

Sprawozdanie specjalne

Unijne systemy informacyjne wspierające kontrole graniczne – narzędzie efektywne, lecz wymagające bardziej aktualnych i kompletnych danych



EUROPEJSKI
TRYBUNAŁ
OBRACHUNKOWY

Spis treści

	Punkty
Streszczenie	I-XII
Wstęp	01-08
Strefa Schengen	01-08
Systemy informacyjne wykorzystywane do kontroli granic zewnętrznych strefy Schengen	03-08
Zakres kontroli i podejście kontrolne	09-15
Uwagi	16-82
Założenia koncepcyjne systemów informacyjnych umożliwiają efektywne przeprowadzanie odpraw granicznych, ale eliminowanie uchybień zajmuje dużo czasu	16-82
Systemy informacyjne spełniały zasadniczo wymogi UE, ale nie wszędzie funkcjonowały tak samo efektywnie	17-23
Ze względu na opóźnienia we wdrażaniu Eurosur i PNR służby graniczne nie mogły wymieniać się istotnymi informacjami	24-32
W ramach ocen Schengen ewaluacji poddawane są krajowe odprawy graniczne, ale eliminowanie wykrytych uchybień zajmuje dużo czasu	33-43
Państwa członkowskie UE jedynie w ograniczonym stopniu korzystają z finansowania unijnego w celu udoskonalenia systemów informacyjnych wykorzystywanych w trakcie kontroli granicznych	44-46
Funkcjonariusze straży granicznej nie zawsze uzyskują kompletne dane z systemów, co negatywnie wpływa na efektywność odpraw	47
Państwa członkowskie w coraz większym stopniu korzystają z systemów w celu udostępniania informacji, ale weryfikacje mogłyby być bardziej systematyczne	48-62
Informacje w niektórych systemach były niekompletne	63-76
Zdarzenia nie zawsze są szybko rejestrowane w systemach	77-82
Wnioski i zalecenia	83-95
Załącznik	
Krótki opis wybranych systemów informacyjnych	

Wykaz akronimów

Glosariusz

Odpowiedzi Komisji

Zespół kontrolny

Kalendarium

Streszczenie

I W następstwie stworzenia strefy Schengen – do której należą 22 państwa członkowskie UE i cztery inne państwa europejskie – zniesiono kontrole graniczne między należącymi do niej państwami. Zniesienie granic wewnętrznych spowodowało jednak, że większe znaczenie mają obecnie skuteczna kontrola i nadzorowanie granic zewnętrznych strefy Schengen. Ochrona granic zewnętrznych to kwestia będąca przedmiotem dużego zainteresowania zarówno ze strony obywateli UE, jak i innych podmiotów.

II Aby wspomóc funkcjonariuszy straży granicznej w kontrolowaniu zewnętrznych granic strefy Schengen, UE ustanowiła następujące systemy informacyjne / wspólne ramy wymiany informacji: system informacyjny Schengen (SIS II), wizowy system informacyjny (VIS) oraz Eurodac (europejska baza danych zawierająca odciski palców i umożliwiającą ich porównywanie). Dodatkowe wsparcie dla służb granicznych zapewniają ponadto europejski system nadzorowania granic (Eurosur) oraz rejestr danych dotyczących przelotu pasażera (PNR).

III Ustanowienie i utrzymywanie tych systemów wiązało się z koniecznością znacznych inwestycji ze strony zarówno UE, jak i państw strefy Schengen. Na podstawie dostępnych informacji Trybunał szacuje, że z budżetu UE wyasygnowano ponad 600 mln euro na utworzenie tych systemów. Zważywszy na rosnącą presję na granicach zewnętrznych UE spowodowaną sytuacją w zakresie bezpieczeństwa i migracji, kontrola przeprowadzona przez Trybunał miała na celu wskazanie tych aspektów w założeniach koncepcyjnych systemów i w ich użytkowaniu, które mogą pomóc funkcjonariuszom straży granicznej skuteczniej wykonywać ich obowiązki. Ponadto uwagi i zalecenia Trybunału mogą przyczynić się do lepszego ukierunkowania finansowania unijnego, które zostanie udostępnione w następnych wieloletnich ramach finansowych na wsparcie tych systemów.

IV Podstawowe pytanie kontrolne Trybunału dotyczyło tego, **czy główne unijne systemy informacyjne w zakresie bezpieczeństwa wewnętrznego efektywnie wspierają kontrole graniczne**. Trybunał stwierdził, że funkcjonariusze straży granicznej w coraz większym stopniu korzystają z tych systemów i polegają na nich przy przeprowadzaniu odpraw granicznych. W systemach brakuje jednak obecnie pewnych danych, a inne dane są niekompletne bądź nie są wprowadzane w przewidzianych na to terminach, co negatywnie wpływa na efektywność niektórych odpraw granicznych.

V Trybunał ustalił, że systemy są ogólnie dobrze opracowane i ułatwiają dokonywanie odpraw granicznych. Państwa członkowskie, w których przeprowadzono wizyty kontrolne (Finlandia, Francja, Włochy, Luksemburg i Polska), zasadniczo przestrzegały obowiązujących ram prawnych. Mimo to krajowe komponenty systemów SIS II i VIS w niektórych państwach umożliwiają sprawniejsze przeprowadzanie odpraw granicznych niż w innych.

VI Przy wdrażaniu rozwiązań informatycznych na potrzeby Eurosur i PNR wystąpiły duże opóźnienia, zarówno na szczeblu UE, jak i krajowym, co spowodowało, że służby graniczne i inne organy nie mogły czerpać z nich oczekiwanych korzyści.

VII Istotną rolę w zabezpieczaniu granic zewnętrznych UE odgrywa mechanizm oceny Schengen. Oceny są zazwyczaj wnikliwe, metodyczne i odnoszą się do kluczowych aspektów systemów. Wyeliminowanie stwierdzonych w ich toku uchybień zajmuje jednak państwom członkowskim dużo czasu, co wynika z braku wiążących terminów przyjmowania sprawozdań z oceny i realizacji działań naprawczych.

VIII Choć państwa członkowskie w coraz większym stopniu korzystają z systemów informacyjnych, mogłyby to robić w sposób bardziej systematyczny. Trybunał przeprowadził ankietę wśród funkcjonariuszy straży granicznej, z której wynika, że ponad połowie z nich zdarzyło się przepuścić osoby przekraczające granicę bez przeprowadzenia odnośnych kontroli w systemach. Ponadto zauważono rozbieżność pomiędzy liczbą wydanych i skontrolowanych wiz.

IX Dane w systemach służą funkcjonariuszom straży granicznej za podstawę do podejmowania decyzji, które mają wpływ na bezpieczeństwo obywateli europejskich. Jakość tych danych ma zatem niebagatelne znaczenie. Zgodnie z prawodawstwem unijnym odpowiedzialność za jakość danych spoczywa na państwach członkowskich. Kontrolerzy stwierdzili jednak, że w aktach prawnych dotyczących europejskich systemów informacyjnych rzadko wspomina się o kontroli jakości danych. Agencja eu-LISA przeprowadza wprawdzie co miesiąc automatyczne weryfikacje danych w systemie SIS II, ale ich wyniki są udostępniane jedynie odpowiednim państwom członkowskim, w związku z czym ani eu-LISA, ani Komisja nie mają możliwości oceny postępów poszczególnych krajów w rozwiązywaniu problemów dotyczących jakości danych. Ani eu-LISA, ani Komisja nie posiadają też odpowiednich uprawnień, by wyegzekwować od państw członkowskich szybkie wyeliminowanie problemów w tym obszarze.

X Funkcjonariusze straży granicznej nie zawsze otrzymują kompletne i aktualne dane z systemów informacyjnych. Jeśli przykładowo chcą oni zweryfikować nazwisko w systemie SIS II, mogą otrzymać setki rezultatów (w większości fałszywych trafień), które następnie mają oni prawny obowiązek sprawdzić ręcznie. Sprawia to nie tylko, że odprawy graniczne są mniej efektywne, ale zwiększa również ryzyko przeoczenia prawidłowych trafień. Ponadto fakt, że dane w SIS II są niekompletne, ma niekorzystny wpływ na inne powiązane systemy.

XI Z wyjątkiem systemu Eurodac zasadniczo nie ma wiążących terminów wprowadzania danych do systemów. Przykładowo Eurosur ma w założeniu zapewniać informacje w czasie rzeczywistym na temat sytuacji na granicach. O ile jednak niektóre państwa objęte kontrolą Trybunału faktycznie wprowadzają dane do tego systemu w czasie rzeczywistym, o tyle inne dokonują tego jedynie raz w tygodniu. Z kolei odkąd Eurodac zaczął funkcjonować w 2003 r., nie odnotowano ani jednego roku, w którym wszystkie państwa członkowskie przekazałyby wymagane informacje w terminie. Tymczasem opóźnienia w przekazywaniu danych mogą spowodować, że za właściwy do rozpatrzenia wniosku o azyl uznany zostanie nieprawidłowy kraj.

XII Trybunał sformułował następujące zalecenia pod adresem Komisji:

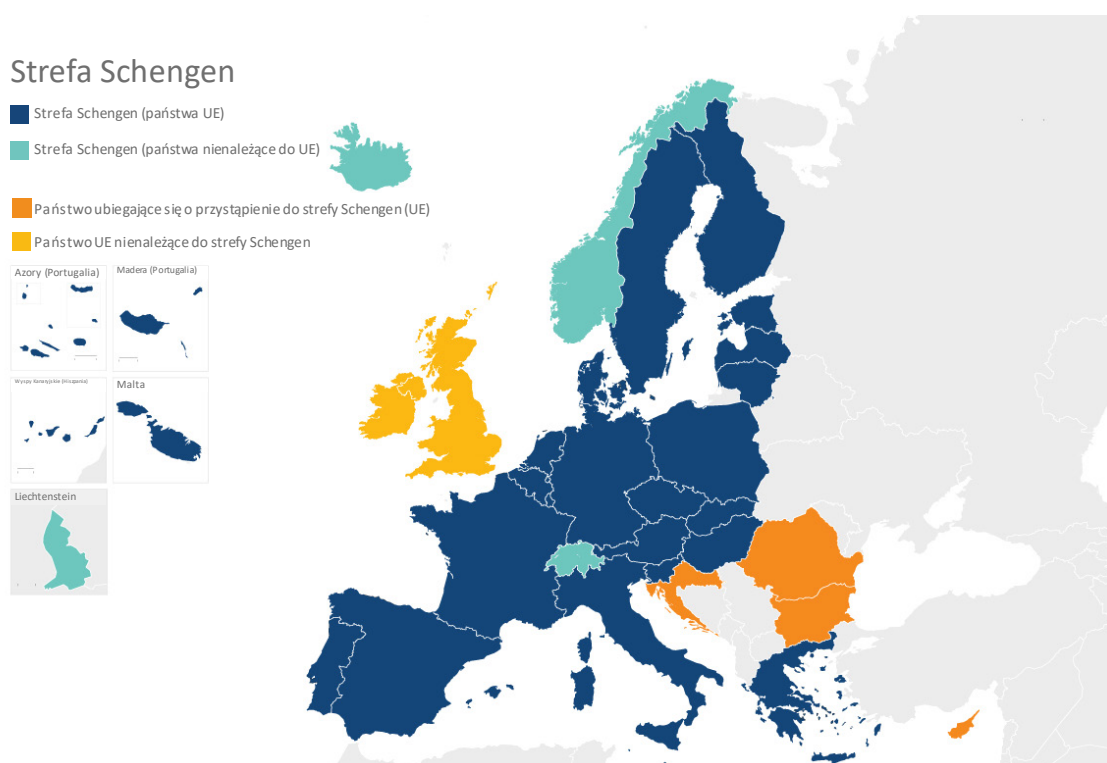
- promowanie korzystania z programów szkoleniowych w zakresie systemów SIS II i VIS,
- szybsze eliminowanie uchybień stwierdzonych w trakcie ocen Schengen,
- przeanalizowanie rozbieżności w przypadku kontroli wizowych,
- udoskonalenie procedur kontroli jakości danych,
- zmniejszenie opóźnień we wprowadzaniu danych.

Wstęp

Strefa Schengen

01 W wyniku stworzenia strefy Schengen, która obejmuje obecnie 26 państw (zob. [rys. 1](#)), wszyscy podróżujący mogą przekraczać granice wewnętrzne bez konieczności przechodzenia odprawy granicznej. Oprócz zniesienia takich odpraw państwa Schengen uzgodniły także wspólną politykę wizową oraz sformalizowały współpracę policyjną i sądową.

Rys. 1 – Obecna mapa strefy Schengen



Źródło: Parlament Europejski.

02 Dwie trzecie obywateli UE postrzega strefę Schengen jako jedno z najważniejszych osiągnięć UE. Niemal 70% jest jednak zdania, że UE powinna dokładać większych starań, by chronić swoje granice zewnętrzne¹.

¹ Badanie Eurobarometr 89.2, 2018.

Systemy informacyjne wykorzystywane do kontroli granic zewnętrznych strefy Schengen

03 Zniesienie granic wewnętrznych wiąże się z koniecznością skutecznego kontrolowania i nadzorowania granic zewnętrznych, tak aby zapobiegać przestępczości i terroryzmowi oraz kontrolować migrację. Aby wspomóc funkcjonariuszy straży granicznej w kontrolowaniu zewnętrznych granic strefy Schengen, UE ustanowiła szereg systemów informacyjnych / wspólnych ram wymiany informacji.

Najpowszechniej wykorzystywane są: system informacyjny Schengen (SIS II), wizowy system informacyjny (VIS), Eurodac (europejska baza danych zawierająca odciski palców i umożliwiająca ich porównywanie), europejski system nadzorowania granic (Eurosur) oraz rejestr danych dotyczących przelotu pasażera (PNR) (zob. [rys. 2](#)).

Ponadto UE prowadzi obecnie prace nad dwoma dodatkowymi systemami informacyjnymi istotnymi w kontekście ochrony granic: systemem wjazdu/wyjazdu i europejskim systemem informacji o podróży oraz zezwoleń na podróż, które powinny zacząć działać odpowiednio w 2020 i 2021 r.

Rys. 2 – Systemy informacyjne wykorzystywane przed kontrolą i w trakcie kontroli na granicach zewnętrznych

Przed granicą



Eurosur (2013)

- nadzorowanie granic zewnętrznych
- ramy umożliwiające wymianę informacji i obrazów sytuacji, obejmujące narzędzia nadzoru
- system zarządzany przez Frontex



PNR (2018)

- dane dotyczące pasażerów w ruchu lotniczym
- użytkownicy publiczni i prywatni (linie lotnicze)
- system zdecentralizowany, zarządzany przez poszczególne kraje

Na granicy



SIS II (2013)

- informacje na temat osób zaginionych lub poszukiwanych
- główny system w strefie Schengen
- system zarządzany przez eu-LISA



VIS (2015)

- wsparcie procedury składania wniosków wizowych
- narzędzie do weryfikacji wiz Schengen
- system zarządzany przez eu-LISA

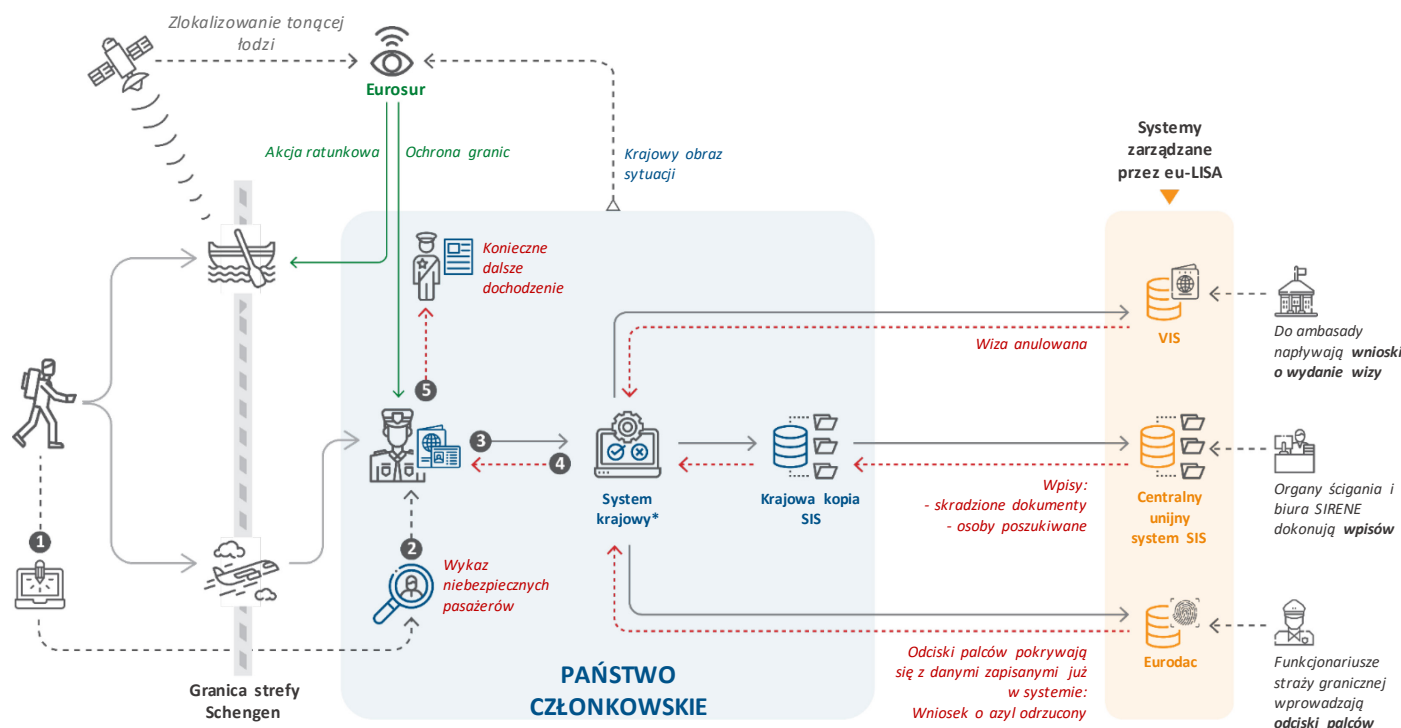


Eurodac (2003)

- baza odcisków palców
- system wykorzystywany przy wjeździe/wyjeździe i w postępowaniach karnych
- system zarządzany przez eu-LISA

04 Funkcjonariusze straży granicznej w państwach Schengen korzystają z systemów SIS II, VIS i Eurodac w celu kontrolowania osób fizycznych w punktach kontroli granicznej. Eurosur i PNR służą z kolei do uzyskania informacji na temat zdarzeń na granicach zewnętrznych UE i poza tymi granicami, jak również danych pasażerów przybywających drogą lotniczą spoza obszaru Schengen. Tym samym umożliwiają one przewidywanie zdarzeń, które mogą mieć wpływ na bezpieczeństwo granic. Na **rys. 3** pokazano, w jaki sposób funkcjonariusze straży granicznej powinni korzystać z tych systemów w trakcie odprawy granicznej. Bardziej szczegółowe informacje na temat tego, które z systemów informacyjnych są dostępne w danym kraju, przedstawiono w **załączniku**.

Rys. 3 – Wykorzystanie wybranych systemów informacyjnych na potrzeby zabezpieczenia granic



Źródło: Europejski Trybunał Obrachunkowy.

05 Użytkownikami systemów są ponadto różne krajowe organy ścigania, jak również służby celne oraz organy wizowe i sądownicze. Jednocześnie są one odpowiedzialne za wprowadzanie odpowiednich danych do tych systemów. W przypadku PNR informacje są przekazywane przez linie lotnicze.

06 Funkcjonariusze straży granicznej (i innych organów) korzystający z systemów w państwach członkowskich mają dostęp do centralnych systemów UE za pośrednictwem systemów krajowych, które zostały opracowane konkretnie do tego celu. Minimalne wymagania dotyczące wdrożenia tych krajowych systemów informacyjnych zostały określone przez ustawodawców UE w prawie unijnym².

07 Na szczeblu UE ogólna odpowiedzialność za rozwój i finansowanie systemów informacyjnych spoczywa na Komisji Europejskiej, a konkretnie na Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych (DG HOME). Wyjątek stanowi rejestr PNR, który nie posiada centralnego komponentu na poziomie UE (ale który może mimo to korzystać z finansowania unijnego). Począwszy od 2012 r. Komisja powierzyła przechowywanie danych i utrzymanie systemów SIS II, Eurodac i VIS Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA). Za zarządzanie systemem Eurosur odpowiada z kolei Europejska Agencja Straży Granicznej i Przybrzeżnej znana również jako Frontex, jak również państwa członkowskie.

² Rozporządzenie (WE) nr 1987/2006 w przypadku SIS II, decyzja Rady 2007/533/WSiSW w przypadku SIS II, rozporządzenie (WE) nr 767/2008 w przypadku VIS, rozporządzenie (UE) nr 603/2013 w przypadku Eurodac oraz rozporządzenie (UE) nr 1052/2013 w przypadku Eurosur. Dyrektywa (UE) 2016/681 w przypadku PNR.

08 Na podstawie dostępnych informacji Trybunał szacuje, że aby pokryć koszt utworzenia unijnych komponentów systemów objętych niniejszą kontrolą, z budżetu UE wyasygnowano łącznie ponad 600 mln euro³. Roczny koszt obsługi tych systemów wynosił natomiast około 61,5 mln euro⁴. Ponadto państwa członkowskie partycypują w kosztach opracowania i utrzymywania systemów krajowych, przeznaczając na ten cel własne środki budżetowe. Chociaż informacje na temat wydatków państw członkowskich na systemy krajowe nie zawsze są dostępne, istnieją przesłanki wskazujące na to, że są to pokaźne kwoty. Przykładowo stworzenie systemu SIS II kosztowało państwa członkowskie w przybliżeniu 235 mln euro, oprócz 95 mln euro pochodzących z budżetu UE⁵.

³ Kwota ta opiera się na informacjach przedstawionych w dokumentach opublikowanych przez Komisję lub informacjach uzyskanych z systemu księgowego (w przypadku SIS II i VIS). Nie obejmuje ona kosztów opracowania systemu Eurodac, ponieważ brak było danych zbiorczych na ten temat.

⁴ Kwota ta obejmuje zobowiązania eu-LISA na 2017 r. związane bezpośrednio z systemami informacyjnymi objętymi niniejszą kontrolą, zobowiązania Frontexu na 2017 r. dotyczące systemu Eurosur oraz środki na płatności z DG HOME na systemy SIS, VIS i Eurodac zrealizowane w 2017 r.

⁵ Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego nr 3/2014 pt. „Wnioski z prac Komisji Europejskiej nad systemem informacyjnym Schengen drugiej generacji (SIS II)”.

Zakres kontroli i podejście kontrolne

09 UE nieustannie podejmuje kroki w celu zapewnienia lepszej ochrony granic UE, co jest ważnym zagadnieniem dla obywateli unijnych. Zważywszy na rosnącą presję na granicach zewnętrznych UE spowodowaną sytuacją w zakresie bezpieczeństwa i migracji, kontrola przeprowadzona przez Trybunał miała na celu wskazanie tych aspektów w założeniach koncepcyjnych systemów i w ich użytkowaniu, które mogą pomóc funkcjonariuszom straży granicznej skuteczniej wykonywać ich obowiązki. Ponadto uwagi i zalecenia Trybunału mogą przyczynić się do lepszego ukierunkowania finansowania unijnego, które zostanie udostępnione w następnych wieloletnich ramach finansowych na wsparcie tych systemów.

10 Podstawowe pytanie kontrolne brzmiało:

- „Czy główne unijne systemy informacyjne w zakresie bezpieczeństwa wewnętrznego efektywnie wspierają kontrole graniczne?”.

11 To pytanie zostało rozbite na następujące pytania szczegółowe:

- Czy unijne systemy informacyjne w dziedzinie bezpieczeństwa wewnętrznego zostały opracowane w taki sposób, by zapewnić efektywne odprawy graniczne?
- Czy unijne systemy informacyjne w dziedzinie bezpieczeństwa wewnętrznego zapewniają funkcjonariuszom straży granicznej właściwe, aktualne i kompletne informacje w trakcie odpraw granicznych?

12 Trybunał objął kontrolą następujących pięć systemów: system informacyjny Schengen (SIS II), wizowy system informacyjny (VIS), Eurodac (europejska baza danych zawierająca odciski palców i umożliwiająca ich porównywanie), europejski system nadzorowania granic (Eurosur) oraz rejestr danych dotyczących przelotu pasażera (PNR).

13 W trakcie kontroli oceniono, na ile skutecznie systemy (zarówno krajowe, jak i centralne komponenty systemów UE) umożliwiały funkcjonariuszom straży granicznej i innych służb dokonywanie odpraw osób fizycznych wjeżdżających do strefy Schengen na wyznaczonych przejściach granicznych⁶. Do przejść takich zalicza się lądowe przejścia graniczne, porty morskie oraz porty lotnicze (w przypadku niektórych państw członkowskich lotniska to jedyne granice zewnętrzne UE).

14 Kontrolerzy dokonali przeglądu i przeanalizowali dokumenty strategiczne, oceny i dane statystyczne dotyczące pięciu systemów objętych kontrolą, jak również rozmaite dokumenty dotyczące wdrożenia tych systemów na poziomie krajowym i UE. Ponadto złożyli oni wizyty w punktach kontroli granicznej i przeprowadzili wywiady ze służbami granicznymi w Finlandii, we Francji, Włoszech, w Luksemburgu i Polsce. Spotkali się również z pracownikami DG HOME, Frontexu i eu-LISA.

15 W ramach kontroli przeprowadzono także ankietę skierowaną do funkcjonariuszy straży granicznej w 28 państwach członkowskich UE i czterech państwach stowarzyszonych w ramach strefy Schengen (Islandia, Liechtenstein, Norwegia i Szwajcaria) w celu uzyskania ich opinii jako użytkowników systemów. Łącznie otrzymano 951 odpowiedzi.

⁶ Trybunał poruszył już niektóre kwestie dotyczące nielegalnej migracji w sprawozdaniu specjalnym nr 6/2017 pt. „Podejście »Hotspot« – unijna odpowiedź na kryzys uchodźczy” i zamierza dalej analizować te zagadnienia w kolejnych publikacjach.

Uwagi

Założenia koncepcyjne systemów informacyjnych umożliwiają efektywne przeprowadzanie odpraw granicznych, ale eliminowanie uchybień zajmuje dużo czasu

16 Kontrolerzy ocenili, czy państwa strefy Schengen, w których przeprowadzono wizyty, stworzyły systemy informacyjne zgodnie z wymogami i terminami przewidzianymi w odnośnych przepisach UE. Przeanalizowali także mechanizm oceny Schengen i sprawdzili, w jakim zakresie państwa strefy Schengen korzystały z dostępnych środków finansowych UE w celu ustanowienia i doskonalenia systemów krajowych.

Systemy informacyjne spełniały zasadniczo wymogi UE, ale nie wszędzie funkcjonowały tak samo efektywnie

17 Każde państwo należące do strefy Schengen jest wprowadzić samodzielnie odpowiedzialne za zabezpieczenie własnych granic, aby jednak zapewnić ochronę całej strefy, niezbędna jest skuteczna współpraca, która wymaga pewnego stopnia koordynacji odpraw granicznych. W tym celu ustanowiono minimalne wymogi nadzorcze, które pomagają zagwarantować spójność i odpowiednią jakość odpraw granicznych i danych wprowadzanych do systemów informacyjnych.

18 Każde państwo strefy Schengen jest zobowiązane do stworzenia własnych komplementarnych systemów krajowych, które są podłączone do centralnych systemów UE. Państwa, w których przeprowadzono wizyty, wywiązały się z tego obowiązku zgodnie z wymogami określonymi w odnośnych przepisach. Kontrolerzy stwierdzili jednak, że o ile systemy spełniały wspólne wymogi minimalne, o tyle nie wszędzie funkcjonowały one tak samo skutecznie. Poniżej przedstawiono przykłady ilustrujące taki stan rzeczy.

19 Niektóre państwa nie udostępniają za pośrednictwem systemów krajowych wszystkich funkcji oferowanych w centralnych systemach UE, co odbija się niekorzystnie na skuteczności odpraw granicznych. Przykładowo w centralnym systemie SIS II istnieje opcja przechowywania i weryfikacji odcisków palców. Funkcja ta jest istotna, ponieważ nie zawsze istnieje możliwość zidentyfikowania danej osoby w oparciu o podstawowe dane osobowe, takie jak nazwisko i data urodzenia. Dane takie mogą być sfałszowane lub osoba może odmówić ich podania. Odciski palców

umożliwiają zidentyfikowanie osoby z dużo większym prawdopodobieństwem. Mimo to opcja wyszukiwania biometrycznego na podstawie odcisków palców przechowywanych w systemie SIS nie jest jeszcze dostępna we wszystkich systemach krajowych państw strefy Schengen, jako że niektóre z nich potrzebują więcej czasu, by wdrożyć niezbędne rozwiązania techniczne. W momencie gdy opcję identyfikacji daktyloskopijnej udostępniono na poziomie centralnym, swoją gotowość do korzystania z niej potwierdziło jedynie 10 państw strefy Schengen.

20 W trakcie kontroli wizy lub paszportu przez funkcjonariuszy straży granicznej w systemach pojawia się niekiedy komunikat o błędzie. Przyczyny takiej sytuacji mogą być wielorakie, np. niedostateczna jakość odcisków palców zapisanych w systemie, zakłócenia w łączności internetowej lub problemy z odczytem wizy. W centralnych systemach UE zazwyczaj pojawia się informacja o charakterze błędu, jednak w niektórych systemach krajowych (np. w Luksemburgu czy Finlandii) wyświetlany jest jedynie komunikat o błędzie, bez wskazania przyczyn. W takiej sytuacji funkcjonariusze straży granicznej muszą sprawdzić przyczyny błędu i ewentualnie poddać pasażera dodatkowej weryfikacji (w ramach tzw. drugiej linii kontroli), co wydłuża odprawę graniczną, a dla pasażera oznacza opóźnienie w podróży.

21 W przypadku systemu SIS II państwa strefy Schengen mogą korzystać z systemu i przysyłać zapytania bezpośrednio do centralnej bazy danych bądź stworzyć jej kopię krajową do tych celów. Większość państw korzysta z kopii krajowych, ale niektóre (Dania, Finlandia, Liechtenstein, Norwegia i Słowenia) są podłączone bezpośrednio do bazy europejskiej. Jeśli państwa decydują się na korzystanie z kopii krajowych SIS II, muszą dopilnować, by były one na bieżąco synchronizowane z centralną bazą europejską, tak aby zagwarantować, że kontrole graniczne będą przeprowadzane na podstawie najbardziej aktualnych informacji. Tymczasem w dwóch państwach w próbie kontrolnej (w Polsce i we Francji) przeprowadzone oceny wykazały rozbieżności między danymi w kopiach krajowych i w centralnej bazie danych.

22 Kontrolerzy stwierdzili również istnienie pewnych barier prawnych na szczeblu państw członkowskich (przepisy dotyczące bezpieczeństwa narodowego i ochrony danych osobowych), które uniemożliwiały wspólne korzystanie z zasobów ludzkich. Okazuje się bowiem, że funkcjonariusze straży granicznej wykonujący obowiązki w innym państwie strefy Schengen (np. w ramach pomocy przy wzmocnionych kontrolach w trakcie kryzysu migracyjnego w Grecji i we Włoszech) nie mogą korzystać z systemów krajowych w tym państwie. Zasadniczo nie są oni w stanie przeprowadzać odpraw samodzielnie, lecz mogą jedynie asystować funkcjonariuszom krajowym. Mogą oni wprawdzie zapewniać różnego rodzaju pomoc na drugiej linii kontroli (np. dane państwo Schengen może korzystać z usług eksperta ds. sfalszowanych dokumentów

z innego państwa), lecz ich pomoc przy weryfikacji dokumentów w punktach kontroli granicznej (tj. na pierwszej linii kontroli) ma ograniczony zakres. Dodatkową barierą są trudności językowe związane z pracą w innym państwie strefy Schengen.

23 Korzyści, jakie funkcjonariusze straży granicznej czerpią z systemów, są uzależnione od tego, w jakim stopniu zostali oni przeszkoleni w zakresie ich obsługi. Trybunał stwierdził, że w skontrolowanych państwach członkowskich nie wdrożono programu szkoleń na poziomie krajowym, które dotyczyłyby systemów SIS II i VIS, w związku z czym funkcjonariusze musieli uczyć się korzystania z tych systemów „na żywo” w praktyce, nie zaś w „bezpiecznym” otoczeniu, gdzie mogliby wypróbować różne funkcje i przećwiczyć scenariusze, z którymi nie będą się stykać często w codziennej pracy (np. trafienie w systemie dotyczące domniemanego terrorysty bądź zaginionej osoby nieletniej na przejściu granicznym).

Ze względu na opóźnienia we wdrażaniu Eurosur i PNR służby graniczne nie mogły wymieniać się istotnymi informacjami

24 W przypadku Eurosur i PNR mechanizmy ich wdrożenia były inne niż w odniesieniu do systemów opracowanych i zarządzanych przez eu-LISA. Z rozmaitych powodów w trakcie wdrażania obydwu tych systemów doszło do przypadków niedotrzymania terminów i opóźnień. W rezultacie istotne informacje, które miały być zapewniane przez te systemy, przez wiele miesięcy były niedostępne.

25 Eurosur został opracowany przez Frontex (komponent europejski) oraz państwa członkowskie (komponenty krajowe). Wszyscy uczestniczący w nim użytkownicy końcowi z organów krajowych korzystają z takiego samego interfejsu. System ma za zadanie wspierać współpracę między Frontexem a państwami członkowskimi UE, tak aby zapewnić im lepsze rozeznanie sytuacji i zwiększyć ich zdolności reagowania na granicach zewnętrznych UE. Państwa członkowskie powinny zapewniać wkład do tego systemu w postaci informacji na temat sytuacji na ich granicach (tzw. krajowy obraz sytuacji, obejmujący informacje na temat przypadków nielegalnego przekroczenia granicy, przestępczości transgranicznej, sytuacji kryzysowych oraz innych zdarzeń istotnych w tym kontekście), zapewniając tym samym wspólne dane wywiadowcze pozwalające uzyskać ogólnoeuropejski obraz sytuacji. Informacje takie są przydatne na przykład przy podejmowaniu decyzji o rozmieszczeniu funkcjonariuszy straży granicznej bądź do wykrywania podejrzanych pojazdów / statków.

26 W przypadku Eurosur opóźnienia wystąpiły w procesie tworzenia krajowych ośrodków koordynacji. Ośrodki te mają koordynować wymianę informacji pomiędzy wszystkimi służbami odpowiedzialnymi za nadzorowanie granic zewnętrznych.

W rozporządzeniu w sprawie Eurosur przewidziano wymóg, by wszystkie państwa członkowskie ustanowiły krajowe ośrodki koordynacji do grudnia 2014 r. Ewaluacja przeprowadzona niemal cztery lata później wykazała jednak, że niektóre państwa wciąż nie do końca spełniły wszystkie wymogi⁷. Ponadto jedynie połowa państw członkowskich udostępniała dobrowolnie informacje na temat rozmieszczenia swoich zasobów na potrzeby nadzorowania granic oraz dodatkowe informacje pochodzące z krajowych obrazów sytuacji.

27 Wdrażanie systemu Eurosur było opóźnione również na szczeblu UE. Frontex uzyskał wymagany certyfikat bezpieczeństwa dla odnośnej sieci dopiero pod koniec 2017 r., czyli trzy lata po wejściu w życie przepisów. Tymczasem bez tej certyfikacji nie było możliwości przesyłania informacji niejawnych za pośrednictwem sieci Eurosur. Opóźnienia we wdrażaniu systemu Eurosur oznaczały ponadto, że nie można było zapewnić pełnego ogólnounijnego obrazu sytuacji na granicach, co utrudniało współpracę między państwami członkowskimi.

28 Rejestr PNR nie jest jeszcze w pełni operacyjny. W przeciwieństwie do pozostałych systemów został on ustanowiony na mocy dyrektywy, a nie rozporządzenia. Oznacza to, że państwa członkowskie musiały osobno ustanowić swoje własne systemy PNR, bez wspólnej platformy europejskiej. Powodem podjęcia decyzji o zdecentralizowanym wdrażaniu był przede wszystkim brak konsensusu co do ochrony, przechowywania i ujawniania danych osobowych.

29 Wiele państw członkowskich nie wdrożyło PNR w przewidzianym na to terminie. 14 państw nie wdrożyło w terminie przepisów w sprawie danych dotyczących przelotu pasażera⁸. Termin przewidziany na to w dyrektywie⁹ upłynął 25 maja 2018 r. Mimo to do końca marca 2019 r., a więc 10 miesięcy po terminie, Hiszpania, Niderlandy i Finlandia nie notyfikowały do Komisji żadnych działań na szczeblu krajowym w celu wdrożenia PNR¹⁰.

⁷ Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie ewaluacji europejskiego systemu nadzorowania granic (EUROSUR), COM(2018) 632 final.

⁸ https://europa.eu/rapid/press-release_MEMO-18-4486_pl.htm

⁹ 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.

¹⁰ https://europa.eu/rapid/press-release_MEMO-19-1472_pl.htm

30 PNR wymaga przekazywania danych osobowych pasażerów w przypadku wszystkich lotów do i ze strefy Schengen. Do czasu kontroli żadne z państw członkowskich, w których przeprowadzono wizyty, z wyjątkiem Luksemburga, nie zawarło odnośnych porozumień ze wszystkimi liniami lotniczymi.

31 Rejestr PNR został ustanowiony jako istotne narzędzie do zapobiegania terroryzmowi i innym poważnym przestępstwom, ich wykrywania i ścigania. Poprzez porównanie danych z PNR z informacjami w bazach danych w obszarze bezpieczeństwa właściwe organy mogą wykryć osoby niebezpieczne. Ze względu na fakt, że niektóre krajowe systemy PNR nie zostały jeszcze ustanowione, służby graniczne w tych państwach nie mają dostępu z wyprzedzeniem do informacji na temat osób wysokiego ryzyka przekraczających granice.

32 Jako że rejestr PNR służy wyłącznie do gromadzenia danych identyfikacyjnych pasażerów i informacji na temat ich podróży, niezbędne są inne bazy danych umożliwiające zweryfikowanie, czy dany pasażer stanowi zagrożenie. Większość państw członkowskich korzysta w tym celu z systemu SIS II. Tekst rozporządzenia jest jednak interpretowany na różne sposoby. Przykładowo, zgodnie z interpretacją rozporządzenia w sprawie SIS II przyjętą przez Francję, w odniesieniu do list pasażerów nie dopuszcza się składania zapytań za pośrednictwem SIS II. W praktyce oznacza to, że aby sprawdzić listy pasażerów pod kątem osób podejrzewanych o terroryzm, we Francji wykorzystuje się jedynie informacje z krajowych baz danych. Jeśli więc w systemie SIS II istnieje wpis dotyczący osoby podejrzanej, która jest znana organom pozostałych państw europejskich, ale nie służbom francuskim, przeprowadzana przez te służby weryfikacja danych w rejestrze PNR nie wykaże żadnych trafień.

W ramach ocen Schengen ewaluacji poddawane są krajowe odprawy graniczne, ale eliminowanie wykrytych uchybień zajmuje dużo czasu

33 Począwszy od 2013 r. państwa Schengen oraz Komisja były wspólnie odpowiedzialne za wdrożenie mechanizmu monitorowania i oceny przewidzianego w przepisach dotyczących strefy Schengen (tzw. dorobku Schengen). Mechanizm ten ma na celu zagwarantowanie, by państwa strefy Schengen stosowały przepisy dorobku Schengen w sposób skuteczny, spójny i przejrzysty. Trybunał sprawdził, czy cel ten jest realizowany.

34 Obecnie obowiązujący wieloletni program ocen na lata 2015–2019 został przyjęty w 2014 r. i obejmuje wszystkie 26 państw strefy Schengen. Każde państwo jest oceniane raz w ciągu pięciu lat.

35 W **ramce 1** opisano standardową wizytę w ramach oceny. Członkowie zespołów oceniających są wyznaczani przez państwa strefy Schengen na podstawie wyników zaproszenia do nominacji kandydatów wystosowanego przez Komisję (na potrzeby każdej z ocen ogłaszane jest osobne zaproszenie z terminem dwóch tygodni na wyznaczenie kandydatów przez państwa strefy Schengen). W wizytach mogą uczestniczyć weryfikatorzy z ramienia eu-LISA, ale nie stanowi to regularnej praktyki. Koszt ocen Schengen jest stosunkowo niski w porównaniu z wydatkami na same systemy informacyjne. W latach 2014-2018 Komisja przeznaczyła na te oceny 11,9 mln euro. Obecny program wieloletni jest realizowany zgodnie z planem, za pośrednictwem rocznych planów ocen.

Ramka 1

Wizyty zespołów ds. oceny Schengen w państwach strefy Schengen

W lipcu w roku poprzedzającym wizytę państwa członkowskie otrzymują standardowy kwestionariusz do wypełnienia, który powinien zostać odesłany w ciągu ośmiu tygodni. Zespół ds. oceny przygotowuje wizytę w oparciu o udzielone w nim odpowiedzi.

Wizyty w ramach oceny trwają zazwyczaj tydzień. W skład zespołu wchodzi maksymalnie ośmiu ekspertów wyznaczonych przez państwa strefy Schengen oraz dwóch przedstawicieli Komisji. Członkowie zespołu dysponują wiedzą fachową w różnych obszarach, dzięki czemu są w stanie ocenić wszystkie aspekty dorobku Schengen. Na czele każdego zespołu stoi dwóch ekspertów wiodących (jeden z państwa członkowskiego i jeden z Komisji), którzy odpowiadają za treść i jakość sprawozdania końcowego.

Wizyty rozpoczynają się na szczeblu strategicznym od spotkań w ministerstwach i w siedzibie głównej służb granicznych. Następnie wykonywane są czynności na poziomie operacyjnym. Członkowie zespołu przydzielani są do konkretnych zadań w zależności od posiadanej wiedzy specjalistycznej i spotykają się z przedstawicielami różnych organów krajowych, na przykład z funkcjonariuszami straży granicznej i policji czy ekspertami ds. IT.

Przykładowo w ramach przeprowadzonej w 2017 r. oceny Schengen dotyczącej wdrożenia systemu SIS II we Francji zespół odwiedził 38 placówek w terenie, w tym krajowe centrum informatyczne SIS II, posterunki policji, urzędy celne, porty, lotniska i stacje kolejowe.

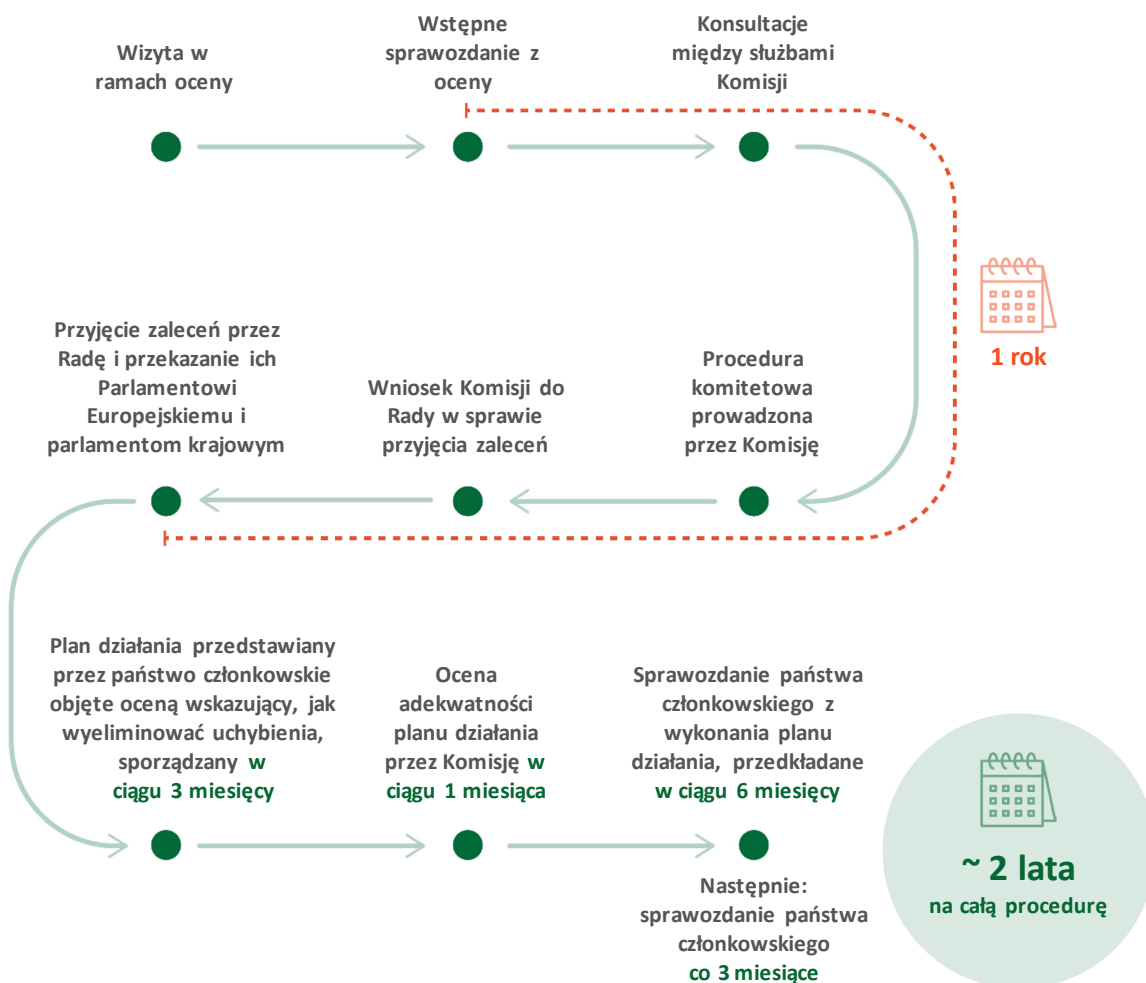
36 Kontrolerzy przeanalizowali oceny Schengen przeprowadzone w państwach objętych kontrolą i stwierdzili, że były one wnikliwe, metodyczne i uwzględniały kluczowe aspekty odnośnych systemów. W ich następstwie sformułowano szereg szczegółowych zaleceń operacyjnych, jak również konkretne zalecenia dotyczące udoskonalenia systemów informacyjnych. Wyeliminowanie wykrytych uchybień może jednak zająć kilka lat.

37 Wstępne sprawozdanie z oceny jest sporządzane w ciągu sześciu tygodni po zakończeniu wizyty, lecz następnie może minąć nawet rok, nim Komisja przyjmie sprawozdanie, a Rada przyjmie zalecenia. Wiąże się to bowiem z wieloma procedurami konsultacji z danym państwem strefy Schengen i Komisją. W przypadku tych konsultacji nie określono żadnych ram czasowych na ich przeprowadzenie.

38 Po przyjęciu zaleceń przez Radę państwo strefy Schengen ma trzy miesiące na przedstawienie planu działania uwzględniającego zalecenia Rady. Plan ten musi zostać zweryfikowany i zatwierdzony przez Komisję oraz zespół, który przeprowadził ocenę.

39 Choć na realizację planów działania nie przewidziano żadnych terminów, państwa strefy Schengen muszą zacząć przekazywać raporty na temat ich wdrażania sześć miesięcy po ich zatwierdzeniu. Oznacza to, że od momentu wykrycia danego uchybienia mogą minąć niemal dwa lata, nim państwo strefy Schengen zacznie przekazywać informacje na temat podjętych działań naprawczych. Na [rys. 4](#) zilustrowano procedurę po zakończonej wizycie w ramach oceny Schengen.

Rys. 4 – Kroki proceduralne w ramach mechanizmu oceny Schengen



Źródło: Europejski Trybunał Obrachunkowy.

40 Dotychczas żadne państwo strefy Schengen nie zostało objęte więcej niż jedną zapowiadzaną wizytą w ramach bieżącego cyklu ocen. Komisja polega na sprawozdawczości państw strefy Schengen z realizacji uzgodnionych planów działania. Istnieje zatem ryzyko, że pewne niedociągnięcia nie zostaną wyeliminowane aż do momentu przeprowadzenia kolejnej rundy ocen pięć lat później. Następnie mogą minąć kolejne dwa lata, zanim organy danego państwa wdrożą działania naprawcze.

41 Jeśli państwo strefy Schengen nie zrealizuje planu działania, Komisja może zalecić przeprowadzenie kolejnej wizyty, nie ma jednak innych mechanizmów, z których mogłaby skorzystać, by wyegzekwować wdrożenie tego planu. Teoretycznie jeśli w danym państwie stwierdzone zostaną utrzymujące się, poważne niedociągnięcia w obszarze zarządzania zewnętrznymi granicami, Rada, działając w oparciu o wniosek Komisji, może zalecić, by państwo to przywróciło kontrole na granicach z innymi państwami strefy Schengen.

42 Zgodnie z rozporządzeniem z 2013 r. w sprawie mechanizmu oceny Schengen¹¹ Komisja ma obowiązek przedstawiać co roku Parlamentowi Europejskiemu i Radzie sprawozdanie z przeprowadzonych ocen wraz z informacjami na temat wydanych zaleceń i stanu działań naprawczych. Komisja nie opracowała jeszcze takiego sprawozdania.

43 Z wyjątkiem Finlandii, w przypadku której sprawozdanie z oceny nie zostało sfinalizowane w momencie przeprowadzania kontroli, wszystkie państwa strefy euro, w których przeprowadzono wizyty, zostały objęte oceną. W związku z tym kontrolerzy sprawdzili postępy w realizacji ich planów działania i stwierdzili, że zostały one wykonane w różnym stopniu. Jak wynika z przedstawionych dowodów, Polska zrealizowała 79% zaleceń w ciągu dwóch lat od zakończenia wizyty, Francja wdrożyła 87% zaleceń w ciągu czterech lat od wizyty, natomiast Luksemburg, który został objęty oceną w 2018 r., zrealizował 92% zaleceń. Dowody przekazane przez Włochy sugerują z kolei, że dwa lata po wizycie w ramach oceny kraj ten był w trakcie realizacji 15% skierowanych do niego zaleceń.

Państwa członkowskie UE jedynie w ograniczonym stopniu korzystają z finansowania unijnego w celu udoskonalenia systemów informacyjnych wykorzystywanych w trakcie kontroli granicznych

44 Głównym instrumentem UE zapewniającym wsparcie w zakresie kontroli granicznych jest Fundusz Bezpieczeństwa Wewnętrznego (ISF), którego budżet na lata 2014–2020 wynosi 3,8 mld euro. Na Fundusz składają się:

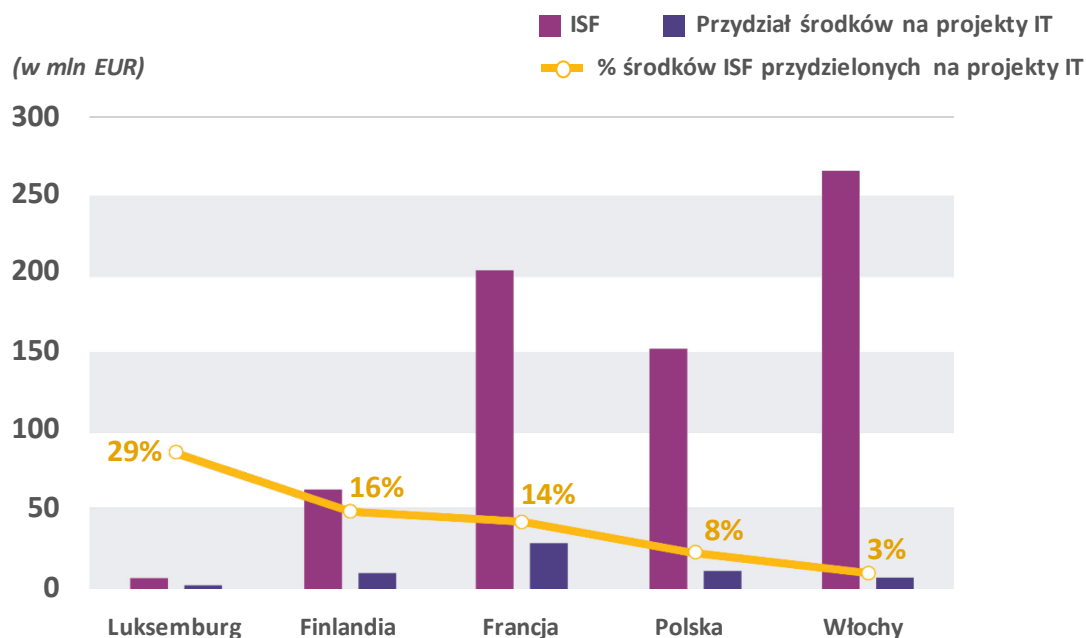
- komponent ISF „Granice i wizy” (2,76 mld euro), zapewniający wsparcie finansowe w zakresie zarządzania granicami zewnętrznymi oraz wspólnej polityki wizowej. W jego wdrażaniu uczestniczą wszystkie państwa członkowskie UE z wyjątkiem Irlandii i Zjednoczonego Królestwa oraz cztery państwa stowarzyszone w ramach Schengen (Islandia, Liechtenstein, Norwegia i Szwajcaria);
- komponent ISF „Policja” (1,04 mld euro) zapewniający wsparcie finansowe na rzecz współpracy policyjnej oraz zapobiegania i zwalczania przestępczości, w tym przemytu migrantów. W jego wdrażaniu uczestniczą wszystkie państwa członkowskie UE z wyjątkiem Danii i Zjednoczonego Królestwa.

¹¹ Art. 20 rozporządzenia Rady (UE) nr 1053/2013 z dnia 7 października 2013 r.

45 Do 2017 r. większość państw członkowskich nie zgłosiła żadnych istotnych wydatków. Jako że do wydatkowania przystąpiono z opóźnieniem, tempo wykorzystania środków przez państwa członkowskie było powolne. Zdaniem Komisji główną przyczyną takiego stanu rzeczy są skomplikowane procedury udzielania zamówień publicznych. Państwa objęte kontrolą zwracały również uwagę na dodatkowe obciążenia administracyjne. Zauważyły one na przykład, że nawet niewielki wzrost kwoty przydzielonej na rzecz programu krajowego wymaga kompletnej rewizji tego programu.

46 Skontrolowane państwa przeznaczyły od 3% do 29% środków przyznanych im z Funduszu Bezpieczeństwa Wewnętrznego (61,2 mln euro) na pięć systemów będących przedmiotem niniejszej kontroli (zob. [rys. 5](#)). 43% z tej kwoty (tj. 26,5 mln euro) posłużyło na sfinansowanie projektów związanych z konserwacją, a 57% (34,7 mln euro) na projekty dotyczące rozbudowy systemów. Państwa wykorzystały te środki przede wszystkim na konserwację systemów SIS II i VIS oraz na rozwój systemu Eurosur i rejestru PNR.

Rys. 5 – Odsetek środków finansowych ISF przydzielonych na projekty informatyczne



Źródło: Europejski Trybunał Obrachunkowy na podstawie informacji Komisji Europejskiej.

Funkcjonariusze straży granicznej nie zawsze uzyskują kompletne dane z systemów, co negatywnie wpływa na efektywność odpraw

47 Kontrolerzy Trybunału ocenili, w jakim zakresie państwa członkowskie udostępniają odpowiednie, aktualne i kompletne informacje za pośrednictwem systemów informacyjnych objętych kontrolą. Dokonany przez nich przegląd dostępnych danych statystycznych posłużył do oceny, w jakim stopniu państwa strefy Schengen korzystają z tych systemów na potrzeby odpraw granicznych i wymiany informacji. Ponadto kontrolerzy sprawdzili, czy państwa te wprowadzały kompletne dane do systemów bez zbędnej zwłoki.

Państwa członkowskie w coraz większym stopniu korzystają z systemów w celu udostępniania informacji, ale weryfikacje mogłyby być bardziej systematyczne

48 Od momentu gdy osoba chcąca przekroczyć granicę pojawi się w punkcie kontroli granicznej na granicy strefy Schengen, funkcjonariusze straży granicznej są zdani na europejskie systemy informacyjne, z których korzystają w celu potwierdzenia tożsamości tej osoby i sprawdzenia, czy jest ona upoważniona do wjazdu do strefy Schengen.

System SIS II

49 Każde państwo strefy Schengen posiadające informacje na temat osoby, która ma zostać zatrzymana na granicy (zgodnie z odpowiednimi przepisami), powinno stworzyć wpis w systemie SIS II. Dzięki temu funkcjonariusze straży granicznej w dowolnym państwie uczestniczącym będą mogli odpowiednio zareagować, jeśli wykryją taką osobę w trakcie odprawy granicznej (zob. [ramka 2](#)).

Ramka 2

Jak zidentyfikować osobę, która ma zostać zatrzymana?

Gdy osoba przedstawia dokument podróży, funkcjonariusz straży granicznej korzysta z czytnika, który odczytuje identyfikator na dokumencie. Najbardziej nowoczesne dokumenty są wyposażone w elektroniczny chip, natomiast starsze dokumenty mają specjalny kod na dole strony (w tzw. polu przeznaczonym do odczytu maszynowego). Niektóre dokumenty nie posiadają takich zabezpieczeń (np. większość włoskich dokumentów tożsamości). Jeśli numer dokumentu nie może zostać odczytany za pomocą czytnika, funkcjonariusz może go wpisać ręcznie w systemie.

Na podstawie danych wpisanych do komputera generowane jest zapytanie dotyczące danej osoby, przesyłane do krajowej i europejskiej bazy danych systemu SIS II. W przypadku gdy dane w bazie pokrywają się z danymi podanymi przez funkcjonariusza, mówimy o *trafieniu*.

Jeśli pierwotny wpis w bazie danych został stworzony w innym państwie niż kraj, skąd przesłano zapytanie, jest to tzw. *trafienie zagraniczne*.

Trafienia występują w sytuacji, gdy właściwe służby zgłosiły daną osobę jako poszukiwaną lub gdy dokument podróży został odpowiednio oznaczony w systemie.

Bywa jednak tak, że służby dokonujące wpisu nie posiadają wszystkich informacji niezbędnych do jednoznacznego zidentyfikowania tej osoby. Z tego względu może się zdarzyć, że trafienie będzie dotyczyć osoby, która nie jest poszukiwana, ale ma to samo imię i nazwisko. Mowa jest wtedy o *fałszywym trafieniu*. W takich przypadkach funkcjonariusze straży granicznej muszą podjąć dalsze działania, aby ustalić tożsamość danej osoby.

Jednym ze sposobów pozwalających jednoznacznie zidentyfikować osobę są dane biometryczne (tj. odciski palców), w związku z czym coraz więcej wpisów w systemie SIS II zawiera dane daktyloskopijne.

50 Kontrolerzy ustalili, że w latach 2013–2017 liczba trafień dotyczących poszukiwanych osób i przedmiotów na podstawie wpisów pochodzących z innych krajów wzrosła niemal trzykrotnie (zob. [rys. 6](#)).

Rys. 6 – Liczba trafień w systemie SIS II na podstawie wpisów z innych państw



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych przekazanych przez eu-LISA.

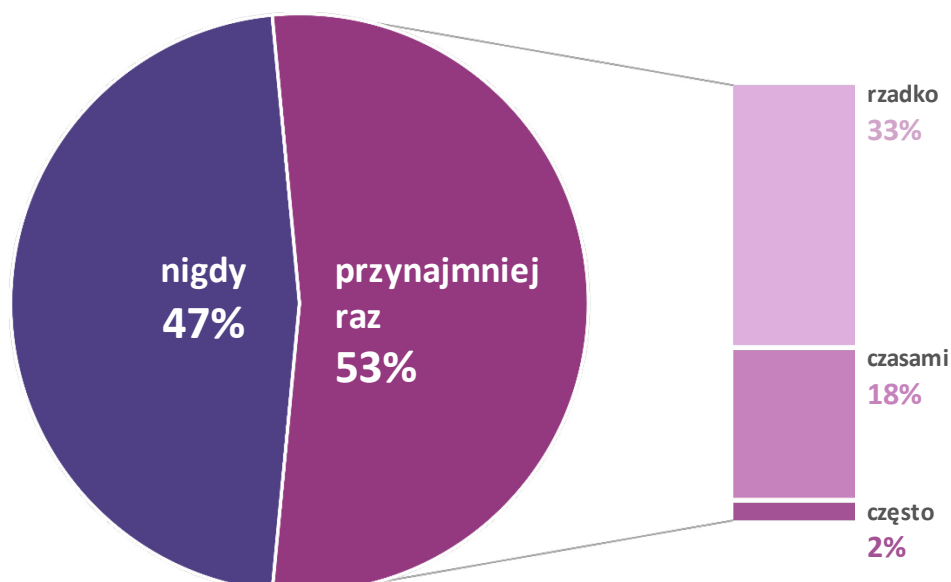
51 Ta większa liczba trafień wynika ze stałego wzrostu liczby wpisów w systemie SIS II, z około 50 mln w 2013 r. do ponad 76 mln w 2017 r. Większość wpisów (76%) dotyczy zgubionych lub skradzionych dokumentów.

52 Jak wynika z danych Eurostatu¹², liczba obywateli państw trzecich, którym odmówiono wjazdu na granicach zewnętrznych, oscylowała między 440 000 w 2017 r. a rekordową liczbą niemal 500 000 w 2009 r. Systemy informacyjne umożliwiają uzyskanie informacji na temat najczęstszych powodów odmowy wjazdu. Państwa strefy Schengen nie zawsze podają lub dokumentują jednak, dlaczego danej osobie odmówiono wjazdu na granicy zewnętrznej.

53 Jak wspomniano wyżej, liczba zapytań przesyłanych do systemów informacyjnych nieustannie rośnie. W trakcie wywiadów przeprowadzonych w ramach kontroli organy krajowe podkreśliły, że kontrolują każdą osobę, która pragnie przekroczyć granicę zewnętrzną. Z ankiety Trybunału wynika tymczasem, że ponad połowa funkcjonariuszy straży granicznej znalazła się już kiedyś w sytuacji, w której musieli oni podjąć decyzję o przepuszczeniu osoby przez granicę bez możliwości sprawdzenia jej danych w systemach.

¹² https://ec.europa.eu/eurostat/web/products-datasets/-/migr_eirfs

Rys. 7 – Ankieta: Czy zdarzyło się Panu/Pani podjąć decyzję o przepuszczeniu kogoś przez granicę bez możliwości sprawdzenia danych w systemie?



Źródło: ankieta Europejskiego Trybunału Obrachunkowego.

54 Korzystanie z systemów informacyjnych uzależnione jest również od warunków zewnętrznych, w jakich odbywają się odprawy. Na pewnych rodzajach przejść granicznych występują bowiem większe trudności niż na innych. Przykładowo w trakcie odpraw przeprowadzanych na pokładach statków często pojawiają się problemy z łącznością. W ramach wizyt w dwóch państwach kontrolerzy zaobserwowali tego typu trudności, które uniemożliwiły przeprowadzenie pełnych odpraw granicznych. Z podobnymi wyzwaniami technicznymi wiążą się kontrole w pociągach w trakcie jazdy.

System Eurodac

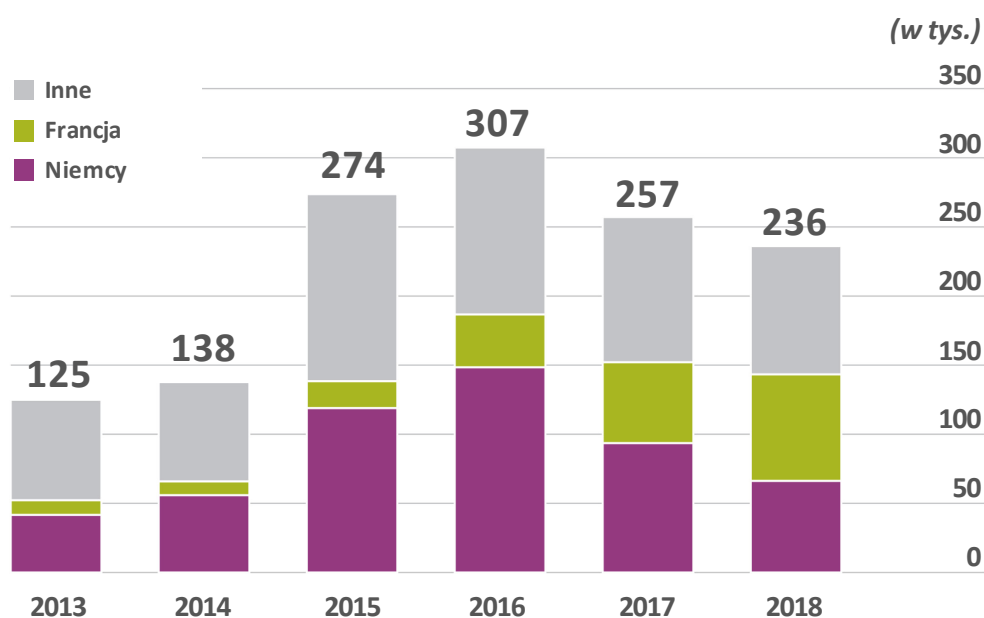
55 Państwa Schengen wymieniają się w coraz większym stopniu informacjami również za pośrednictwem systemu Eurodac, który służy do rejestracji (poprzez pobranie odcisków palców) osób ubiegających się o azyl oraz osób usiłujących nielegalnie przekroczyć granicę. Od 2003 r. państwa członkowskie UE są objęte porozumieniem¹³ stanowiącym, że wnioski o azyl powinny być rozpatrywane w państwie, w którym wnioskodawca po raz pierwszy zgłosi zamiar ubiegania się

¹³ Rozporządzenie Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiające kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego (rozporządzenie Dublin II).

o azyl. W przypadku gdy organ administracji krajowej porównuje odciski palców danej osoby z danymi w systemie Eurodac, otrzyma on trafienie, jeśli osoba ta wystąpiła już wcześniej o azyl w innym państwie członkowskim UE i powinna tam zostać odesłana.

56 Liczba wniosków o azyl złożonych przez osoby, które wystąpiły już z takim wnioskiem w innym państwie członkowskim, znacznie rosła do roku 2016, na który przypadło apogeum kryzysu migracyjnego. Jak pokazano na [rys. 8](#), większość osób ubiegających się o azyl we Francji lub w Niemczech przekroczyła granicę strefy Schengen w innym państwie UE.

Rys. 8 – Osoby ubiegające się o azyl, które złożyły wcześniej wniosek w innym państwie członkowskim



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych przekazanych przez eu-LISA.

Rejestr danych dotyczących przelotu pasażera

57 PNR to nowy system. Wprawdzie podstawa prawna do jego wdrażania jest wspólna dla wszystkich państw członkowskich, jednak możliwości korzystania przez nie z tego systemu w celu wymiany informacji są ograniczone, co wyjaśniono w pkt [28](#).

System Eurosur

58 Państwa członkowskie w bardzo nierównomierny sposób korzystają z systemu Eurosur. W latach 2013–2017 zarejestrowano w nim ponad 140 000 incydentów. Wiele uczestniczących państw nie zgłosiło jednak większej liczby incydentów¹⁴. Austria, Belgia, Cypr, Republika Czeska, Niemcy, Dania, Francja, Litwa, Luksemburg, Malta, Niderlandy, Portugalia, Szwecja i Słowenia zgłosiły mniej niż 5 000 incydentów, podczas gdy Węgry, najbardziej aktywne państwo pod tym względem, zarejestrowały ich ponad 25 000. Różnice występują również, jeśli chodzi o rodzaje informacji przekazywanych do systemu przez państwa członkowskie. Mogą one bowiem zdecydować, że będą zgłaszać jedynie informacje obowiązkowe (np. dane dotyczące nielegalnej migracji i przestępczości transgranicznej oraz informacje z nadzorowania granic lądowych i morskich) bądź też poszerzone informacje dodatkowe, dotyczące na przykład środków prawnych lub administracyjnych podjętych po przechwyceniu osób, oraz informacje na temat granic powietrznych i odpraw na przejściach granicznych. Przykładowo Finlandia postanowiła udostępniać wszystkie informacje z krajowego obrazu sytuacji, zarówno obowiązkowe, jak i opcjonalne, natomiast Polska i Francja przekazują jedynie informacje obowiązkowe.

System VIS

59 Państwa strefy Schengen mają wspólną politykę wizową. Mogą one wydawać wspólne wizy krótkoterminowe umożliwiające ich posiadaczom pobyt do 90 dni w którymkolwiek z 26 państw Schengen. W 2018 r. wydano ponad 14 mln wiz krótkoterminowych¹⁵.

60 System umożliwia kontrolę tożsamości posiadacza wizy Schengen na całym terytorium strefy Schengen. Taka osoba może wielokrotnie przekraczać granice zewnętrzne strefy w różnych państwach Schengen. Dane statystyczne z systemu VIS pokazują, ile razy sprawdzono wizy na granicach. W ciągu pierwszych dziewięciu miesięcy 2017 r. na granicach przeprowadzono 35 mln kontroli wizowych, w porównaniu z 12 mln wiz wydanych w tym okresie. Liczba przeprowadzonych kontroli znacznie różni się w zależności od państwa Schengen.

¹⁴ Ocena rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1052/2013 z dnia 22 października 2013 r. ustanawiającego europejski system nadzorowania granic, SWD(2018) 410 z 19.12.2018.

¹⁵ <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-policy#stats>

61 Kontrolerzy stwierdzili, że między październikiem 2015 r. a wrześniem 2017 r. pięć państw, które wydały największą liczbę wiz (Francja, Niemcy, Włochy, Hiszpania i Grecja), przeprowadziło na swoich granicach mniej kontroli wizowych niż wskazywałaby na to liczba wydanych wiz. Kraje te przeprowadziły niecałe 14 mln kontroli, zaś wydanych wiz było niemal 18 mln.

62 Teoretycznie taki stan rzeczy może wynikać z tego, że duża liczba podróżujących z wizą wydaną przez te kraje wjechała do strefy Schengen przez inny kraj, bądź też przesunęła termin podróży lub z niej zrezygnowała. Zważywszy jednak na to, że większość osób podróżujących występuje o wizę kraju, do którego zamierzają się udać, i że uzyskanie wizy wiąże się z pewnymi kosztami¹⁶, może to świadczyć o braku systematycznych kontroli wizowych we wszystkich punktach kontroli granicznej.

Informacje w niektórych systemach były niekompletne

63 Jakość danych w systemach informacyjnych ma niebagatelne znaczenie. Za wpisywanie danych do systemu odpowiadają organy sądowe i organy ścigania, jak również służby graniczne państw członkowskich. Funkcjonariusze straży granicznej wykorzystują te dane jako podstawę do podejmowania decyzji, które mają wpływ na bezpieczeństwo obywateli europejskich.

64 Zgodnie z prawodawstwem unijnym odpowiedzialność za jakość danych spoczywa na państwach członkowskich. Z tego względu kontrolerzy stwierdzili, że na szczęblu UE rzadko wspomina się o procedurach kontroli jakości danych. Jedynie w rozporządzeniu w sprawie Eurodac ustanowiono ramy kontroli jakości odcisków palców, przy czym opracowanie standardów jakości powierzono eu-LISA.

65 W rozporządzeniu w sprawie systemu SIS II nie przewidziano udziału Komisji bądź eu-LISA w procesie zapewniania jakości danych. Odpowiedzialność za to, by dane w systemie były prawidłowe, aktualne i adekwatne, powierzono natomiast państwom członkowskim¹⁷. Za funkcjonowanie SIS II i koordynację kontroli jakości informacji wprowadzanych do systemu odpowiedzialne są biura krajowe¹⁸.

¹⁶ Wiza Schengen kosztuje 60 euro.

¹⁷ Art. 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1987/2006 z dnia 20 grudnia 2006 r.

¹⁸ Art. 7 tamże.

66 Kwestia jakości danych zyskała na znaczeniu w 2018 r. wraz z wejściem w życie nowego rozporządzenia w sprawie eu-LISA¹⁹, na mocy którego Komisji i Agencji powierzono obowiązki w zakresie zapewniania jakości danych. W rozporządzeniu wprowadzono również wymóg przeprowadzania przez eu-LISA zautomatyzowanych kontroli jakości danych i prowadzenia sprawozdawczości na temat wskaźników jakości danych w odniesieniu do systemów SIS II, VIS i Eurodac.

67 Począwszy od kwietnia 2017 r. eu-LISA co miesiąc przeprowadza zautomatyzowane kontrole jakości danych dotyczące niektórych wpisów w systemie SIS II (np. w odniesieniu do problemów z transliteracją nazwisk zapisanych w alfabetach innych niż łaciński lub w przypadku gdy nie doszło do automatycznej kontroli ze względu na wpisanie ogólnego słowa, takiego jak „nieznany”). W następstwie tych kontroli generowany jest raport zawierający wykaz poszczególnych wpisów, w których wystąpiły potencjalne problemy z jakością. Jest on bezpośrednio przekazywany właściwemu państwu. Zgodnie z przepisami dotyczącymi ochrony danych eu-LISA nie ma wglądu do poszczególnych wpisów. Może ona jedynie uzyskać dostęp do informacji na temat łącznej liczby wykrytych problemów związanych z jakością w podziale na rodzaje wpisów i kraje.

68 Z comiesięcznych raportów wynika, że liczba ostrzeżeń dotyczących potencjalnych problemów z jakością wynosi około 3 milionów (spośród średnio 82 milionów wpisów), co oznacza, że dane te mogą nie spełniać wymogów jakościowych obowiązujących w SIS II. Kontrolerzy stwierdzili, że ani eu-LISA, ani Komisja nie posiadają odpowiednich uprawnień, by wyegzekwować od państw członkowskich szybkie usunięcie problemów w tym zakresie. Co więcej, ze sprawozdań nie wynika, by liczba ostrzeżeń w przypadku SIS II znacznie się zmniejszała. Ponieważ eu-LISA nie ma wglądu do indywidualnych wpisów, nie wiadomo też, czy wpisy w danym miesiącu są nowe, czy też zostały przeniesione z poprzednich sprawozdań jako nierozwiązane przypadki. Oprócz tak ogólnych informacji, których użyteczność z punktu widzenia zarządzania jakością jest ograniczona, kontrolerzy nie uzyskali żadnych dowodów świadczących o przeprowadzaniu innych zautomatyzowanych kontroli jakości danych na szczeblu UE.

¹⁹ Art. 12 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1726 w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA).

69 Jak wynika z przeprowadzonej przez Komisję oceny systemu SIS II²⁰, państwa Schengen zgłaszały niedociągnięcia dotyczące jakości danych jako częsty i powtarzający się problem. Ogólnie rzecz biorąc, w toku wizyt kontrolnych w państwach członkowskich stwierdzono, że problemy w tym zakresie są dwojakie: jedną z kwestii problematycznych jest kompletność danych, drugą zaś opóźnienia we wprowadzaniu danych do systemów.

70 Dane w systemie powinny umożliwiać funkcjonariuszom straży granicznej jednoznaczną identyfikację osoby w trakcie odprawy granicznej oraz podjęcie decyzji co do jej wjazdu do strefy Schengen. Kontrolerzy stwierdzili jednak, że niekiedy funkcjonariusze nie uzyskiwali odpowiednich informacji z systemu, by móc podjąć taką decyzję.

71 Przykładowo w trakcie kontroli wykryto wpisy, w których imię osoby zostało wpisane jako jej nazwisko bądź brakowało daty urodzenia, co utrudniało identyfikację tych osób²¹. W następstwie takich problemów, jeśli funkcjonariusze straży granicznej zechcą zweryfikować nazwisko w systemie SIS II, mogą otrzymać setki rezultatów (w większości fałszywych trafień), które następnie muszą sprawdzić ręcznie. Sprawia to nie tylko, że kontrole graniczne są mniej efektywne, ale zwiększa również ryzyko przeoczenia prawidłowych trafień.

72 Fakt, że dane w SIS II są niekompletne, ma również niekorzystny wpływ na skuteczne funkcjonowanie innych powiązanych systemów. Na przykład kiedy organy państw Schengen sprawdzają dane pasażerów na wykazie PNR, zazwyczaj porównują je z wpisami w systemie SIS II. Niekompletne wpisy skutkują dużą liczbą fałszywych trafień, które błędnie sugerują, że pasażer jest podejrzany. Ponieważ każdy taki wpis musi zostać zweryfikowany ręcznie, wiążą się z tym znaczne nakłady pracy po stronie jednostek do spraw informacji o pasażerach, które odpowiadają za obsługę wykazów PNR. Co więcej, dane w rejestrze PNR również mogą być niekompletne. Bywa bowiem

²⁰ Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny Systemu Informacyjnego Schengen drugiej generacji (SIS II) zgodnie z art. 24 ust. 5, art. 43 ust. 3 i art. 50 ust. 5 rozporządzenia (WE) nr 1987/2006 i art. 59 ust. 3 i art. 66 ust. 5 decyzji 2007/533/WSiSW, 21.12.2016, s. 11.

²¹ Z przeprowadzonej przez Komisję oceny systemu SIS II wynika, że wiele państw członkowskich zgłaszało niedociągnięcia w zakresie jakości danych jako częsty i powtarzający się problem. Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny Systemu Informacyjnego Schengen drugiej generacji (SIS II) zgodnie z art. 24 ust. 5, art. 43 ust. 3 i art. 50 ust. 5 rozporządzenia (WE) nr 1987/2006 i art. 59 ust. 3 i art. 66 ust. 5 decyzji 2007/533/WSiSW, 21.12.2016.

tak, że zestaw danych przekazanych z systemów rezerwacji obejmuje jedynie nazwiska pasażerów i numer lotu.

73 W systemie VIS można rejestrować tylko krótkoterminowe wizy Schengen, mimo że państwa strefy Schengen w dalszym ciągu wydają ponad 200 różnych rodzajów wiz krajowych i zezwoleń na pobyt umożliwiających obywatelom państw trzecich wjazd i swobodne poruszanie się po strefie Schengen. Zezwolenia te są rejestrowane wyłącznie w krajowych bazach danych, do których dostępu nie mają inne państwa. W 2017 r. w strefie Schengen wydano niemal 2,6 mln takich dokumentów²². Obecnie nie ma podstawy prawnej, która regulowałaby kwestię rejestrowania ich w centralnym systemie VIS.

74 Komisja wykryła tę lukę informacyjną i prowadzi obecnie prace nad rozporządzeniem, które ma ją wyeliminować²³. Ponieważ jednak te dokumenty podróży mogą być ważne nawet przez 10 lat, będą one w użyciu – i poza systemem – przez wiele lat, zanim ta luka zostanie wyeliminowana.

75 W przypadku Eurosur jedno z niedociągnięć wynika z tego, że państwa członkowskie przekazują swoje sprawozdania w różnych formatach. Oznacza to, że nie można w łatwy sposób agregować zawartych w nich informacji, a niekiedy sprawozdania mogą być niedostępne dla innych państw członkowskich z przyczyn technicznych.

76 W systemie Eurosur dane wprowadzane są zazwyczaj ręcznie. Jeśli liczba zdarzeń na granicach rośnie, operatorzy mogą mieć trudności z szybkim zarejestrowaniem ich w systemie, w wyniku czego ucierpieć może jakość danych²⁴. Ponadto niektóre państwa członkowskie zgłaszają incydenty indywidualnie, podczas gdy inne przekazują jedynie dane zbiorcze. Niektóre państwa sporządzają raport z incydentu w odniesieniu do każdej osoby, inne natomiast przygotowują jeden raport dotyczący kilku osób.

²² Dane statystyczne Eurostatu (pierwsze zezwolenia w 2017 r.):

http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=migr_resfirst&lang=en

²³ COM(2018) 302, Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 767/2008, rozporządzenie (WE) nr 810/2009, rozporządzenie (UE) 2017/2226, rozporządzenie (UE) 2016/399, rozporządzenie XX/2018 [rozporządzenie w sprawie interoperacyjności] i decyzję 2004/512/WE oraz uchylającego decyzję Rady 2008/633/WSiSW.

²⁴ Źródło: Ocena rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1052/2013 z dnia 22 października 2013 r. ustanawiającego europejski system nadzorowania granic (Eurosur), 12.9.2018, s. 44.

Powoduje to, że dane statystyczne dotyczące liczby incydentów przekazywane przez państwa członkowskie stają się bezużyteczne, ponieważ nie pokazują prawdziwej skali problemu. Frontexowi z kolei trudno jest monitorować zmieniającą się sytuację i podejmować decyzje o przydziale dodatkowych zasobów zgodnie z potrzebami.

Zdarzenia nie zawsze są szybko rejestrowane w systemach

77 Aby móc skutecznie wykonywać swoje obowiązki, funkcjonariusze straży granicznej muszą mieć dostęp do aktualnych informacji na temat osób przekraczających granice. Niekiedy jednak państwa nie wprowadzają informacji do systemów natychmiast po ich uzyskaniu.

78 Dane na potrzeby PNR są generowane w trakcie rezerwacji, a liniom lotniczym grożą grzywny w razie opóźnień przy przekazywaniu list pasażerów. W przypadku VIS dane generowane są automatycznie w momencie wydania wizy. Jeśli chodzi o Eurodac, w przepisach przewidziano termin przekazania informacji o osobach ubiegających się o azyl. W przypadku systemów SIS II i Eurosur natomiast nie wyznaczono konkretnych ram czasowych na wpisanie danych²⁵.

79 Eurosur ma w założeniu zapewniać informacje w czasie rzeczywistym na temat sytuacji na granicach, jednak to, czy informacje te będą faktycznie aktualne, zależy od tego, jak szybko państwa członkowskie wprowadzają je do systemu. Niektóre państwa objęte kontrolą Trybunału faktycznie wprowadzają dane do systemu Eurosur w czasie rzeczywistym, podczas gdy inne dokonują tego jedynie raz w tygodniu. Oznacza to, że informacja na temat zdarzenia na granicy (np. o przybyciu dużej liczby migrantów) może pojawić się w systemie europejskim dopiero tydzień później.

80 Zgodnie z przepisami rozporządzenia dublińskiego²⁶ za rozpatrzenie wniosku o azyl odpowiada państwo, przez którego granicę osoba ubiegająca się o azyl po raz pierwszy wjechała na terytorium Unii Europejskiej. Od momentu gdy dana osoba wystąpi o azyl lub zostanie zatrzymana w trakcie nielegalnego przekraczania granicy, państwa członkowskie mają maksymalnie 72 godziny²⁷ na pobranie odcisków palców i przekazanie ich do systemu Eurodac. Jeśli taka osoba przemieści się do innego

²⁵ Dane na potrzeby PNR są generowane w trakcie rezerwacji, a liniom lotniczym grożą grzywny w razie opóźnień przy przekazywaniu list pasażerów. W przypadku VIS dane generowane są automatycznie w momencie wydania wizy.

²⁶ Rozporządzenie (UE) nr 604/2013.

²⁷ Art. 9 ust. 1 i art. 14 ust. 2 rozporządzenia w sprawie Eurodac.

państwa członkowskiego, opóźnienia w przekazywaniu danych mogą sprawić, że za właściwy do rozpatrzenia wniosku o azyl uznany zostanie nieprawidłowy kraj (zob. pkt 55–56).

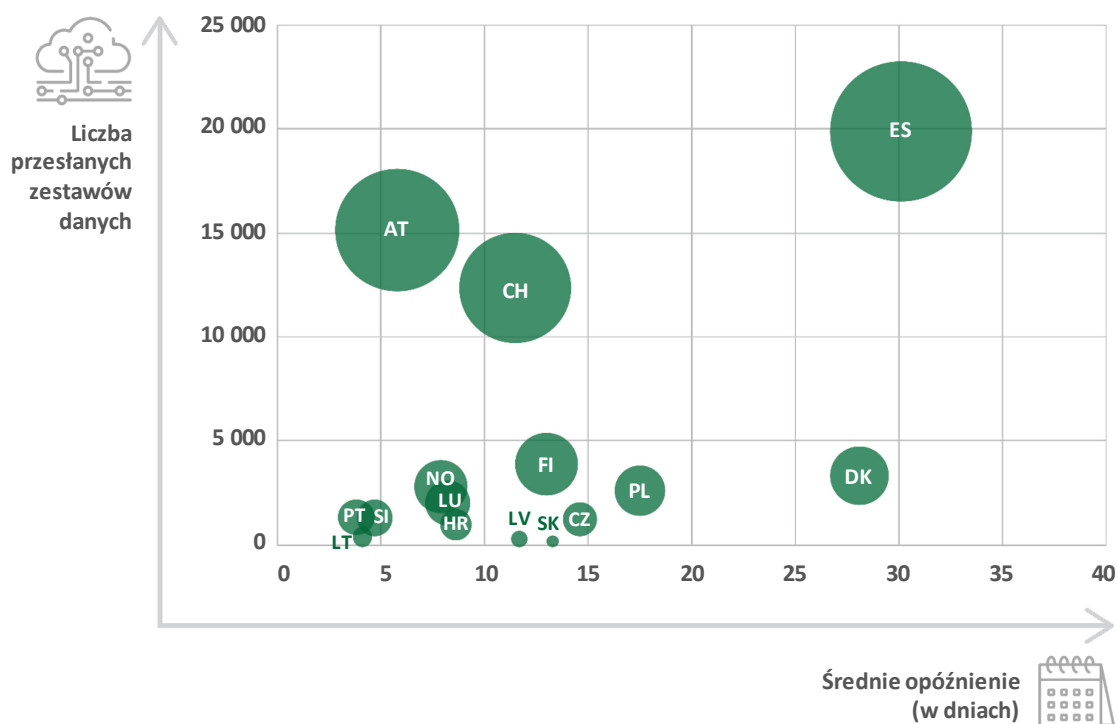
Zdjęcie 1 – Pobieranie odcisków palców na potrzeby rejestracji w systemie Eurodac



© Unia Europejska, 2015 / Źródło: Serwis audiowizualny KE / Fotograf: Angelos Tzortzinis.

81 Odkąd Eurodac zaczął funkcjonować, nie odnotowano ani jednego roku, w którym wszystkie państwa członkowskie przekazałyby wymagane informacje w terminie. W 2017 r. w przypadku piętnastu państw średni czas przekazywania danych przekraczał ustalony termin na przekazanie odcisków palców – zob. [rys. 9](#). W rozporządzeniu przewidziano pewne odstępstwa od terminów wpisywania danych, nie ma jednak mechanizmu, który umożliwiłby odróżnienie takich przypadków od opóźnień niezgodnych z przepisami.

Rys. 9 – Średnie opóźnienia w przekazywaniu odcisków palców w 2017 r.



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych przekazanych przez eu-LISA, Roczne sprawozdanie z działalności dotyczące centralnego systemu Eurodac.

82 Jak pokazano na [rys. 9](#), w 2017 r. w Hiszpanii przekazanie odcisków palców do systemu Eurodac zajmowało średnio 30 dni. Oznacza to, że osoba zatrzymana w trakcie nielegalnego przekraczania granicy hiszpańskiej miała średnio 30 dni, by przedostać się do innego państwa członkowskiego w celu złożenia tam wniosku o azyl. W trakcie weryfikacji odcisków palców w systemie Eurodac organy w takim państwie nie otrzymałyby żadnych trafień. Tym samym państwo to byłoby zobowiązane do rozpatrzenia wniosku o azyl złożonego przez taką osobę.

Wnioski i zalecenia

83 Trybunał przeanalizował, czy unijne systemy informacyjne w zakresie bezpieczeństwa wewnętrznego efektywnie wspierają kontrole graniczne. Na podstawie tej analizy stwierdził, że funkcjonariusze straży granicznej w coraz większym stopniu korzystają z tych systemów i polegają na nich przy dokonywaniu odpraw granicznych. W systemach brakuje jednak obecnie pewnych danych, a inne dane są niekompletne bądź nie są wprowadzane w przewidzianych na to terminach, co negatywnie wpływa na efektywność niektórych odpraw granicznych.

84 Kontrolerzy stwierdzili, że unijne systemy informacyjne zostały zasadniczo opracowane w sposób umożliwiający sprawne dokonywanie odpraw granicznych. Państwa, w których przeprowadzono wizyty kontrolne, ustanowiły swoje systemy zgodnie z obowiązującymi przepisami. Mimo to niektóre komponenty krajowe systemów SIS II i VIS umożliwiały sprawniejsze dokonywanie odpraw granicznych niż inne (zob. pkt 17–21).

85 Państwa członkowskie wprowadziły w coraz większym zakresie udostępniają informacje za pośrednictwem systemów, jednak bariery prawne (przepisy dotyczące ochrony danych osobowych i bezpieczeństwa narodowego) uniemożliwiają wspólne korzystanie z zasobów ludzkich. Funkcjonariusze straży granicznej oddelegowani do innego państwa członkowskiego nie mają dostępu do systemów informacyjnych w celu dokonywania odpraw granicznych. Kontrolerzy zauważyli ponadto, że ustanowieniu systemów nie towarzyszyły kursy szkoleniowe, w ramach których funkcjonariusze straży granicznej mogliby przećwiczyć scenariusze, z którymi nie stykają się często w codziennej pracy (zob. pkt 22–23).

Zalecenie 1 – Promowanie korzystania z programów szkoleniowych w zakresie systemów SIS II i VIS

Komisja powinna promować korzystanie przez państwa członkowskie z centralnych programów szkoleniowych w zakresie systemów SIS II i VIS, co umożliwiłoby funkcjonariuszom straży granicznej zetknięcie się z rzeczywistymi sytuacjami w trakcie szkoleń.

Termin realizacji: koniec 2020 r.

86 Przy wdrażaniu rozwiązań informatycznych występowały niekiedy opóźnienia, zarówno na szczeblu UE, jak i krajowym. Cztery lata po wejściu w życie rozporządzenia

w sprawie Eurosur zaledwie połowa państw członkowskich udostępniała wszystkie obowiązkowe i dobrowolne informacje na platformie stworzonej na potrzeby tego systemu. 14 państw nie wdrożyło w terminie przepisów w sprawie danych dotyczących przelotu pasażera. Spowodowało to, że służby graniczne nie miały pełnego obrazu sytuacji na zewnętrznych granicach strefy Schengen ani nie miały dostępu z wyprzedzeniem do informacji na temat osób wysokiego ryzyka przekraczających granice (zob. pkt 24–32).

87 Mechanizm oceny Schengen odgrywa istotną rolę w monitorowaniu przestrzegania przez państwa strefy Schengen przepisów dorobku Schengen. Z obserwacji kontrolerów wynika, że oceny te były ogólnie wnikliwe, metodyczne i uwzględniały kluczowe aspekty odnośnych systemów. Wyeliminowanie stwierdzonych w ich toku uchybień zajmuje jednak państwom strefy Schengen dużo czasu, co wynika z braku terminów na przyjęcie sprawozdań z oceny i realizację planów działań naprawczych (zob. pkt 33–41).

88 Komisja nie wywiązała się z obowiązku przekazywania co roku Parlamentowi Europejskiemu i Radzie sprawozdania na temat przeprowadzonych ocen. Kontrolerzy stwierdzili, że choć od zakończenia niektórych ocen upłynęły już nawet cztery lata, żadne z państw strefy Schengen objętych kontrolą nie zrealizowało w pełni planu działania. Fakt ten świadczy o tym, że proces oceny nie skutkuje szybkim wyeliminowaniem wykrytych uchybień (zob. pkt 42–43).

Zalecenie 2 – Szybsze eliminowanie uchybień stwierdzonych w trakcie ocen Schengen

Komisja powinna:

- a) przekazując Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny zgodnie z art. 22 rozporządzenia nr 1053/2013, zawrzeć w nim informacje na temat opóźnień we wdrażaniu przez państwa strefy Schengen ich planów działania uwzględniających zalecenia Rady;
- b) zaproponować odpowiednie środki ustawodawcze i proceduralne, aby skrócić czas trwania cyklu ocen Schengen.

Termin realizacji: koniec 2020 r.

89 Za pośrednictwem Funduszu Bezpieczeństwa Wewnętrznego UE zapewnia państwom członkowskim środki finansowe na rozwijanie i utrzymywanie systemów

informacyjnych objętych niniejszą kontrolą. Państwa, w których Trybunał przeprowadził wizyty kontrolne, przeznaczały na te pięć systemów średnio 15% środków przyznanych im z Funduszu Bezpieczeństwa Wewnętrznego. Wykorzystywały one te środki przede wszystkim na konserwację systemów SIS II i VIS oraz na rozwój systemu Eurosur i rejestru PNR (zob. pkt 44–46).

90 Z ustaleń kontrolerów wynika, że państwa członkowskie w coraz większym stopniu korzystają z tych systemów. W latach 2013–2017 liczba trafień w systemie SIS II dotyczących osób i przedmiotów poszukiwanych na podstawie wpisów pochodzących z innych krajów wzrosła niemal trzykrotnie (zob. pkt 47–58).

91 Sposób korzystania z systemów mógłby być jednak bardziej systematyczny. Z ankiety Trybunału wynika bowiem, że ponad połowa funkcjonariuszy straży granicznej znalazła się już kiedyś w sytuacji, w której musiała podjąć decyzję o przepuszczeniu osoby przez granicę bez sprawdzenia jej danych w systemach. Zauważono także rozbieżność pomiędzy liczbą wydanych i skontrolowanych wiz. Co więcej, system VIS obsługuje tylko krótkoterminowe wizy Schengen i obecnie nie jest przystosowany do tego, by rejestrować informacje na temat wiz krajowych, których posiadacze również mają prawo wjazdu do dowolnego państwa strefy Schengen. Tymczasem tylko w 2017 r. w strefie Schengen wydano niemal 2,6 mln takich dokumentów (zob. pkt 59–62). Komisja wykryła tę lukę informacyjną i przedłożyła wniosek w sprawie rewizji ram prawnych dotyczących VIS.

Zalecenie 3 – Przeanalizowanie rozbieżności w przypadku kontroli wizowych

Komisja powinna przeanalizować przyczyny rozbieżności między liczbą wydanych i skontrolowanych wiz Schengen oraz zaproponować środki naprawcze.

Termin realizacji: koniec 2020 r.

92 Dane w systemach służą funkcjonariuszom straży granicznej za podstawę do podejmowania decyzji, które mają wpływ na bezpieczeństwo obywateli europejskich. Jakość tych danych ma zatem niebagatelne znaczenie. Kontrolerzy stwierdzili jednak, że w aktach prawnych dotyczących europejskich systemów informacyjnych rzadko wspomina się o kwestii jakości danych. W rozporządzeniu w sprawie systemu SIS II odpowiedzialność za jakość danych powierzono państwom członkowskim, bez udziału Komisji bądź eu-LISA (zob. pkt 63–65).

93 Agencja eu-LISA przeprowadza wprawdzie co miesiąc automatyczne weryfikacje danych w systemie SIS II i przekazuje wyniki tych weryfikacji odnośnym państwom, ale ma dostęp jedynie do informacji zbiorczych na temat liczby wykrytych problemów związanych z jakością w podziale na rodzaje wpisów i kraje. Takie raporty nie są jednak dostatecznie szczegółowe, by umożliwić prześledzenie postępów w rozwiązywaniu problemów w zakresie jakości danych. Ponadto ani eu-LISA, ani Komisja nie posiadają odpowiednich uprawnień, by wyegzekwować od państw strefy Schengen szybkie wyeliminowanie problemów w tym obszarze (zob. pkt [67–70](#)).

94 W trakcie kontroli stwierdzono, że funkcjonariusze straży granicznej nie zawsze uzyskują aktualne i kompletne dane z systemów informacyjnych, co negatywnie wpływa na skuteczność odpraw granicznych. Jeśli przykładowo chcą oni zweryfikować nazwisko w systemie SIS II, mogą otrzymać setki rezultatów (w większości fałszywych trafień), które następnie muszą sprawdzić ręcznie. Sprawia to nie tylko, że odprawy graniczne są mniej efektywne, ale zwiększa również ryzyko przeoczenia prawidłowych trafień (zob. pkt [71–76](#)).

Zalecenie 4 – Udoskonalenie procedur kontroli jakości danych

Komisja powinna:

- a) zwrócić się do eu-LISA o uwzględnienie w prowadzonym przez nią co miesiąc monitorowaniu danych statystycznych na temat działań naprawczych podjętych przez państwa strefy Schengen;
- b) jeśli monitorowanie jakości danych nie przyniesie poprawy sytuacji – podjąć niezbędne kroki (np. poprzez wydanie wytycznych lub za pośrednictwem istniejących grup doradczych) w celu zachęcenia państw strefy Schengen do zintensyfikowania działań naprawczych.

Termin realizacji: do końca 2020 r.

95 Z wyjątkiem systemu Eurodac zasadniczo nie ma wiążących terminów wprowadzania danych do systemów. Przykładowo Eurosur ma w założeniu zapewniać informacje w czasie rzeczywistym na temat sytuacji na granicach zewnętrznych. O ile jednak niektóre państwa objęte kontrolą Trybunału faktycznie wprowadzają dane do tego systemu w czasie rzeczywistym, o tyle inne dokonują tego jedynie raz w tygodniu. Z kolei odkąd Eurodac zaczął funkcjonować w 2003 r., nie odnotowano ani jednego roku, w którym wszystkie państwa członkowskie przekazałyby wymagane informacje w terminie. Tymczasem opóźnienia w przekazywaniu danych mogą spowodować, że za

właściwy do rozpatrzenia wniosku o azyl uznany zostanie nieprawidłowy kraj (zob. pkt 77–82).

Zalecenie 5 – Zmniejszenie opóźnień we wprowadzaniu danych

Komisja powinna:

- a) przeanalizować przyczyny niezgodnych z przepisami opóźnień we wprowadzaniu danych do systemu Eurodac i podjąć odpowiednie działania w przypadku odnośnych państw członkowskich;
- b) zaproponować w ramach najbliższego przeglądu przepisów dotyczących systemu Eurosur, by uwzględniono w nich wiążące terminy wprowadzania danych.

Termin realizacji: koniec 2021 r.

Niniejsze sprawozdanie zostało przyjęte przez Izbę III, której przewodniczy Bettina JAKOBSEN, członek Trybunału Obrachunkowego, na posiedzeniu w Luksemburgu w dniu 8 października 2019 r.

W imieniu Europejskiego Trybunału Obrachunkowego

Klaus-Heiner Lehne
Prezes

Załącznik

Krótki opis wybranych systemów informacyjnych

System SIS II

System informacyjny Schengen (SIS) to najpowszechniej wykorzystywany i największy system wymiany informacji do celów bezpieczeństwa i zarządzania granicami w Europie. SIS II umożliwia właściwym organom krajowym, np. policji lub służbom granicznym, wprowadzanie lub sprawdzanie wpisów dotyczących osób bądź przedmiotów. Oprócz informacji na temat konkretnej osoby lub przedmiotu wpis w systemie SIS zawiera także instrukcje określające sposób postępowania po zidentyfikowaniu danej osoby lub odnalezieniu danego przedmiotu przez organy.

Na system SIS II składają się trzy główne komponenty: system centralny, systemy krajowe oraz infrastruktura (sieć) umożliwiająca łączność między tymi systemami. Wpis dokonany w systemie SIS II w jednym państwie strefy Schengen jest przekazywany w czasie rzeczywistym do systemu centralnego, gdzie następnie jest widoczny dla wszystkich pozostałych państw.

Każde państwo strefy Schengen korzystające z systemu SIS II odpowiada za ustanowienie, obsługę i utrzymanie swojego systemu krajowego oraz krajowego biura SIRENE, które pełni rolę pojedynczego punktu kontaktowego w zakresie wymiany informacji i koordynacji działań dotyczących wpisów SIS II.

Za zarządzanie operacyjne centralnym systemem i infrastrukturą łączności odpowiada Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi (eu-LISA).

Komisja Europejska jest z kolei odpowiedzialna za ogólny nadzór nad systemem i jego ocenę, jak również za przyjmowanie środków wykonawczych.

System SIS II funkcjonuje w 30 państwach europejskich, w tym w 26 państwach członkowskich UE (do SIS II nie są podłączone jedynie Irlandia i Cypr) i w czterech państwach stowarzyszonych w ramach Schengen (Szwajcaria, Norwegia, Liechtenstein i Islandia).

System VIS

Wizowy system informacyjny (VIS) wspiera wdrażanie wspólnej unijnej polityki wizowej i służy państwom strefy Schengen do wymiany danych wizowych. Umożliwia on kojarzenie danych biometrycznych, przede wszystkim odcisków palców, do celów identyfikacji i weryfikacji.

Tym samym pozwala on funkcjonariuszom straży granicznej zweryfikować, czy osoba okazująca wizę jest jej prawowitym posiadaczem, czy wiza jest autentyczna oraz czy osoba ta nadal spełnia wymogi wizowe.

Od osób ubiegających się o wizę wymagane jest zdjęcie cyfrowe oraz odciski dziesięciu palców. Te dane biometryczne, jak również informacje podane we wniosku o wizę, są rejestrowane w bezpiecznej centralnej bazie danych. Wykorzystanie danych biometrycznych w celu potwierdzenia tożsamości posiadacza wizy pozwala przeprowadzać odprawy graniczne szybciej, precyzyjniej i bezpieczniej. System ten usprawnia ponadto proces wydawania wiz.

Na system VIS składa się centralny system informatyczny oraz infrastruktura łączności między systemem centralnym a systemami krajowymi. VIS zapewnia łączność między konsulatami w krajach spoza UE i wszystkimi przejściami granicznymi na granicach zewnętrznych państw strefy Schengen. Służy on do przetwarzania i przechowywania danych i decyzji dotyczących wniosków o wizy krótkoterminowe.

System VIS, jako instrument Schengen, jest wykorzystywany we wszystkich państwach strefy Schengen. Za zarządzanie operacyjne systemem odpowiada Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi (eu-LISA).

System Eurodac

Eurodac to unijna baza odcisków palców osób ubiegających się o azyl. Służy przede wszystkim wdrożeniu rozporządzenia (UE) nr 604/2013 (tzw. rozporządzenie dublińskie). Gdy dana osoba występuje o azyl, bez względu na miejsce pobytu w UE, jej odciski palców są przesyłane do centralnego systemu Eurodac.

Od momentu utworzenia w 2003 r. Eurodac pomaga w ustaleniu państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie azylu.

Poza odciskami palców (łącznie z datą i miejscem ich pobrania) w Eurodac nie są gromadzone żadne inne dane osobowe. Z systemu tego korzysta 28 państw członkowskich UE oraz państwa stowarzyszone w ramach Schengen: Islandia, Liechtenstein, Norwegia i Szwajcaria.

System Eurosur

Europejski system nadzorowania granic (Eurosur) zapewnia ramy zarządzania i współpracy między państwami członkowskimi i **Europejską Agencją Straży Granicznej i Przybrzeżnej (Frontex)** w celu zagwarantowania lepszej znajomości sytuacji europejskiej na zewnętrznych granicach oraz zapewnienia większych zdolności reagowania. Ma on na celu zapobieganie nieuregulowanej imigracji i przestępczości transgranicznej, a także przyczynianie się do ochrony życia migrantów.

Zgodnie z rozporządzeniem w sprawie Eurosur każde państwo strefy Schengen posiada krajowy ośrodek koordynacji zajmujący się koordynacją i wymianą informacji pomiędzy wszystkimi organami krajowymi odpowiedzialnymi za nadzorowanie granic zewnętrznych, jak również z pozostałymi ośrodkami i Frontexem.

Frontex odpowiada za koordynację tzw. wspólnego stosowania narzędzi nadzoru – państwa członkowskie mogą zwrócić się do niego o pomoc w monitorowaniu wybranych obszarów lub statków na potrzeby systemu Eurosur, z wykorzystaniem narzędzi takich jak obrazy satelitarne czy systemy zgłaszania statków morskich. Informacje te mogą posłużyć do wykrywania przypadków nieuregulowanej migracji lub przestępczości transgranicznej, ale również do zlokalizowania łodzi znajdującej się w niebezpieczeństwie na morzu.

Z systemu Eurosur korzystają wszystkie państwa strefy Schengen, jak również Bułgaria, Rumunia i Chorwacja.

Rejestr danych dotyczących przelotu pasażera (PNR)

Rejestr danych dotyczących przelotu pasażera zawiera informacje przekazywane liniom lotniczym przez pasażerów w trakcie dokonywania rezerwacji i podczas odprawy. Może on zatem obejmować informacje takie jak daty podróży, trasa podróży, informacje o bilecie, dane kontaktowe, biuro podróży, metoda płatności, numer miejsca i informacje o bagażu. 27 kwietnia 2016 r. Parlament Europejski i Rada przyjęły dyrektywę (UE) 2016/681 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.

Na jej mocy wszystkie państwa członkowskie UE z wyjątkiem Danii²⁸ są zobowiązane do ustanowienia podmiotów odpowiedzialnych za gromadzenie, przechowywanie i przetwarzanie danych PNR, tzw. jednostek do spraw informacji o pasażerach (PIU). Jednostki te zbierają dane PNR od przewoźników lotniczych, korzystając w tym celu ze specjalnego systemu informatycznego, i porównują je z danymi w odnośnych bazach danych organów ścigania. Przetwarzają je również według wcześniej ustalonych kryteriów w celu wykrycia osób, które mogą brać udział w przestępstwach terrorystycznych lub w poważnej przestępczości. Odpowiadają one ponadto za przesyłanie danych PNR funkcjonariuszom straży granicznej oraz innym właściwym służbom krajowym, Europolowi oraz jednostkom do spraw informacji o pasażerach z innych państw członkowskich.

²⁸ Na podstawie protokołu nr 22 do Traktatów Dania nie wdraża dyrektywy w sprawie PNR.

Wykaz akronimów

DG HOME – Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych

EBCG – Europejska Agencja Straży Granicznej i Przybrzeżnej

eu-LISA – Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości

Eurodac – europejski system identyfikacji odcisków palców

Eurosur – europejski system nadzorowania granic

Frontex – *zob. EBCG*

ISF – Fundusz Bezpieczeństwa Wewnętrznego

NCC – krajowy ośrodek koordynacji

PNR – rejestr danych dotyczących przelotu pasażera

SIS II – system informacyjny Schengen II

VIS – wizowy system informacyjny

Glosariusz

Funkcjonariusz straży granicznej – każdy funkcjonariusz publiczny wyznaczony zgodnie z prawem krajowym do pełnienia obowiązków służbowych na przejściu granicznym lub na odcinku granicy, lub w bezpośrednim sąsiedztwie tej granicy, który realizuje zadania w zakresie kontroli granicznej.

Interoperacyjność – terminu tego używa się powszechnie w odniesieniu do zdolności różnych systemów informacyjnych do komunikowania się, wymiany danych i wykorzystywania pozyskanych w ten sposób informacji.

Kontrola drugiej linii – szczegółowa odprawa, która może zostać przeprowadzona w odpowiednim miejscu, innym niż miejsce, w którym dokonywana jest odprawa wszystkich osób (pierwsza linia).

Państwa stowarzyszone w ramach strefy Schengen – cztery państwa europejskie należące do Europejskiego Stowarzyszenia Wolnego Handlu (EFTA) (Islandia, Liechtenstein, Norwegia i Szwajcaria), które nie są członkami UE, ale podpisały umowy o uczestnictwie w dorobku prawnym Schengen.

Państwa strefy Schengen – 26 państw europejskich, które zniosły kontrole paszportowe na wspólnych granicach, z których 22 to państwa członkowskie UE, a cztery to kraje EFTA: Belgia, Republika Czeska, Dania, Niemcy, Estonia, Grecja, Hiszpania, Francja, Włochy, Łotwa, Litwa, Luksemburg, Węgry, Malta, Niderlandy, Austria, Polska, Portugalia, Słowenia, Słowacja, Finlandia, Szwecja, Islandia, Liechtenstein, Norwegia, Szwajcaria.

Pierwsza linia – miejsce, w którym wszystkie osoby przekraczające granicę są poddawane kontroli na przejściu granicznym.

Przejście graniczne – każde przejście graniczne wyznaczone przez właściwe organy do celów przekraczania granic zewnętrznych.

ODPOWIEDZI KOMISJI NA SPRAWOZDANIE SPECJALNE EUROPEJSKIEGO TRYBUNAŁU OBRACHUNKOWEGO

„UNIJNE SYSTEMY INFORMACYJNE WSPIERAJĄCE KONTROLE GRANICZNE – NARZĘDZIE EFEKTYWNE, LECZ WYMAGAJĄCE BARDZIEJ AKTUALNYCH I KOMPLETNYCH DANYCH”

STRESZCZENIE

II Należy podkreślić, że dane dotyczące przelotu pasażera (PNR) gromadzone na podstawie dyrektywy w sprawie danych PNR można wykorzystywać jedynie do celów ścigania przestępstw w ramach zwalczania poważnej przestępczości i terroryzmu, a nie do celów kontroli granicznej/imigracyjnej.

VI Termin transpozycji dyrektywy w sprawie danych PNR upłynął z dniem 25 maja 2018 r. Jest to zatem stosunkowo nowy instrument w porównaniu z innymi systemami objętymi kontrolą Trybunału Obrachunkowego.

Państwa członkowskie mają obowiązek wyposażyć jednostki do spraw informacji o pasażerach w sprzęt i oprogramowanie pozwalające na gromadzenie i przetwarzanie danych PNR. Zapewnienie łączności z przewoźnikiem lotniczym to długi i skomplikowany proces, który nie zależy wyłącznie od organów krajowych. Ponadto nie można zbierać ani przetwarzać danych PNR, jeżeli nie istnieje podstawa prawna (tj. przed przyjęciem i wejściem w życie krajowych środków wykonawczych). Wszystkie te czynniki stanowią powód, dla którego może minąć trochę czasu, zanim jednostki do spraw informacji o pasażerach osiągną pełną operacyjność. Komisja udziela pomocy państwom członkowskim w procesie wdrażania, w tym udostępniając finansowanie UE na zakup i rozwój niezbędnego sprzętu i oprogramowania.

Komisja nie uważa, że przy wdrażaniu rozwiązań informatycznych na potrzeby Eurosur wystąpiły duże opóźnienia.

Sieć komunikacyjna Eurosur – zapewniająca łączność między krajowymi ośrodkami koordynacji ochrony granic państw członkowskich oraz między tymi ośrodkami a Europejską Agencją Straży Granicznej i Przybrzeżnej (Frontex) – została ustanowiona w wyznaczonym terminie, co umożliwiło na przykład wymianę informacji na temat zdarzeń związanych z migracją nieuregulowaną i przestępczością transgraniczną.

Doszło jednak faktycznie do opóźnienia w ukończeniu procesu akredytacji w odniesieniu do wymiany niektórych informacji w związku z wymogami dotyczącymi poufności.

VII Komisja zgadza się z Trybunałem Obrachunkowym, że konkretne i wiążące terminy wdrożenia zaleceń przez dane państwa członkowskie znacznie zwiększyłyby skuteczność mechanizmu oceny Schengen i przyczyniłyby się do szybszego wyeliminowania zidentyfikowanych luk.

Jeżeli chodzi o termin przyjmowania sprawozdań z oceny, Komisja analizuje możliwe zmiany proceduralne, które skróciłyby ten okres.

VIII Mając na uwadze nieustannie rosnący przepływ pasażerów, należy inwestować w rozwiązania umożliwiające systematyczne sprawdzanie wszystkich pasażerów we wszystkich stosownych systemach niezależnie od sytuacji lub liczby oczekujących pasażerów.

IX Jeżeli chodzi o uprawnienia Komisji w zakresie egzekwowania prawa, Komisja odpowiada za monitorowanie prawidłowego wdrożenia przepisów UE przez państwa członkowskie. W związku z tym – mimo że Komisja nie ma dostępu do danych SIS i nie może przeprowadzać oceny w poszczególnych przypadkach – może jednak sprawdzić, czy na szczeblu krajowym istnieją struktury i mechanizmy zapewniające wysoką jakość danych wprowadzanych do SIS.

X Jeżeli chodzi o dane w systemie SIS, aby stworzyć wpis, należy wprowadzić uzgodniony zestaw obowiązkowych danych (a zatem wpis w systemie SIS zawsze zawiera kompletne dane), SIS zawiera jednak również dane wprowadzane tylko wówczas, gdy są dostępne lub gdy organy wydające uznają ich uwzględnienie za bezpieczne. Dodatkowe informacje mogą być również dostępne w biurze SIRENE. Wpis zawsze zawiera informacje dla użytkowników końcowych o możliwości skontaktowania się z krajowym biurem SIRENE (w niektórych przypadkach bezpośrednio).

Jeżeli chodzi o system VIS i fałszywe trafienia, system VIS co do zasady zawiera dane biometryczne (10 dobrej jakości odcisków palców), w związku z czym – pod warunkiem prawidłowego przeprowadzania kontroli (odcisków palców danej osoby fizycznej) – oznacza to, że w przypadku systemu VIS nie zachodzi możliwość uzyskania fałszywych trafień. Co więcej, z ustaleń REFIT z 2016 r. dotyczącego VIS wynika, że jakość danych, w tym danych biometrycznych, w systemie VIS jest bardzo dobra.

XI W sprawozdaniu Komisji z oceny Eurosur z 2018 r. zwrócono również uwagę na różne harmonogramy wprowadzania informacji przez państwa członkowskie do Eurosur. Problem ten rozwiązano w nowym rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej (którego zakres zastosowania obecnie obejmuje również Eurosur) umożliwiającym uzgodnienie w przyszłości wiążących przepisów wykonawczych w sprawie wymiany informacji w ramach Eurosur.

XII Komisja przyjmuje te zalecenia.

WSTEP

03 W dyrektywie (UE) 2016/681 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, zwanej dyrektywą w sprawie danych PNR, nie wprowadza się scentralizowanego systemu informatycznego na szczeblu UE. Każde państwo członkowskie posiada własną jednostkę do spraw informacji o pasażerach (PIU), która zbiera, przetwarza i przechowuje dane PNR. Krajowe jednostki do spraw informacji o pasażerach państw członkowskich mogą przekazywać dane PNR tego typu jednostkom innych państw członkowskich lub zwracać się do takich jednostek innych państw członkowskich z wnioskiem o przekazanie danych PNR zgodnie z procedurą określoną w art. 9 dyrektywy w sprawie danych PNR.

W porównaniu z SIS, VIS lub PNR Eurosur nie stanowi szczególnego systemu informacyjnego, tylko „wspólne ramy wymiany informacji i współpracy między państwami członkowskimi” a Europejską Agencją Straży Granicznej i Przybrzeżnej (Frontex). Dane w systemie Eurosur mogą być zbierane za pomocą różnych systemów informacyjnych.

UWAGI

20 Za komponenty krajowe systemów SIS II i VIS odpowiadają państwa członkowskie.

24 System Eurosur, który stanowi ramy dotyczące nie tylko wymiany informacji, ale również współpracy, składa się z różnych komponentów. Sieć komunikacyjna Eurosur została ustanowiona w wyznaczonym terminie, zapewniając łączność między wszystkimi uczestniczącymi państwami członkowskimi na przełomie lat 2013/2014 oraz między nimi a Europejską Agencją Straży Granicznej i Przybrzeżnej (Frontex). Doszło jednak do opóźnień w ukończeniu procesu akredytacji sieci komunikacyjnej Eurosur w zakresie wymiany informacji niejawnych.

27 Akredytacja bezpieczeństwa w zakresie wymiany informacji niejawnych w sieci komunikacyjnej Eurosur była opóźniona, należy jednak zauważyć, że tego typu informacje stanowią jedynie bardzo małą część wymienianych informacji.

28 Komisja udziela stałego wsparcia państwom członkowskim w procesie wdrażania i stosowania systemu, zapewniając finansowanie, pomoc, organizując regularne spotkania i warsztaty ułatwiające partnerską wymianę informacji oraz zapewniając szkolenia (głównie za pośrednictwem CEPOL).

29 W międzyczasie Niemcy i Finlandia zgłosiły pełną transpozycję dyrektywy w sprawie danych PNR (Finlandia w dniu 25 czerwca 2019 r., a Niemcy w dniu 8 lipca 2019 r.).

30 Ustanowienie łączności z liniami lotniczymi to skomplikowany technicznie i długotrwały proces, który w przypadku poszczególnych linii lotniczych może potrwać 6–9 miesięcy. W procesie tym uczestniczą przedsiębiorstwa świadczące usługi w zakresie rezerwacji na rzecz linii lotniczych. Od momentu przyjęcia dyrektywy w sprawie danych PNR znacząco wzrosła liczba żądań zapewnienia łączności między przewoźnikami lotniczymi a jednostkami do spraw informacji o pasażerach.

Należy również zauważyć, że od marca 2019 r. wiele państw członkowskich poczyniło znaczne postępy w zakresie procesu zapewnienia łączności.

31 System ten jest stosunkowo nowy i nadal znajduje się na etapie wdrażania.

Dane PNR są nie tylko poddawane kontroli krzyżowej obejmującej porównanie z informacjami w bazach danych, ale także przez porównanie z ustalonymi wcześniej zasadami namierzania służącymi identyfikacji pasażerów, którzy odpowiadają określonym profilom, na podstawie dostępnych danych wywiadowczych.

Technika ta umożliwia identyfikację osób fizycznych nieznanym władzom, które biorą udział w nielegalnej działalności, m.in. terroryzmie lub przemyśle.

32 Dane PNR można wykorzystywać wyłącznie do celów zwalczania terroryzmu i poważnej przestępczości, jak określono w dyrektywie w sprawie danych PNR. Zakres stosowania przepisów dotyczących SIS jest szerszy (np. możliwe jest wprowadzanie wpisów

w przypadkach przestępstw nieobjętych zakresem stosowania dyrektywy w sprawie danych PNR).

Dane PNR to dane przekazywane przez pasażerów podczas rezerwacji lotów. W przypadku lotów wewnątrzunijnych dane te nie obejmują danych API (tj. danych zawartych w urzędowych dokumentach tożsamości, m.in. daty urodzenia, która stanowi element danych niezbędny przy identyfikacji osób fizycznych). W związku z tym z punktu widzenia egzekwowania prawa dane PNR są zarówno niesprawdzone, jak i niekompletne.

Przewoźnicy lotniczy przekazują dane wszystkich pasażerów. Porównanie tych danych z informacjami zawartymi w bazach danych i z zasadami namierzania umożliwia identyfikację znanych lub nieznanym osób podejrzanych.

SIS II to jedna z baz danych wykorzystywanych przez organy krajowe przy przetwarzaniu danych PNR.

40 Oprócz regularnych wizyt każdego roku przeprowadzanych jest również szereg niezapowiedzianych ocen. Takie wizyty mogą obejmować ocenę wdrożenia wcześniejszych zaleceń. Przeprowadzono jedną niezapowiedzianą wizytę i cztery kolejne wizyty dotyczące SIS II.

41 Celem kolejnej wizyty organizowanej przez Komisję jest ocena wdrożenia wcześniejszych zaleceń.

Ramka 2 – Jak zidentyfikować osobę, która ma zostać zatrzymana?

Należy zauważyć, że w dane w SIS pokrywają się w przypadku wyszukania wpisu wydanego przez inne państwo członkowskie (w wyniku automatycznego wyszukiwania). Wykaz potencjalnych „pokrywających się danych” zostaje wyświetlony użytkownikowi końcowemu (na przykład funkcjonariuszowi straży granicznej), który musi sprawdzić takie dane. Takie sprawdzenie zawsze odbywa się ręcznie zgodnie z wymogami unijnych przepisów o ochronie danych osobowych. Dopiero po ręcznym sprawdzeniu takie pokrywające się dane zostają potwierdzone i możemy mówić o trafieniu.

58 Kwestią tą zajęto się w nowym rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej, które wejdzie w życie jeszcze w tym roku i uchyli obecnie obowiązujące rozporządzenie w sprawie Eurosur.

W szczególności Europejska Agencja Straży Granicznej i Przybrzeżnej będzie monitorować dane podlegające wymianie i informować wszystkie państwa członkowskie w czasie rzeczywistym o sytuacji w zakresie zgłaszania.

Składanie sprawozdań dotyczących przejść granicznych będzie obowiązkowe.

61 Wykorzystywanie systemu VIS do kontroli posiadaczy wiz na granicy stanowi obowiązek wynikający z kodeksu granicznego Schengen. Tę ewentualną rozbieżność można by przeanalizować z wykorzystaniem mechanizmu oceny Schengen, aby zapewnić systematyczne kontrole wizowe przy użyciu systemu VIS.

68 Są to potencjalne problemy wymagające przeprowadzenia kontroli krzyżowej przez odpowiedzialny organ, a nie potwierdzone błędy w zakresie jakości danych. Ponadto należy zauważyć, że liczba ta obejmuje również wszystkie wpisy, które już zostały zweryfikowane

przez państwa członkowskie i wobec których nie stwierdzono problemu w zakresie jakości danych. Takie zweryfikowane wpisy nie są usuwane ze szczegółowego sprawozdania, w którym widnieją tak długo, jak istnieją.

71 Przepisy dotyczące SIS określają zbiór danych, które mogą widnieć we wpisie (wspólny art. 20 decyzji w sprawie systemu SIS II i rozporządzenia w sprawie systemu SIS II). Minimalizacja danych stanowi istotną zasadę ochrony danych osobowych. W przepisach tych określono również minimalny zbiór danych, bez których żaden wpis nie może powstać. Każdy wpis zawierający takie minimalne elementy danych jest kompletny. Inne (opcjonalne) elementy danych należy wprowadzić, jeżeli są dostępne. W przypadku niewprowadzenia takich opcjonalnych danych Komisji pozostaje jedynie założenie, że organ wydający nie dysponował takimi danymi.

72 Obowiązek przeprowadzenia weryfikacji ręcznej stanowi wymóg określony w unijnych przepisach o ochronie danych (ogólne rozporządzenie o ochronie danych (rozporządzenie (UE) 2016/679) i dyrektywa o ochronie danych w związku ze współpracą policyjną (dyrektywa (UE) 2016/680)). Ponadto jest to wymóg określony w dyrektywie w sprawie danych PNR.

Większość danych PNR jest niewystarczająca, nieistotna, a czasem za mało wiarygodna na potrzeby kontroli w systemie SIS, na przykład dane PNR nieobejmujące wartości API można porównać jedynie z bardzo ograniczonym zbiorem danych SIS. Problemy związane z wiarygodnością danych PNR wynikają również z faktu, że dane te są przekazywane za pomocą oświadczeń własnych.

74 Trybunał Obrachunkowy słusznie zauważył, że wniosek Komisji dotyczący zmiany ram prawnych VISA (COM(2018) 302), nad którym obecnie debatują współprawodawcy, przewiduje włączenie do VIS wiz krajowych i dokumentów pobytowych. Wyeliminowałoby to lukę informacyjną, o której mówi Trybunał Obrachunkowy. O ile faktycznie włączono by jedynie nowo wydane dokumenty pobytowe długoterminowe, z czasem problem ten zniknie, gdyż dokumenty pobytowe długoterminowe mają ograniczony okres ważności, po upływie którego wymagają przedłużenia/zastąpienia.

75 Kwestię przekazywania przez państwa członkowskie sprawozdań w różnych formatach rozwiązano w nowym rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej, które ma wejść w życie do końca 2019 r. i uchyli obecnie obowiązujące rozporządzenie w sprawie Eurosur.

Sprawozdania przekazywane w ramach systemu Eurosur zostaną znormalizowane w drodze aktu wykonawczego.

76 Zob. odpowiedź Komisji do pkt 75.

Ponadto Komisja będzie wspierać rozwój bramy automatycznej wymiany informacji w celu ograniczenia dublowania wprowadzanych danych.

79 Kwestię terminu na przekazanie informacji przez państwa członkowskie w ramach Eurosur rozwiązano w nowym rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej, które ma wejść w życie do końca 2019 r. i uchyli obecnie obowiązujące rozporządzenie w sprawie Eurosur.

Kwestia terminu na przekazywanie informacji w systemie Eurosur oraz poziomu odpowiedzialności w zakresie zgłaszania zostanie rozwiązana w drodze aktu wykonawczego.

WNIOSKI I ZALECENIA

84 Za komponenty krajowe systemów SIS II i VIS odpowiadają państwa członkowskie.

85 Komisja, państwa członkowskie, CEPOL i eu-LISA zapewniają regularne wspólne szkolenia funkcjonariuszy biura SIRENE z zakresu SIS II / SIRENE. Przeprowadzono również analizę potrzeb szkoleniowych.

Państwa członkowskie coraz częściej rozważają inwestycje w zintegrowane/internetowe praktyczne kursy szkoleniowe.

Zmienione przepisy ustanawiające stosowne systemy informatyczne (np. SIS II) umożliwią Europejskiej Agencji Straży Granicznej i Przybrzeżnej (Frontex) opracowanie szczególnych interfejsów odpowiednich do wykorzystania przez zaproszonych funkcjonariuszy rozmieszczonych w dowolnych państwach członkowskich.

Zalecenie 1 – Propagowanie wykorzystania kursów szkoleniowych w zakresie systemów SIS II i VIS

Komisja przyjmuje zalecenie 1.

86 Jeżeli chodzi o Eurosur, należy zauważyć, że jedynie część informacji podlegających wymianie jest obowiązkowa. Przykładowo państwa członkowskie nieposiadające zewnętrznych granic lądowych ani morskich mogą prowadzić wymianę informacji na temat granic powietrznych, ale nie mają takiego obowiązku. Dzięki nowemu rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej w systemie Eurosur uwzględniono jednak również (jako element obowiązkowy) odprawy graniczne i ochronę granicy powietrznej, co oznacza, że w przyszłości niemal wszystkie państwa członkowskie będą aktywnie przekazywać informacje do systemu Eurosur.

Zob. odpowiedzi Komisji do pkt 24–32.

Zalecenie 2 – Szybsze eliminowanie uchybień stwierdzonych w trakcie ocen Schengen

Komisja przyjmuje zalecenie 2.

Zalecenie 3 – Zbadanie przyczyn rozbieżności w przypadku kontroli wizowych

Komisja przyjmuje zalecenie 3.

Zalecenie 4 – Udoskonalenie procedur kontroli jakości danych

Komisja przyjmuje zalecenie 4.

Komisja i eu-LISA obecnie pracują już nad udoskonaleniem tego mechanizmu. Kwestia ta jest regularnie podejmowana na posiedzeniach Komitetu SIS–VIS.

95 Kwestię terminu na przekazanie informacji rozwiązano w nowym rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej, które ma wejść w życie do końca

2019 r. i uchyli obecnie obowiązujące rozporządzenie w sprawie Eurosur. Kwestia terminu na przekazywanie informacji w systemie Eurosur oraz poziomu odpowiedzialności w zakresie zgłaszania zostanie rozwiązana w drodze aktu wykonawczego.

Zalecenie 5 – Zmniejszenie opóźnień we wprowadzaniu danych

Komisja przyjmuje zalecenie 5 lit. a).

Komisja przyjmuje zalecenie 5 lit. b).

Komisja zgadza się z częścią dotyczącą Eurosur. Kwestię terminów na wprowadzanie danych rozwiązano w nowym rozporządzeniu w sprawie Europejskiej Straży Granicznej i Przybrzeżnej, które ma wejść w życie do końca 2019 r. oraz które uchyli obecnie obowiązujące rozporządzenie w sprawie Eurosur i umożliwi uzgodnienie w przyszłości wiążących przepisów wykonawczych w sprawie wymiany informacji w ramach Eurosur.

Zespół kontrolny

Sprawozdania specjalne Trybunału przedstawiają wyniki kontroli dotyczących wybranych obszarów polityki i programów unijnych bądź kwestii związanych z zarządzaniem w wybranych obszarach budżetowych. Trybunał wybiera i opracowuje zadania kontrolne w taki sposób, aby miały one jak największe oddziaływanie, biorąc pod uwagę kryteria takie jak zagrożenia dla wykonania zadań lub zgodności, poziom dochodów lub wydatków w danym obszarze, nadchodzące zmiany oraz interes polityczny i społeczny.

Niniejsza kontrola wykonania zadań została przeprowadzona przez Izbę III, zajmującą się obszarami wydatków dotyczącymi działań zewnętrznych, bezpieczeństwa i sprawiedliwości. Izbie tej przewodniczy członek Trybunału Bettina Jakobsen. W działania kontrolne zaangażowani byli ponadto: Katja Mattfolk, szefowa gabinetu; Kim Storup, attaché; Alejandro Ballester Gallardo, kierownik, a także kontrolerzy: Piotr Senator, Alexandre Tan i Mirko Iaconisi. Wsparcie językowe zapewnił Michael Pyper.



Od lewej: Mirko Iaconisi, Piotr Senator, Michael Pyper, Bettina Jakobsen, Alejandro Ballester Gallardo, Katja Mattfolk.

Kalendarium

Wydarzenie	Data
Zatwierdzenie ramowego programu kontroli / rozpoczęcie kontroli	17.4.2018
Oficjalne przesłanie wstępnej wersji sprawozdania Komisji (lub innej jednostce kontrolowanej)	11.7.2019
Przyjęcie ostatecznej wersji sprawozdania po postępowaniu kontradiktoryjnym	8.10.2019
Otrzymanie oficjalnych odpowiedzi Komisji (lub innej jednostki kontrolowanej) we wszystkich językach	31.10.2019

© Unia Europejska, 2019.

Powielanie materiałów dozwolone pod warunkiem podania źródła.

W celu wykorzystania lub powielenia zdjęć lub innych materiałów nieobjętych prawem autorskim Unii Europejskiej należy wystąpić o zgodę bezpośrednio do właścicieli praw autorskich.

PL	PDF	ISBN 978-92-847-3866-3	doi:10.2865/23405	QJ-AB-19-020-PL-N
PL	HTML	ISBN 978-92-847-3815-1	doi:10.2865/840819	QJ-AB-19-020-PL-Q

Zniesienie kontroli granicznych na granicach wewnętrznych strefy Schengen spowodowało, że większe znaczenie mają obecnie skuteczna kontrola i nadzorowanie granic zewnętrznych tej strefy. Aby wspomóc funkcjonariuszy straży granicznej w ich kontrolowaniu, UE ustanowiła szereg systemów informacyjnych. W ramach kontroli Trybunał przeanalizował, czy główne unijne systemy informacyjne w zakresie bezpieczeństwa wewnętrznego efektywnie wspierają kontrole graniczne. Na podstawie tej analizy stwierdził, że funkcjonariusze straży granicznej w coraz większym stopniu korzystają z tych systemów i polegają na nich przy dokonywaniu odpraw granicznych. W systemach brakuje jednak obecnie pewnych danych, a inne dane są niekompletne bądź nie są wprowadzane w przewidzianych na to terminach, co negatywnie wpływa na efektywność niektórych odpraw granicznych. Trybunał przedstawił szereg zaleceń dotyczących m.in. udoskonalenia procedur kontroli jakości danych, ograniczenia opóźnień we wprowadzaniu danych oraz skrócenia czasu potrzebnego na skorygowanie stwierdzonych uchybień.

Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego przedstawiono na mocy art. 287 ust. 4 akapit drugi TFUE.



EUROPEJSKI
TRYBUNAŁ
OBRACHUNKOWY



Urząd Publikacji

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
12 rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel.: +352 4398-1

Formularz kontaktowy: eca.europa.eu/pl/Pages/ContactForm.aspx

Strona internetowa: eca.europa.eu

Twitter: @EUAuditors