tabelę korelacji między różnymi portami lotniczymi odlotu i lądowania a państwami, do których te porty lotnicze należą.

W przypadku lotów wewnątrzunijnych router przekazuje jednak dane API do odpowiedniej JIP wyłącznie w odniesieniu do lotów ujętych w wykazie, o którym mowa w ust. 2.

Router przekazuje dane API zgodnie ze szczegółowymi przepisami, o których mowa w ust. 3, w przypadku gdy takie przepisy zostały przyjęte i mają zastosowanie. 2. Państwa członkowskie, które podejmują decyzję o stosowaniu dyrektywy (UE) 2016/681 do lotów wewnątrzunijnych zgodnie z art. 2 tej dyrektywy, ustanawiają wykaz odnośnych lotów wewnątrzunijnych i do dnia rozpoczęcia stosowania niniejszego rozporządzenia, o którym mowa w art. 21 akapit drugi, przekazują ten wykaz eu-LISA. Te państwa członkowskie, zgodnie z art. 2 tej dyrektywy, regularnie dokonują przeglądu i w razie potrzeby aktualizacji tych wykazów oraz niezwłocznie przekazują eu-LISA wszelkie zaktualizowane wykazy. Informacje zawarte w tych wykazach są traktowane jako poufne.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 19 w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie niezbędnych szczegółowych przepisów technicznych i proceduralnych dotyczących przekazywania danych API z routera, o którym to przekazywaniu danych mowa w ust. 1.

ROZDZIAŁ 3

REJESTRY, OCHRONA I BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Artykuł 6

Przechowywanie rejestrów

1. Przewoźnicy lotniczy tworzą rejestry wszystkich operacji przetwarzania prowadzonych na podstawie niniejszego rozporządzenia przy użyciu zautomatyzowanych środków, o których mowa w art. 4 ust. 3. Rejestry te obejmują datę, godzinę i miejsce przekazania danych API.

2. Rejestry, o których mowa w ust. 1, wykorzystuje się wyłącznie w celu zapewnienia bezpieczeństwa i integralności danych API oraz zgodności przetwarzania z prawem, w szczególności w odniesieniu do zgodności z wymogami określonymi w niniejszym rozporządzeniu, w tym postępowań w sprawie kar za naruszenie tych wymogów zgodnie z art. 15 i 16 niniejszego rozporządzenia.

3. Przewoźnicy lotniczy wprowadzają odpowiednie środki w celu ochrony rejestrów, które stworzyli na podstawie ust. 1, przed nieuprawnionym dostępem i innymi rodzajami ryzyka dla bezpieczeństwa.

4. Przewoźnicy lotniczy przechowują rejestry, które stworzyli na podstawie ust. 1, przez okres jednego roku od momentu utworzenia tych rejestrów. Po upływie tego okresu niezwłocznie i trwale usuwają te rejestry.

   Jeżeli jednak rejestry te są potrzebne do celów procedur monitorowania lub zapewniania bezpieczeństwa i integralności danych API lub legalności operacji przetwarzania, o których to celach mowa w ust. 2, a procedury te już rozpoczęły się w momencie upływu okresu, o którym mowa w akapicie pierwszym, przewoźnicy lotniczy mogą przechowywać te rejestry tak długo, jak jest to konieczne do przeprowadzenia tych procedur. W takim przypadku niezwłocznie usuwają te rejestry, jeżeli nie są już one konieczne do przeprowadzenia tych procedur.

Artykuł 7

Administratorzy danych osobowych

JIP są administratorami w rozumieniu art. 3 pkt 8 dyrektywy (UE) 2016/680 w odniesieniu do przetwarzania danych API stanowiących dane osobowe na podstawie niniejszego

rozporządzenia za pośrednictwem routera, w tym przekazywania i przechowywania tych danych na routerze ze względów technicznych.

Przewoźnicy lotniczy są administratorami w rozumieniu art. 4 pkt 7 rozporządzenia (UE) 2016/679 w odniesieniu do przetwarzania danych API stanowiących dane osobowe w związku z gromadzeniem tych danych i ich przekazywaniem do routera na podstawie niniejszego rozporządzenia.

Artykuł 8

Bezpieczeństwo

JIP i przewoźnicy lotniczy zapewniają bezpieczeństwo danych API, w szczególności danych API stanowiących dane osobowe, które to dane przetwarzają zgodnie z niniejszym rozporządzeniem.

JIP i przewoźnicy lotniczy współpracują ze sobą oraz z eu-LISA, zgodnie ze swoimi odpowiednimi obowiązkami i zgodnie z prawem Unii, w celu zapewnienia takiego bezpieczeństwa.

Artykuł 9

Monitorowanie własnej działalności

Przewoźnicy lotniczy i JIP monitorują wypełnianie swoich odpowiednich obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do przetwarzania przez nich danych API stanowiących dane osobowe, w tym poprzez częstą weryfikację rejestrów zgodnie z art. 7.

ROZDZIAŁ 4

KWESTIE DOTYCZĄCE ROUTERA

Artykuł 10

Połączenia JIP z routerem

1. Państwa członkowskie zapewniają swoim JIP połączenie z routerem. Zapewniają one, aby ich krajowe systemy i infrastruktura do odbioru i dalszego przetwarzania danych API przekazywanych na podstawie niniejszego rozporządzenia były zintegrowane z routerem.

   Państwa członkowskie zapewniają, by połączenie z routerem i integracja z routerem umożliwiały ich JIP otrzymywanie i dalsze przetwarzanie danych API, a także wymianę wszelkich związanych z nimi komunikatów w sposób zgodny z prawem, bezpieczny, skuteczny i szybki.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 19 w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie niezbędnych szczegółowych przepisów dotyczących połączeń i integracji z routerem, o których mowa w ust. 1.

Artykuł 11

Połączenia przewoźników lotniczych z routerem

1. Przewoźnicy lotniczy zapewniają swoje połączenie z routerem. Zapewniają oni, aby ich systemy i infrastruktura do przekazywania danych API do routera na podstawie niniejszego rozporządzenia były zintegrowane z routerem.

   Przewoźnicy lotniczy zapewniają, by połączenie z routerem i integracja z routerem umożliwiały im przekazywanie danych API, a także wymianę wszelkich związanych z nimi komunikatów w sposób zgodny z prawem, bezpieczny, skuteczny i szybki.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 19 w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie niezbędnych szczegółowych przepisów dotyczących połączeń i integracji z routerem, o których mowa w ust. 1.

Artykuł 12

Koszty ponoszone przez państwa członkowskie

1. Koszty ponoszone przez państwa członkowskie w związku z ich połączeniami z routerem i integracją z routerem, o których mowa w art. 10, pokrywane są z budżetu ogólnego Unii.

   Następujące koszty są jednak wyłączone i ponoszone przez państwa członkowskie:

   a) koszty zarządzania projektem, w tym koszty spotkań, podróży służbowych i biur;

   b) koszty hostingu krajowych systemów informatycznych (IT), w tym koszty przestrzeni, wdrażania, energii elektrycznej i chłodzenia;

   c) koszty eksploatacji krajowych systemów informatycznych, w tym umów z operatorami i umów w zakresie wsparcia;

   d) koszty projektowania, rozwoju, wdrażania, funkcjonowania i utrzymania krajowych sieci łączności.

2. Państwa członkowskie ponoszą również koszty powstałe w wyniku administrowania, użytkowania i konserwacji krajowych połączeń z routerem i integracji z routerem.

Artykuł 13

Działania w przypadku braku technicznej możliwości korzystania z routera

1. Jeżeli korzystanie z routera do przekazywania danych API jest technicznie niemożliwe z powodu awarii routera, eu-LISA niezwłocznie w sposób zautomatyzowany powiadamia przewoźników lotniczych i JIP o braku tej technicznej możliwości. W takim przypadku eu-LISA niezwłocznie wprowadza środki w celu rozwiązania problemu braku technicznej możliwości korzystania z routera i niezwłocznie powiadamia te strony, gdy skutecznie zajęto się tą kwestią.

   W okresie między tymi powiadomieniami art. 4 ust. 6 nie ma zastosowania, o ile brak technicznej możliwości nie pozwala na przekazanie danych API do routera. W takim zakresie, w jakim ma to miejsce, również art. 4 ust. 1 nie ma zastosowania do przedmiotowych danych API w tym okresie.

2. Jeżeli korzystanie z routera do przekazywania danych API jest technicznie niemożliwe z powodu awarii systemów lub infrastruktury państwa członkowskiego, o których mowa w art. 10, JIP tego państwa członkowskiego niezwłocznie w sposób zautomatyzowany powiadamia przewoźników lotniczych, pozostałe JIP, eu-LISA i Komisję o tym braku technicznej możliwości. W takim przypadku dane państwo członkowskie niezwłocznie wprowadza środki w celu rozwiązania problemu braku technicznej możliwości korzystania z routera i niezwłocznie powiadamia te strony, gdy skutecznie zajęto się tą kwestią.

   W okresie między tymi powiadomieniami art. 4 ust. 6 nie ma zastosowania, o ile brak technicznej możliwości nie pozwala na przekazanie danych API do routera. W takim zakresie, w jakim ma to miejsce, również art. 4 ust. 1 nie ma zastosowania do przedmiotowych danych API w tym okresie.

3. Jeżeli korzystanie z routera do przekazywania danych API jest technicznie niemożliwe z powodu awarii systemów lub infrastruktury przewoźnika lotniczego, o których mowa w art. 11, przewoźnik ten niezwłocznie w sposób zautomatyzowany powiadamia jednostki JIP, eu-LISA i Komisję o tym braku technicznej możliwości. W takim przypadku przewoźnik lotniczy niezwłocznie wprowadza środki w celu rozwiązania problemu braku technicznej możliwości korzystania z routera i niezwłocznie powiadamia te strony, gdy skutecznie zajęto się tą kwestią.

   W okresie między tymi powiadomieniami art. 4 ust. 6 nie ma zastosowania, o ile brak technicznej możliwości nie pozwala na przekazanie danych API do routera. W takim zakresie, w jakim ma to miejsce, również art. 4 ust. 1 nie ma zastosowania do przedmiotowych danych API w tym okresie.

   Po skutecznym rozwiązaniu problemu braku technicznej możliwości dany przewoźnik lotniczy niezwłocznie przedkłada właściwemu krajowemu organowi nadzorczemu, o którym mowa w art. 15, sprawozdanie zawierające wszystkie niezbędne szczegóły dotyczące braku technicznej możliwości, w tym przyczyny braku technicznej możliwości, jego zakres i konsekwencje, a także środki podjęte w celu zaradzenia temu brakowi technicznej możliwości.

Artykuł 14

Odpowiedzialność za router

Jeżeli niewywiązanie się przez państwo członkowskie lub przewoźnika lotniczego z obowiązków wynikających z niniejszego rozporządzenia spowoduje szkodę w routerze, dane państwo członkowskie lub dany przewoźnik lotniczy odpowiada za taką szkodę, chyba że – i w zakresie w jakim – eu-LISA nie zastosowała rozsądnych środków, by zapobiec wystąpieniu szkody lub zminimalizować jej skutki.

ROZDZIAŁ 5

NADZÓR, KARY I PODRĘCZNIK

Artykuł 15

Krajowy organ nadzorczy

1. Państwa członkowskie wyznaczają co najmniej jeden krajowy organ nadzorczy odpowiedzialny za monitorowanie stosowania przepisów niniejszego rozporządzenia na terytorium krajowym przez przewoźników lotniczych i zapewnienie przestrzegania tych przepisów.

2. Państwa członkowskie zapewniają, by krajowe organy nadzorcze posiadały wszelkie niezbędne środki i wszelkie niezbędne uprawnienia dochodzeniowe i wykonawcze do wykonywania swoich zadań na podstawie niniejszego rozporządzenia, w tym – w stosownych przypadkach – poprzez nakładanie kar, o których mowa w art. 16. Ustanawiają one szczegółowe przepisy dotyczące wykonywania tych zadań i wykonywania tych uprawnień, zapewniając, aby wykonywanie zadań i wykonywanie uprawnień były skuteczne, proporcjonalne i odstraszające oraz by podlegały zabezpieczeniom zgodnie z prawami podstawowymi zagwarantowanymi na mocy prawa Unii.

3. Do daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 21 akapit drugi, państwa członkowskie powiadamiają Komisję o nazwie i danych kontaktowych organów wyznaczonych na podstawie ust. 1 oraz o szczegółowych przepisach ustanowionych na podstawie ust. 2. Niezwłocznie powiadamiają Komisję o wszelkich późniejszych zmianach lub poprawkach w tym zakresie.

4. Niniejszy artykuł pozostaje bez uszczerbku dla uprawnień organów nadzorczych, o których mowa w art. 51 rozporządzenia (UE) 2016/679 i art. 41 dyrektywy (UE) 2016/680.

Artykuł 16

Kary

Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń przepisów niniejszego rozporządzenia i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.

Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 21 akapit drugi, i niezwłocznie przekazują informacje o wszelkich późniejszych zmianach, które ich dotyczą.

Artykuł 17

Praktyczny podręcznik

Komisja, w ścisłej współpracy z JIP, innymi właściwymi organami państw członkowskich, przewoźnikami lotniczymi i odpowiednimi agencjami unijnymi, przygotowuje i publicznie udostępnia praktyczny podręcznik zawierający wytyczne, zalecenia i najlepsze praktyki dotyczące wdrażania niniejszego rozporządzenia.

Praktyczny podręcznik uwzględnia odpowiednie istniejące już podręczniki.

Komisja przyjmuje praktyczny podręcznik w formie zalecenia.

ROZDZIAŁ 6

ZWIĄZEK Z INNYMI OBOWIĄZUJĄCYMI INSTRUMENTAMI

Artykuł 18

Zmiany w rozporządzeniu (UE) 2019/818

_____

Art. 39 ust. 1 i 2 otrzymują brzmienie:

„1. Centralne repozytorium sprawozdawczo-statystyczne ustanawia się, aby wspierać realizację celów SIS, Eurodac i ECRIS-TCN zgodnie z odpowiednimi aktami prawnymi regulującymi te systemy oraz zapewniać międzysystemowe dane statystyczne i sprawozdania analityczne służące strategiom politycznym, celom operacyjnym i związanym z jakością danych. Centralne repozytorium sprawozdawczo-statystyczne wspiera ponadto realizację celów rozporządzenia Parlamentu Europejskiego i Rady (UE) .../...* [*niniejsze rozporządzenie*].

* Rozporządzenie Parlamentu Europejskiego i Rady (UE) [numer] z dnia xy r. w sprawie [oficjalnie przyjęty tytuł] (Dz.U. L … z …, s. …).

2. eu-LISA ustanawia, wdraża i obsługuje centralne repozytorium sprawozdawczo-statystyczne w swoich centrach technicznych zawierające dane i statystyki, o których mowa art. 74 rozporządzenia (UE) 2018/1862 oraz art. 32 rozporządzenia (UE) 2019/816, logicznie oddzielone według systemu informacyjnego UE. eu-LISA gromadzi ponadto dane i statystyki z routera, o których mowa w art. 13 ust. 1 rozporządzenia (UE) .../...* [*niniejsze rozporządzenie*]. Dostęp do centralnego

repozytorium sprawozdawczo-statystycznego w postaci kontrolowanego, bezpiecznego dostępu i określonych profili użytkowników przyznaje się – wyłącznie w celach sprawozdawczo-statystycznych – organom, o których mowa w art. 74 rozporządzenia (UE) 2018/1862, art. 32 rozporządzenia (UE) 2019/816 oraz art. 13 ust. 1 rozporządzenia (UE) .../...* [*niniejsze rozporządzenie*].”.

ROZDZIAŁ 7

PRZEPISY KOŃCOWE

Artykuł 19

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 4 ust. 5 i 9, art. 5 ust. 3, art. 10 ust. 2 i art. 11 ust. 2, powierza się Komisji na okres pięciu lat od [*dnia przyjęcia niniejszego rozporządzenia*]. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

3. Przekazanie uprawnień, o którym mowa w art. 4 ust. 5 i 9, art. 5 ust. 3, art. 10 ust. 2 i art. 11 ust. 2, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

Artykuł 20

Monitorowanie i ocena

1. Do dnia [*cztery lata od daty wejścia w życie niniejszego rozporządzenia*], a następnie co cztery lata Komisja sporządza sprawozdanie zawierające ogólną ocenę niniejszego rozporządzenia, w tym ocenę:

a) stosowania niniejszego rozporządzenia;

b) zakresu, w jakim niniejsze rozporządzenie osiągnęło swoje cele;

c) wpływu niniejszego rozporządzenia na prawa podstawowe chronione prawem Unii;

d) Komisja przekazuje powyższe sprawozdanie oceniające Parlamentowi Europejskiemu, Radzie, Europejskiemu Inspektorowi Danych Osobowych i Agencji Praw Podstawowych Unii Europejskiej. W stosownych przypadkach, w świetle przeprowadzonej oceny, Komisja przedkłada Parlamentowi Europejskiemu i Radzie wniosek ustawodawczy mający na celu zmianę niniejszego rozporządzenia.

2. Państwa członkowskie i przewoźnicy lotniczy dostarczają Komisji na żądanie informacji niezbędnych do sporządzenia sprawozdania, o którym mowa w ust. 1. Państwa członkowskie mogą jednak powstrzymać się od przekazywania takich informacji, jeżeli i w zakresie, w jakim jest to konieczne, aby nie ujawniać poufnych metod pracy lub nie zagrażać toczącym się postępowaniom przygotowawczym prowadzonym przez krajowe JIP lub inne organy ścigania. Komisja zapewnia odpowiednią ochronę wszelkich przekazywanych informacji poufnych.

Artykuł 21

Wejście w życie i rozpoczęcie stosowania

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się po upływie dwóch lat od daty uruchomienia routera, określonej przez Komisję zgodnie z art. 27 rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami].

Art. 4 ust. 5 i 9, art. 5 ust. 3, art. 10 ust. 2, art. 11 ust. 2 oraz art. 19 stosuje się jednak od [*daty wejścia w życie niniejszego rozporządzenia*].

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w Strasburgu dnia r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

Skutki finansowe niniejszego wniosku zostały uwzględnione we wspólnej ocenie skutków finansowych regulacji załączonej do wniosku dotyczącego rozporządzenia (UE) [w sprawie danych API w obszarze zarządzania granicami].