KOMISJA
EUROPEJSKA

Bruksela, dnia 6.4.2016 r.
COM(2016) 205 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa

1. WPROWADZENIE

Europa jest mobilnym społeczeństwem. Wewnętrzne i zewnętrzne granice przekraczają codziennie miliony obywateli UE i obywateli państw trzecich. W 2015 r. Unię odwiedziło ponad 50 mln obywateli państw spoza UE, którzy w sumie ponad 200 mln razy przekroczyli granice zewnętrzne strefy Schengen.

Oprócz tego legalnego ruchu turystycznego w samym 2015 r., w następstwie konfliktu w Syrii i sytuacji kryzysowych w innych miejscach na świecie, na granicach zewnętrznych Europy odnotowano 1,8 mln przypadków nielegalnego wjazdu. Obywatele UE oczekują, aby kontrole osób na granicach zewnętrznych były skuteczne, umożliwiały skuteczne zarządzanie migracjami oraz zwiększały bezpieczeństwo wewnętrzne. Ataki terrorystyczne w Paryżu w 2015 r. i w Brukseli w marcu 2016 r. pokazały gorzką prawdę: bezpieczeństwo wewnętrzne Europy jest cały czas zagrożone.

Obie wspomniane kwestie uwydatniły potrzebę połączenia naszych wysiłków i udoskonalenia ram współpracy w zakresie zarządzania granicami UE, migracji i bezpieczeństwa oraz narzędzi informacyjnych. Zarządzanie granicami, egzekwowanie prawa i kontrola migracji są ze sobą dynamicznie powiązane. Znane są przypadki, że obywatele UE przekroczyli granicę zewnętrzną, aby przedostać się do stref konfliktu w celach terrorystycznych, i po powrocie takie osoby stanowią zagrożenie. Istnieją dowody na to, że terroryści skorzystali ze szklaków nielegalnej migracji, aby dotrzeć do UE, i następnie niepostrzeżenie poruszali się po strefie Schengen.

W ramach Europejskiej agendy bezpieczeństwa i Europejskiego programu w zakresie migracji określono kierunek rozwoju i wdrożenia unijnej polityki ukierunkowanej na podjęcie równolegle występujących wyzwań związanych z zarządzaniem migracjami oraz z walką z terroryzmem i przestępczością zorganizowaną. Niniejszy komunikat opiera się na efektach synergii między tymi dwoma programami i ma stanowić punkt wyjścia do dyskusji na temat tego, w jaki sposób istniejące i przyszłe systemy informacyjne mogą przyczynić się do poprawy zarówno zarządzania granicami zewnętrznymi, jak i bezpieczeństwa wewnętrznego w UE. Uzupełnia on wniosek z grudnia 2015 r. dotyczący utworzenia Europejskiej Straży Granicznej i Przybrzeżnej oraz poprawy zapobiegania sytuacjom kryzysowym i interwencji na granicach zewnętrznych.

Na szczeblu UE funkcjonuje szereg systemów informacyjnych, które zapewniają funkcjonariuszom straży granicznej i funkcjonariuszom policji dostęp do istotnych informacji na temat osób, lecz unijna architektura zarządzania danymi nie jest doskonała. W niniejszym komunikacie przedstawiono kilka możliwości maksymalizacji korzyści płynących z istniejących systemów informacyjnych oraz, w razie potrzeby, zaplanowania nowych i uzupełniających działań mających na celu likwidację luk. Podkreślono również potrzebę zwiększenia interoperacyjności systemów informacyjnych (cel długoterminowy), na co zwróciły również uwagę Rada Europejska i Rada UE[1], oraz przedstawiono propozycje rozwoju systemów informacyjnych w przyszłości w celu zapewnienia funkcjonariuszom straży granicznej, organom celnym, funkcjonariuszom policji i organom wymiaru sprawiedliwości dostępu do niezbędnych informacji.

[1] Konkluzje z posiedzenia Rady Europejskiej w dniach 17-18 grudnia 2015 r.; wspólne oświadczenie unijnych ministrów sprawiedliwości i spraw wewnętrznych oraz przedstawicieli instytucji UE w sprawie zamachów terrorystycznych, do których doszło w Brukseli 22 marca 2016 r. (24 marca 2016 r.); konkluzje Rady UE i państw członkowskich zebranych w Radzie w sprawie zwalczania terroryzmu (20 listopada 2015 r.).

Każda przyszła inicjatywa zostanie przygotowana na podstawie zasad lepszego stanowienia prawa, a towarzyszyć jej będą konsultacje społeczne i ocena skutków, z uwzględnieniem praw podstawowych oraz w szczególności prawa do ochrony danych osobowych.

2. WYZWANIA, KTÓRYM NALEŻY SPROSTAĆ

Ze względu na brak granic wewnętrznych w strefie Schengen konieczne jest solidne i niezawodne zarządzanie przepływem osób przez granice zewnętrzne. Jest to niezbędny warunek, aby zapewnić wysoki poziom bezpieczeństwa wewnętrznego oraz swobodny przepływ osób w granicach tego obszaru. Jednocześnie brak granic wewnętrznych oznacza, że organy ścigania w państwach członkowskich również mają dostęp do istotnych informacji na temat osób. Na szczeblu UE funkcjonuje szereg systemów informacyjnych i baz danych, które zapewniają funkcjonariuszom straży granicznej, funkcjonariuszom policji i innym organom dostęp do istotnych informacji na temat osób odpowiednio do wykonywanych przez nich zadań[2].

Jednak systemy informacyjne wykazują również niedociągnięcia, które utrudniają pracę wspomnianych organów krajowych. Dlatego w Europejskiej agendzie bezpieczeństwa podkreślono, że poprawa wymiany informacji stanowi kluczowy priorytet. Do głównych niedociągnięć zalicza się: a) niedostateczną funkcjonalność istniejących systemów informacyjnych, b) luki w unijnej architekturze zarządzania danymi, c) wielorakość systemów informacyjnych regulowanych w różny sposób oraz d) rozdrobnioną architekturę zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa.

Istniejące w UE systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa wewnętrznego obejmują szeroki zakres funkcji. Jednak **funkcjonalność istniejących systemów jest cały czas niewystarczająca**. Jeśli przyjrzymy się procesom kontroli granic w odniesieniu do różnych kategorii podróżnych, okaże się, że braki występują nie tylko w niektórych z tych procesów, lecz także między systemami informacyjnymi wykorzystywanymi do celów kontrolowania granic. Należy również zoptymalizować funkcjonowanie istniejących narzędzi służących do egzekwowania prawa. W związku z tym należy zastanowić się nad działaniami mającymi na celu udoskonalenie istniejących systemów informacyjnych (sekcja 5).

Oprócz tego występują **luki w unijnej architekturze zarządzania danymi**. W dalszym ciągu problemy stwarzają kontrole graniczne określonych kategorii podróżnych takich jak obywatele państw trzecich posiadający wizę długoterminową. Ponadto występuje luka informacyjna przed przybyciem na granice obywateli państw trzecich, którzy są zwolnieni z obowiązku wizowego. Należy zastanowić się nad tym, czy istnieje potrzeba wyeliminowania tych luk przez opracowanie dodatkowych systemów informacyjnych tam, gdzie jest to konieczne (sekcja 6).

Funkcjonariusze straży granicznej i zwłaszcza funkcjonariusze policji muszą sobie radzić z **wielorakością systemów informacyjnych regulowanych w różny sposób** na szczeblu UE. Taki złożony charakter stwarza praktyczne problemy, w szczególności w kontekście wyboru odpowiednich baz danych w konkretnej sytuacji. Co więcej, nie wszystkie państwa członkowskie mają dostęp do wszystkich istniejących systemów[3]. Obecną

[2] W sekcji 4 znajduje się przegląd systemów informacyjnych do celów zarządzania granicami i zapewnienia bezpieczeństwa; w załączniku 2 znajduje się bardziej szczegółowy wykaz.

[3] Zgodnie ze szczegółowymi warunkami protokołu nr 22 (w odniesieniu do Danii) oraz protokołów nr 21 i 36 (w odniesieniu do Wielkiej Brytanii i Irlandii), a także z odnośnymi aktami przystąpienia.

złożoność dostępu do systemów informacyjnych na szczeblu UE można by zmniejszyć przez ustanowienie pojedynczego interfejsu wyszukiwania na poziomie krajowym, który uwzględniałby różne cele dostępu (sekcja 7.1).

Obecna unijna architektura zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa charakteryzuje się **rozdrobnieniem**. Wynika to z różnych kontekstów instytucjonalnych, prawnych i politycznych, w których systemy te zostały opracowane. Informacje są przechowywane oddzielnie w różnych systemach, które rzadko są ze sobą połączone. Bazy danych są niespójne, a stosowane zasady dostępu właściwych organów do zawartych w nich danych są rozbieżne. W związku z tym organy ścigania mogą napotkać problem „martwych stref", ponieważ może być bardzo trudno określić powiązania między fragmentami danych. Dlatego tak ważnym i pilnym zadaniem jest wypracowanie wspólnych rozwiązań w zakresie poprawy dostępu do danych do celów zarządzania granicami i zapewnienia bezpieczeństwa, przy pełnym poszanowaniu praw podstawowych. W tym celu należy zapoczątkować proces zwiększania interoperacyjności istniejących systemów informacyjnych (sekcja 7).

3. PRAWA PODSTAWOWE

Do sprostania każdemu z wyżej opisanych wyzwań konieczne jest pełne poszanowanie praw podstawowych oraz przepisów o ochronie danych.

Przestrzeganie praw podstawowych wymaga odpowiednio zaprojektowanych i prawidłowo wykorzystywanych rozwiązań technologicznych i systemów informacyjnych. Technologia i systemy informacyjne mogą pomóc władzom publicznym w zapewnieniu ochrony praw podstawowych przysługujących obywatelom. Technologia biometryczna może zmniejszyć ryzyko błędnego stwierdzenia tożsamości, a także ryzyko dyskryminacji i profilowania rasowego. Oprócz tego może przyczynić się do eliminowania zagrożeń związanych z bezpieczeństwem dzieci, takich jak ryzyko ich zaginięcia lub ryzyko, że padną ofiarami handlu ludźmi, pod warunkiem że technologii tej towarzyszyć będą gwarancje poszanowania praw podstawowych i środki ochronne. Może też zmniejszyć ryzyko bezpodstawnego zatrzymywania i aresztowania. Ponadto może przyczynić się do zwiększenia bezpieczeństwa obywateli przebywających w strefie Schengen, pomagając w walce z terroryzmem i poważną przestępczością.

Istnienie wielkoskalowych systemów informacyjnych wiąże się również z potencjalnymi zagrożeniami dla prywatności, które należy przewidzieć i którymi należy się odpowiednio zająć. Gromadzenie i wykorzystywanie danych osobowych w tych systemach wpływa na prawo do prywatności i ochrony danych osobowych zapisane w Karcie praw podstawowych Unii Europejskiej. Wszystkie systemy muszą być zgodne z zasadami ochrony danych oraz z wymogami konieczności, proporcjonalności, celowości i jakości danych. Wymagane są również zabezpieczenia, które zapewnią osobom, których dane dotyczą, prawa w zakresie ochrony ich życia prywatnego i danych osobowych. Dane powinno się zatrzymywać jedynie tak długo, jak jest to konieczne dla celów, dla których zostały zgromadzone. Należy przewidzieć mechanizmy zapewniające właściwe zarządzanie ryzykiem oraz skuteczną ochronę praw osób, których dane dotyczą.

W grudniu 2015 r. współustawodawcy osiągnęli porozumienie polityczne w sprawie reformy ochrony danych. Nowe ogólne rozporządzenie o ochronie danych oraz nowa dyrektywa o ochronie danych na potrzeby policji i organów wymiaru sprawiedliwości w

sprawach karnych[4] wejdą w życie w 2018 r. i będą stanowić zharmonizowane ramy przetwarzania danych osobowych.

Zasada celowości jest jedną z najważniejszych zasad ochrony danych zapisanych w Karcie praw podstawowych Unii Europejskiej. Zważywszy na różne warunki instytucjonalne, prawne i polityczne, w których systemy informacyjne funkcjonujące na szczeblu UE zostały opracowane, zasada celowości została wdrożona za pomocą rozproszonej struktury zarządzania informacjami[5]. Jest to jeden z powodów, dla których unijna architektura zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa wewnętrznego charakteryzuje się obecnie rozdrobnieniem. Biorąc pod uwagę nowe kompleksowe ramy ochrony danych osobowych w UE oraz istotny postęp technologiczny i rozwój w dziedzinie bezpieczeństwa informatycznego, zasadę celowości można łatwiej wdrożyć na poziomie dostępu do przechowywanych danych i ich wykorzystywania przy zachowaniu pełnej zgodności z Kartą praw podstawowych Unii Europejskiej i najnowszym orzecznictwem Europejskiego Trybunału Sprawiedliwości. Zabezpieczenia takie jak podział danych w ramach jednego systemu i szczególne zasady dotyczące dostępu i wykorzystania w odniesieniu do poszczególnych kategorii danych i użytkowników powinny zapewnić wymaganą celowość w zintegrowanych rozwiązaniach w zakresie zarządzania danymi. Stanowi to krok w kierunku zapewnienia interoperacyjności systemów informacyjnych w powiązaniu z niezbędnymi surowymi zasadami dostępu do danych i ich wykorzystywania, pozostającymi bez wpływu na obowiązującą zasadę celowości.

„Uwzględnienie ochrony danych już w fazie projektowania" i „domyślna ochrona danych" to zasady, które są obecnie zapisane w unijnych przepisach o ochronie danych. Przy opracowywaniu nowych instrumentów opartych na wykorzystaniu technologii informacyjnej, Komisja będzie kierować się tym podejściem. Oznacza to włączenie ochrony danych osobowych do podstawy technicznej proponowanego instrumentu, przy jednoczesnym ograniczeniu przetwarzania danych do tego, co jest niezbędne do osiągnięcia określonego celu, i udzieleniu dostępu do danych jedynie wskazanym jednostkom, zgodnie z zasadą ograniczonego dostępu[6].

Wymagania określone w Karcie praw podstawowych Unii Europejskiej i w szczególności nowe instrumenty, które mają zostać wprowadzone w ramach reformy ochrony danych, wytyczą kierunek działań, jakie Komisja będzie podejmować, aby wyeliminować obecne luki i niedociągnięcia w unijnej architekturze zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa. Dzięki temu dalszy rozwój systemów informacyjnych wykorzystywanych w tych obszarach będzie zgodny z najwyższymi standardami ochrony danych, a systemy informacyjne będą zapewniać poszanowanie praw podstawowych zagwarantowanych w Karcie praw podstawowych Unii Europejskiej i będą przyczyniały się do ich przestrzegania.

---

4 Zob. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

5 COM(2010) 385 final.

6 Pełna definicja terminu „uwzględnienie ochrony prywatności już w fazie projektowania" znajduje się w opinii Europejskiego Inspektora Ochrony Danych w sprawie promowania zaufania w społeczeństwie informacyjnym poprzez promowanie ochrony danych i prywatności, Europejski Inspektor Ochrony Danych, 18.3.2010 r.

4. PRZEGLĄD SYSTEMÓW INFORMACYJNYCH DO CELÓW ZARZĄDZANIA GRANICAMI I ZAPEWNIENIA BEZPIECZEŃSTWA[7]

Poszczególne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa wewnętrznego, które istnieją w UE, mają swoje własne cele, przeznaczenie, podstawy prawne[8], grupy użytkowników i własny kontekst instytucjonalny. Wspólnie stanowią złożoną strukturę odpowiednich baz danych.

Do trzech głównych **scentralizowanych systemów informacyjnych**, które zostały opracowane przez UE, zalicza się (i) System Informacyjny Schengen (SIS) z szerokim wachlarzem wpisów dotyczących osób i przedmiotów, (ii) wizowy system informacyjny (VIS) zawierający dane dotyczące wiz krótkoterminowych oraz (iii) system EURODAC zawierający dane o odciskach palców osób ubiegających się o azyl i obywateli państw trzecich, którzy nielegalnie przekroczyli granice zewnętrzne. Te trzy systemy wzajemnie się uzupełniają i – z wyjątkiem SIS – są ukierunkowane przede wszystkim na obywateli państw trzecich. Systemy te wspierają również organy krajowe w walce z przestępczością i terroryzmem[9]. Dotyczy to w szczególności SIS, który obecnie jest najczęściej stosowanym instrumentem wymiany informacji. Wymiana informacji pomiędzy tymi systemami odbywa się w ramach zabezpieczonej dedykowanej infrastruktury komunikacyjnej nazywanej sTESTA[10].

W uzupełnieniu opisanych istniejących systemów Komisja proponuje opracować czwarty scentralizowany system zarządzania granicami, **system wjazdu/wyjazdu** (EES)[11], którego wdrożenie jest planowane do 2020 r.; ten system również ma być ukierunkowany na obywateli państw trzecich.

---

7 Wykaz istniejących systemów informacyjnych do celów zarządzania granicami i egzekwowania prawa znajduje się w załączniku 2.

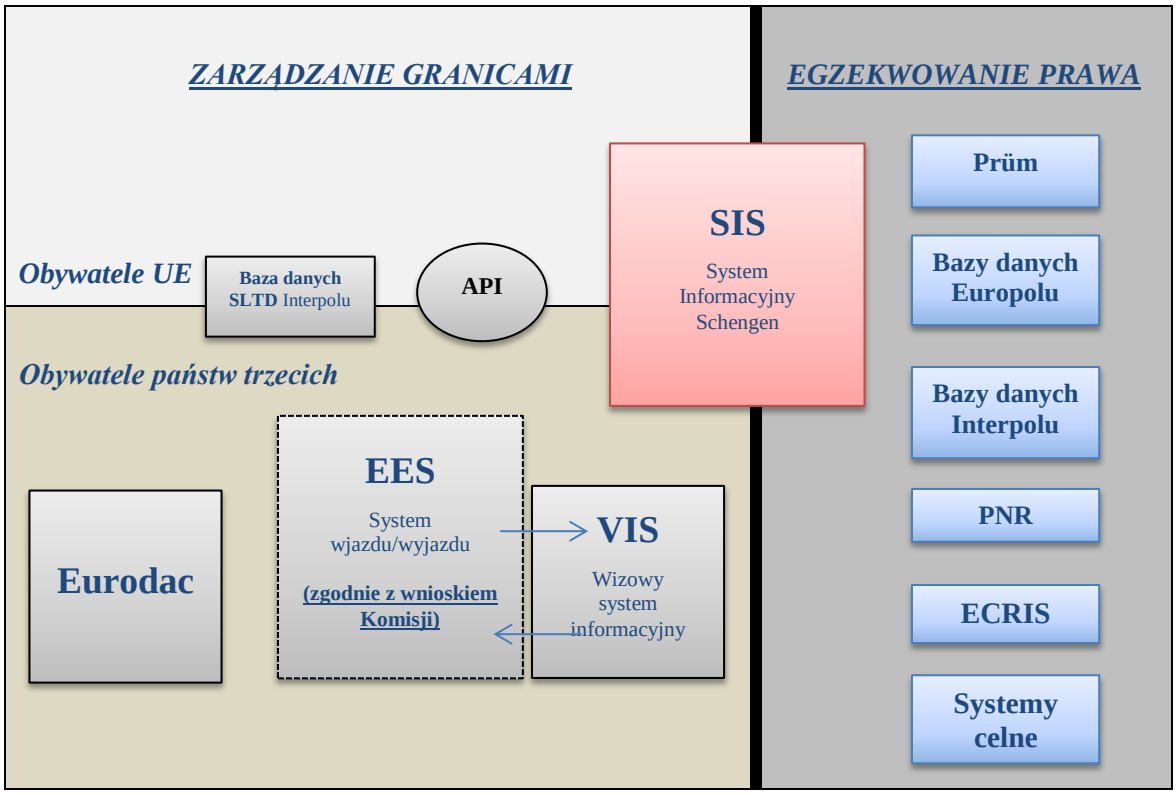
8 Zgodnie ze szczegółowymi warunkami protokołu nr 22 (w odniesieniu do Danii) oraz protokołów nr 21 i 36 (w odniesieniu do Zjednoczonego Królestwa i Irlandii).

9 Dostęp organów ścigania do systemów VIS i EURODAC jest możliwy wyłącznie w określonych warunkach ze względu na to, że egzekwowanie prawa jest dodatkowym celem tych systemów. W odniesieniu do VIS: państwa członkowskie muszą wyznaczyć organ odpowiedzialny za kontrolowanie dostępu organów ścigania do tego systemu, a policja musi przedstawić dowody na to, że dostęp do tego systemu jest jej niezbędny w celu prowadzenia dochodzeń w sprawach karnych. W odniesieniu do EURODAC: organ dochodzeniowy musi przeszukać systemy krajowe, tj. AFIS, Prüm i VIS, zanim uzyska dostęp do systemu EURODAC.

10 Wkrótce infrastruktura ta ma zostać zastąpiona przez TESTA-NG.

11 COM(2016)194 final.

Rysunek 1 *Schematyczny przegląd głównych systemów informacyjnych do celów zarządzania granicami i egzekwowania prawa*



Dodatkowymi istniejącymi instrumentami do zarządzania granicami są: baza danych Interpolu zawierająca dane skradzionych lub utraconych dokumentów podróży (SLTD) oraz baza zawierająca dane pasażera przekazywane przed podróżą (API) – w tej bazie danych gromadzone są informacje o pasażerach lotów do UE. Instrumenty te są wykorzystywane zarówno w odniesieniu do obywateli UE, jak i do obywateli państw trzecich.

Specjalnie do celów egzekwowania prawa, dochodzeń w sprawach karnych i współpracy sądowej UE opracowała **zdecentralizowane narzędzia do wymiany informacji**, a mianowicie: (i) ramy z Prüm – narzędzie umożliwiające porównywanie profili DNA, odcisków palców i danych rejestracyjnych pojazdów oraz (ii) europejski system przekazywania informacji z rejestrów karnych (ECRIS) – narzędzie umożliwiające wymianę informacji z krajowych rejestrów karnych. ECRIS umożliwia wymianę informacji na temat wcześniejszych wyroków skazujących wydanych wobec konkretnej osoby przez sądy karne w Unii Europejskiej; wymiana informacji odbywa się za pośrednictwem zabezpieczonej sieci. Wnioski o udzielenie informacji opierają się głównie na informacjach alfanumerycznych dotyczących tożsamości, chociaż wymiana danych biometrycznych jest możliwa.

Europol wspiera wymianę informacji między krajowymi organami policyjnymi jako centrum informacji o przestępstwach w UE. System informacyjny Europolu (EIS), który jest scentralizowaną bazą danych o przestępstwach, umożliwia państwom członkowskim przechowywanie i przeszukiwanie danych dotyczących poważnej przestępczości i terroryzmu. Punkty kontaktowe w Europolu dostarczają tematyczne pliki robocze do celów analizy, które zawierają informacje na temat bieżących operacji prowadzonych w państwach członkowskich. Aplikacja sieci bezpiecznej wymiany informacji Europolu (SIENA) umożliwia państwom członkowskim szybką, bezpieczną i przyjazną użytkownikom wymianę informacji między sobą, z Europolem lub z osobami trzecimi,

które zawarły porozumienia o współpracy z Europolem. Jednocześnie ważną cechą aplikacji SIENA jest jej współdziałanie z innymi systemami stosowanymi w Europolu, na przykład w celu bezpośredniej wymiany danych z punktami kontaktowymi. Umożliwia to dostarczanie do baz danych Europolu informacji wymienianych między państwami członkowskimi. W związku z tym SIENA powinna być dla państw członkowskich kanałem pierwszego wyboru, jeśli chodzi o wymianę informacji do celów egzekwowania prawa w całej UE.

Dodatkowym zestawem systemów przetwarzania danych osobowych, który zostanie opracowany w państwach członkowskich, jest system **danych dotyczących przelotu pasażera** (PNR)[12]. Dane PNR zawierają informacje o rezerwacji dostarczane w czasie rezerwacji i odprawy.

Organy celne również odgrywają ważną rolę we współpracy interdyscyplinarnej na granicach zewnętrznych. Dysponują one różnymi systemami[13] i bazami danych, które zawierają dane dotyczące przepływu towarów i identyfikacji podmiotów gospodarczych oraz informacje o zagrożeniach, które mogą być wykorzystywane do zwiększenia bezpieczeństwa wewnętrznego. Systemy te również posiadają własną kontrolowaną, ograniczoną i zabezpieczoną infrastrukturę (wspólną sieć łączności), której prawidłowe funkcjonowanie jest potwierdzone. Należy dalej analizować synergie i zbieżności między systemami informacyjnymi oraz ich odpowiednimi infrastrukturami do celów zarządzania granicami UE i operacji celnych.

5. UDOSKONALENIE ISTNIEJĄCYCH SYSTEMÓW INFORMACYJNYCH

Istniejące w UE systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa wewnętrznego obejmują szeroki zakres funkcji. Jednak cały czas występują w tych systemach **niedociągnięcia**, którymi należy się zająć, aby zoptymalizować ich działanie.

System Informacyjny Schengen (SIS)

Kontrole graniczne z wykorzystaniem **Systemu Informacyjnego Schengen** (SIS) obecnie są przeprowadzane na podstawie wyszukiwań alfanumerycznych (tj. imienia i nazwiska oraz daty urodzenia). Odciski palców można jedynie wykorzystywać do weryfikacji i potwierdzenia tożsamości osoby, która została już zidentyfikowana na podstawie swojego imienia i nazwiska. Taka luka w zakresie bezpieczeństwa pozwala osobom, które są objęte wpisem zawierającym ostrzeżenie, posługiwać się fałszywymi dokumentami, aby uniemożliwić dokładne dopasowanie w systemie SIS.

Ta istotna słaba strona zostanie wyeliminowana poprzez dodanie do SIS funkcji wyszukiwania odcisków palców w ramach **systemu automatycznej identyfikacji daktyloskopijnej (AFIS)**, jak przewidziano w istniejących ramach prawnych[14]. AFIS

[12] Zob. sekcja 6.2.

[13] Systemy informacji celnej obejmują wszystkie systemy stworzone na podstawie Wspólnotowego kodeksu celnego (rozporządzenie nr 2913/92) i przyszłego unijnego kodeksu celnego (rozporządzenie nr 952/2013) oraz decyzji w sprawie eliminowania papierowej formy dokumentów w sektorach ceł i handlu (decyzja nr 70/2008/WE), a także system informacji celnej (CIS) ustanowiony na podstawie konwencji CIS z 1995 r. Mają one stanowić pomoc w zwalczaniu przestępczości celnej przez ułatwianie współpracy między europejskimi organami celnymi.

[14] Art. 22 lit. c) rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, s. 4, oraz Dz.U. L 2015 z 7.8.2007, s. 63).

powinien zacząć działać do połowy 2017 r.[15]. Europol będzie mieć dostęp do AFIS i tym samym system ten będzie uzupełniać systemy Europolu wykorzystywane do prowadzenia dochodzeń w sprawach karnych i w ramach walki z terroryzmem, a także do porównywania odcisków palców, które odbywa się na podstawie ram z Prüm. Komisja i eu-LISA zbadają potencjał takiego szerszego wykorzystywania przyszłego systemu AFIS.

Na podstawie bieżącej oceny i analizy technicznej Komisja bada obecnie **możliwe dodatkowe funkcje SIS** w celu przedstawienia wniosków w sprawie zmiany podstawy prawnej SIS. Rozważane aspekty obejmują:

- stworzenie wpisów do SIS dotyczących migrantów o nieuregulowanym statusie podlegających decyzjom nakazującym powrót;
- wykorzystanie obrazów twarzy, oprócz odcisków palców, do identyfikacji biometrycznej;
- automatyczne przekazywanie informacji dotyczących trafienia po przeprowadzeniu kontroli;
- przechowywanie informacji dotyczących trafienia na temat wpisów do celów kontroli niejawnej i kontroli szczególnej w centralnym systemie SIS;
- stworzenie nowej kategorii wpisów „osoba poszukiwana o nieustalonej tożsamości", w przypadku której dane kryminalistyczne mogą istnieć w krajowych bazach danych (np. ślad linii papilarnych pozostawiony na miejscu przestępstwa)[16].

Komisja będzie w dalszym ciągu wspierać finansowo wdrażanie projektów umożliwiających jednoczesne przeszukiwanie SIS i baz danych Interpolu zawierających dane skradzionych lub utraconych dokumentów podróży (SLTD) oraz dane dotyczące poszukiwanych przestępców, pojazdów i broni (iARMS), które stanowią uzupełnienie systemów informacyjnych UE[17].

Baza Interpolu zawierająca dane skradzionych lub utraconych dokumentów podróży (SLTD)

Kluczowe znaczenie dla skutecznego zarządzania granicami ma weryfikacja dokumentów podróży wszystkich obywateli państw trzecich i obywateli UE na podstawie **bazy danych SLTD**. Organy ścigania powinny również korzystać z bazy danych SLTD do celów wyszukiwania informacji w strefie Schengen. Po atakach terrorystycznych w Paryżu z 13 listopada 2015 r. Rada zaapelowała o ustanowienie elektronicznych połączeń z właściwymi bazami danych Interpolu na wszystkich przejściach granicznych na granicach zewnętrznych oraz o wprowadzenie

[15] W marcu 2016 r. Komisja przedstawiła Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące dostępności i gotowości rozwiązań technologicznych umożliwiających identyfikację osoby na podstawie odcisków palców przechowywanych w Systemie Informacyjnym Schengen drugiej generacji (SIS II).

[16] Stworzenie takiego nowego wpisu zostanie poddane ocenie w celu zapewnienia komplementarności oraz uniknięcia pokrywania się z istniejącymi ramami z Prüm, które umożliwiają wyszukiwanie odcisków palców w różnych krajowych bazach danych poszczególnych państw członkowskich UE.

[17] Opracowane przez Interpol narzędzia do wyszukiwania informacji, takie jak FIND (system zapewniający dostęp do baz danych Interpolu w trybie online) i MIND (system zapewniający dostęp do baz danych Interpolu w trybie offline), mają na celu ułatwienie jednoczesnego przeszukiwania systemów Interpolu i systemu SIS.

automatycznego sprawdzania dokumentów podróży do marca 2016 r.[18]. Wszystkie państwa członkowskie powinny ustanowić odpowiednie połączenia elektroniczne oraz wdrożyć systemy umożliwiające automatyczną aktualizację danych dotyczących skradzionych lub utraconych dokumentów podróży w bazie danych SLTD.

Dane pasażera przekazywane przed podróżą (API)

Zgodnie z obowiązującą najlepszą praktyką państwa członkowskie powinny zwiększyć wartość dodaną **danych pasażera przekazywanych przed podróżą** (API) przez wprowadzenie automatycznej kontroli krzyżowej tych danych z danymi zawartymi w bazie SIS i bazie danych SLTD Interpolu. Komisja przeanalizuje potrzebę zmiany podstawy prawnej przetwarzania danych API w celu zapewnienia szerszego wdrożenia oraz potrzebę nałożenia na państwa członkowskie obowiązku wymagania i wykorzystywania danych API w odniesieniu do wszystkich lotów wychodzących i przychodzących. Ma to szczególne znaczenie w kontekście wdrożenia przyszłej dyrektywy w sprawie danych dotyczących przelotu pasażera (PNR), ponieważ łączne wykorzystanie danych PNR i API zwiększa skuteczność wykorzystania danych PNR w walce z terroryzmem i poważną przestępczością[19].

Wizowy system informacyjny (VIS)

Komisja przeprowadza również ogólną ocenę **wizowego systemu informacyjnego** (VIS), która ma zostać zakończona w 2016 r. W ramach tej oceny Komisja bada, między innymi, w jaki sposób system VIS jest wykorzystywany do celów kontroli przeprowadzanych na granicach zewnętrznych i na terytorium państw członkowskich oraz w jaki sposób przyczynia się on do walki z oszustwami dotyczącymi tożsamości i oszustwami wizowymi. Na tej podstawie Komisja następnie przeanalizuje możliwości poprawy funkcjonalności VIS, m.in. przez:

- poprawę jakości obrazów twarzy w celu umożliwienia porównywania danych biometrycznych;
- wykorzystanie danych biometrycznych osób składających wnioski wizowe do wyszukiwania informacji w przyszłym systemie automatycznej identyfikacji daktyloskopijnej (AFIS), który ma zostać opracowany do celów SIS;
- obniżenie limitu wieku dla pobierania odcisków palców od dzieci w wieku od 6 do 12 lat przy jednoczesnym zapewnieniu niezawodnych gwarancji praw podstawowych i środków ochronnych[20];
- ułatwienie sprawdzania bazy danych SLTD Interpolu w trakcie składania wniosków wizowych.

Jeśli chodzi o możliwości dostępu do danych VIS do **celów egzekwowania prawa** na podstawie istniejących ram prawnych, państwa członkowskie wykorzystują te możliwości w niejednakowy sposób. W tym kontekście państwa członkowskie zgłosiły praktyczne problemy związane z procedurami dostępu organów ścigania do VIS. Także wdrażanie dostępu do systemu EURODAC do celów egzekwowania prawa jest w dalszym ciągu bardzo ograniczone. Komisja zbada, czy istnieje potrzeba ponownego rozważenia ram prawnych dostępu do systemów VIS i EURODAC do celów egzekwowania prawa.

---

[18] Konkluzje Rady UE i państw członkowskich zebranych w Radzie w sprawie zwalczania terroryzmu, 20 listopada 2015 r.

[19] Zob. sekcja 6.2 dotycząca zaproponowanej dyrektywy w sprawie danych dotyczących przelotu pasażera (PNR).

[20] Wyniki badania JRC „Fingerprint Recognition for children" (Rozpoznawanie odcisków palców dzieci) potwierdziły możliwości techniczne; EUR 26193 EN; ISBN 978-92-79-33390-3, 2013 r.

EURODAC

Jak określono w komunikacie pt. „W kierunku reformy wspólnego europejskiego systemu azylowego i zwiększenia liczby legalnych sposobów migracji do Europy”[21], Komisja przedstawi wniosek dotyczący reformy systemu **EURODAC** w celu dalszej poprawy jego funkcji w odniesieniu do nielegalnej migracji i powrotu. Wniosek ten ma się przyczynić do wyeliminowania obecnej luki dotyczącej zdolności śledzenia wtórnych przepływów migrantów o nieuregulowanym statusie między państwami członkowskimi. Jego celem jest również zwiększenie skuteczności procedur powrotu i readmisji przez wprowadzenie środków umożliwiających identyfikację migrantów o nieuregulowanym statusie i wydanie im nowych dokumentów tożsamości do celów powrotu. W tym kontekście wniosek ten uwzględnia również wymianę informacji zawartych w systemie EURODAC z państwami trzecimi, przy zachowaniu niezbędnych zabezpieczeń w zakresie ochrony danych.

Europol

UE przyznała **Europolowi** dostęp do głównych centralnych baz danych, ale Agencja nie wykorzystała jeszcze w pełni tej możliwości. Europol ma prawo dostępu do danych wprowadzonych do SIS oraz bezpośredniego przeszukiwania tych danych dotyczących aresztowań, kontroli niejawnych i kontroli szczególnych oraz przedmiotów przeznaczonych do zajęcia. Do tej pory Europol przeprowadził jedynie stosunkowo niewiele wyszukiwań w systemie SIS. Europol posiada prawne możliwości dostępu do systemu VIS do celów konsultacji od września 2013 r. Od lipca 2015 r. podstawa prawna systemu EURODAC umożliwia również dostęp Europolowi. Agencja powinna przyspieszyć prace trwające nad ustanowieniem połączenia z systemami VIS i EURODAC. Mówiąc ogólniej, Komisja zbada, czy konieczne jest zapewnienie dalszego dostępu do systemów informacyjnych innym agencjom UE działającym w obszarze spraw wewnętrznych, w szczególności przyszłej Europejskiej Straży Granicznej i Przybrzeżnej.

Ramy z Prüm

Obecnie możliwości **ram z Prüm** nie są w pełni wykorzystywane. Wynika to z tego, że nie wszystkie państwa członkowskie wdrożyły swoje zobowiązania prawne w zakresie integracji sieci z własnymi systemami. Państwa członkowskie otrzymały znaczące wsparcie finansowe i techniczne, aby wdrożyć ramy z Prüm, i teraz powinny je w pełni wdrożyć. Komisja korzysta z przyznanych jej uprawnień w celu zapewnienia pełnego wdrożenia zobowiązań prawnych państw członkowskich i w styczniu 2016 r. rozpoczęła zorganizowany dialog (EU Pilot) z państwami członkowskimi. Jeśli reakcje państw członkowskich okażą się niezadowalające, Komisja nie zawaha się wszcząć postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego.

Europejski system przekazywania informacji z rejestrów karnych (ECRIS)

Europejski system przekazywania informacji z rejestrów karnych **ECRIS** umożliwia wymianę informacji o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców, lecz brakuje skutecznej procedury takiej wymiany. W styczniu 2016 r. Komisja przyjęła wniosek prawny dotyczący zaradzenia tej sytuacji[22]. W jego ramach Komisja zaproponowała, aby umożliwić organom krajowym wyszukiwanie informacji na temat obywateli państw trzecich na podstawie odcisków palców w celu

[21] COM(2016)197 final.
[22] COM(2016) 7 final, 19.1.2016 r.

zwiększenia pewności identyfikacji. Parlament Europejski i Rada powinny przyjąć tekst legislacyjny w 2016 r.

Kwestie horyzontalne

Ogólnym problemem dotyczącym systemów informacyjnych jest **poziom ich wdrożenia** przez państwa członkowskie. Znamiennymi przykładami są niejednolite wdrożenie ram z Prüm oraz brak połączeń elektronicznych z bazą danych SLTD. Aby zwiększyć poziom wdrożenia systemów informacyjnych, Komisja będzie ściśle monitorować działania poszczególnych państw członkowskich[23]. W ramach monitorowania Komisja będzie badać nie tylko to, czy państwa członkowskie wywiązują się ze swoich zobowiązań prawnych dotyczących systemów informacyjnych, lecz także to, w jaki sposób państwa członkowskie wykorzystują istniejące instrumenty oraz czy stosują najlepsze praktyki. W ramach monitorowania poziomu wdrożenia oraz propagowania jego zwiększenia Komisja będzie korzystać z różnych źródeł, w tym z zawiadomień państw członkowskich oraz z wizyt prowadzonych w ramach mechanizmu oceny i monitorowania w odniesieniu do dorobku Schengen.

Innym problemem o charakterze ogólnym, który dotyczy systemów informacyjnych, jest **jakość wprowadzanych danych**. Niespełnienie przez państwa członkowskie minimalnych wymogów jakościowych znacząco ogranicza wiarygodność i wartość przechowywanych danych, a ryzyko niedopasowania i braku trafień zmniejsza wartość samych systemów. Aby poprawić jakość wprowadzanych danych, eu-LISA opracuje **możliwość centralnego monitorowania jakości danych** dla wszystkich systemów podlegających eu-LISA.

Większość systemów informacyjnych stosowanych w obszarze kontroli granicznej i bezpieczeństwa obsługuje dane identyfikacyjne pochodzące z dokumentów podróży i dokumentów tożsamości. Aby poprawić kontrolę graniczną i zwiększyć bezpieczeństwo w inny sposób niż za pomocą sprawnie działających systemów, należy zapewnić łatwe i bezpieczne poświadczanie autentyczności dokumentów podróży i dokumentów tożsamości. W tym celu Komisja przedstawi środki mające na celu poprawę elektronicznego **zabezpieczenia dokumentów** i zarządzania danymi identyfikacyjnymi oraz zwiększenie skuteczności walki z fałszowaniem dokumentów. Interoperacyjne poziomy bezpiecznej identyfikacji, które można osiągnąć na podstawie rozporządzenia w sprawie eIDAS[24], mogłyby stanowić potencjalny sposób realizacji powyższych celów.

<u>Działania na rzecz udoskonalenia istniejących systemów informacyjnych</u>

System Informacyjny Schengen (SIS)

- Opracowanie i wdrożenie przez Komisję i eu-LISA systemu automatycznej identyfikacji daktyloskopijnej (AFIS) w ramach systemu SIS do połowy 2017 r.
- Przedstawienie przez Komisję do końca 2016 r. wniosków dotyczących zmiany podstawy prawnej SIS w celu dalszej poprawy funkcjonalności tego systemu.
- Maksymalizacja wykorzystania SIS przez państwa członkowskie – zarówno przez wprowadzanie wszystkich istotnych informacji, jak i sprawdzanie w systemie wszelkich wymaganych informacji.

[23] Zgodnie ze szczegółowymi warunkami protokołu nr 22 (w odniesieniu do Danii) oraz protokołów nr 21 i 36 (w odniesieniu do Zjednoczonego Królestwa i Irlandii).

[24] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

Baza Interpolu zawierająca dane skradzionych lub utraconych dokumentów podróży (SLTD)

- Ustanowienie przez państwa członkowskie elektronicznych połączeń z narzędziami Interpolu na wszystkich przejściach granicznych znajdujących się na granicach zewnętrznych.
- Wypełnienie przez państwa członkowskie zobowiązania do wprowadzania i przeglądania danych skradzionych lub utraconych dokumentów podróży w SIS i bazie danych SLTD w tym samym czasie.

Dane pasażera przekazywane przed podróżą (API)

- Zautomatyzowanie przez państwa członkowskie wykorzystania danych API do kontroli na podstawie SIS i bazy danych Interpolu zawierającej dane skradzionych lub utraconych dokumentów podróży (SLTD), zgodnie z obowiązującą najlepszą praktyką.
- Zweryfikowanie przez Komisję potrzeby zmiany podstawy prawnej przetwarzania danych API.

Wizowy system informacyjny (VIS)

- Przeanalizowanie przez Komisję dalszych usprawnień systemu VIS do końca 2016 r.

EURODAC

- Przedstawienie przez Komisję wniosku dotyczącego zmiany podstawy prawnej EURODAC w celu dalszej poprawy funkcjonalności tego systemu w odniesieniu do nielegalnej migracji i powrotu.

Europol

- Pełne wykorzystywanie przez Europol swoich praw dostępu do SIS, VIS i EURODAC do celów konsultacji.
- Zbadanie i propagowanie przez Komisję i Europol synergii między systemem informacyjnym Europolu (EIS) i innymi systemami, w szczególności SIS.
- Przeanalizowanie przez Komisję i eu-LISA, czy system automatycznej identyfikacji daktyloskopijnej (AFIS), który ma zostać opracowany na potrzeby SIS, może uzupełnić systemy Europolu wykorzystywane do prowadzenia dochodzeń w sprawach karnych i w ramach walki z terroryzmem.

Ramy z Prüm

- Pełne wdrożenie i stosowanie ram z Prüm przez państwa członkowskie.
- W razie potrzeby wszczęcie przez Komisję postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego wobec tych państw członkowskich, które nie ustanowiły połączenia z ramami z Prüm.
- Przeanalizowanie przez Komisję i eu-LISA, czy system automatycznej identyfikacji daktyloskopijnej (AFIS), który ma zostać opracowany na potrzeby SIS, może uzupełnić system wymiany danych o odciskach palców na podstawie ram z Prüm.

Europejski system przekazywania informacji z rejestrów karnych (ECRIS)

- W 2016 r. Parlament Europejski i Rada powinny przyjąć wniosek legislacyjny umożliwiający organom krajowym wyszukiwanie informacji na temat obywateli państw trzecich w systemie ECRIS na podstawie odcisków palców.

Kwestie horyzontalne

- **Monitorowanie i promowanie** przez Komisję **odpowiedniego poziomu wdrożenia** systemów informacyjnych.
- Opracowanie przez eu-LISA **możliwości centralnego monitorowania jakości danych** dla wszystkich systemów podlegających eu-LISA.
- Przedstawienie przez Komisję środków mających na celu poprawę elektronicznego **zabezpieczenia dokumentów** i **zarządzania danymi identyfikacyjnymi** oraz zwiększenie skuteczności walki z fałszowaniem dokumentów.
- Przeanalizowanie przez Komisję synergii i zbieżności między systemami informacyjnymi oraz ich odpowiednimi infrastrukturami do celów zarządzania granicami UE i **operacji celnych**.

6. OPRACOWANIE DODATKOWYCH SYSTEMÓW INFORMACYJNYCH I WYELIMINOWANIE LUK

Chociaż istniejące systemy informacyjne obejmują bardzo szeroki zakres danych, który jest wymagany w ramach zarządzania granicami i egzekwowania prawa, występują również istotne luki. Komisja przestawiła propozycje wyeliminowania niektórych z nich w swoich wnioskach legislacyjnych, a mianowicie we wniosku dotyczącym systemu wjazdu/wyjazdu oraz wniosku dotyczącym unijnego systemu danych dotyczących przelotu pasażera (PNR). W odniesieniu do innych stwierdzonych luk należy dokładnie zbadać, czy dodatkowe narzędzia UE są potrzebne.

1. System wjazdu/wyjazdu

Wraz z niniejszym komunikatem Komisja przedstawiła zmienione wnioski legislacyjne dotyczące ustanowienia systemu wjazdu/wyjazdu (EES). Po ich przyjęciu przez współustawodawców eu-LISA opracuje i wdroży ten system we współpracy z państwami członkowskimi należącymi do strefy Schengen.

EES będzie rejestrować przypadki przekroczenia granicy (wjazdu i wyjazdu) przez wszystkich obywateli państw trzecich przybywających do strefy Schengen w ramach pobytu krótkoterminowego (maksymalnie 90 dni w okresie wynoszącym 180 dni), zarówno w odniesieniu do podróżnych podlegających obowiązkowi wizowemu, jak i do podróżnych zwolnionych z obowiązku wizowego, lub w ramach pobytu odbywanego na podstawie nowej wizy objazdowej (do jednego roku). Celem systemu EES jest: a) poprawa zarządzania granicami zewnętrznymi, b) ograniczenie nielegalnej migracji przez zapobieganie bezprawnemu przedłużaniu pobytu oraz c) wsparcie walki z terroryzmem i poważną przestępczością, co w rezultacie przyczyni się do zapewnienia wysokiego poziomu bezpieczeństwa wewnętrznego.

EES będzie rejestrować tożsamość obywateli państw trzecich (dane alfanumeryczne, cztery odciski palców i obraz twarzy) razem ze szczegółowymi danymi dotyczącymi ich dokumentów podróży oraz będzie łączyć wszystkie te dane z elektronicznymi wpisami na temat wjazdu i wyjazdu. Obecna praktyka stemplowania dokumentów podróży zostanie zaniechana. EES umożliwi skuteczne zarządzanie dozwolonymi pobytami krótkoterminowymi, zwiększy automatyzację kontroli granicznych oraz poprawi wykrywanie przypadków fałszowania dokumentów i tożsamości. Centralna rejestracja umożliwi wykrywanie osób nadmiernie przedłużających pobyt oraz identyfikację osób bez dokumentów przebywających w strefie Schengen. W związku z tym system EES wypełnia ważną lukę w krajobrazie istniejących systemów informacyjnych.

2. Dane dotyczące przelotu pasażera

Dane dotyczące przelotu pasażera (PNR) obejmują informacje na temat rezerwacji łącznie z informacjami kontaktowymi, szczegółowe informacje na temat trasy podróży i rezerwacji, uwagi specjalne, informacje dotyczące miejsca siedzenia i bagażu oraz informacje o sposobie płatności. Dane PNR są pomocne oraz niezbędne do wykrywania pasażerów mogących stanowić istotne zagrożenie w kontekście walki z terroryzmem, handlu narkotykami i ludźmi, wykorzystywania seksualnego dzieci oraz innych poważnych przestępstw. Celem zaproponowanej dyrektywy w sprawie PNR jest poprawa współdziałania systemów krajowych oraz zmniejszenie luk w zakresie bezpieczeństwa występujących między poszczególnymi państwami członkowskimi. Dyrektywa w sprawie PNR ma więc służyć wyeliminowaniu istotnej luki w dostępności danych, które są niezbędne do walki z poważną przestępczością i terroryzmem. **Dyrektywa w sprawie PNR powinna zostać przyjęta i wdrożona w trybie pilnym.**

Przyszła dyrektywa nałoży na państwa członkowskie obowiązek utworzenia jednostek do spraw informacji o pasażerach (PIU), które będą otrzymywały dane PNR od przewoźników. Przepisy tej dyrektywy nie będą natomiast wymagały utworzenia centralnego systemu lub centralnej bazy danych; zakłada się korzystanie z pewnego poziomu standaryzacji krajowych rozwiązań technicznych i procedur. Ułatwi to wymianę danych PNR między jednostkami PIU, jak przewidziano w zaproponowanej dyrektywie. W tym celu Komisja wesprze państwa członkowskie w analizowaniu różnych możliwości wzajemnego połączenia jednostek PIU w celu zaproponowania standardowych rozwiązań i procedur. Po przyjęciu dyrektywy Komisja przyspieszy prace nad wspólnymi protokołami i obsługiwanymi formatami danych do celów przekazywania danych PNR przez przewoźników lotniczych do jednostek PIU. Komisja przygotuje projekt aktu wykonawczego w ciągu trzech miesięcy od przyjęcia dyrektywy.

3. Luka informacyjna przed przybyciem obywateli państw trzecich zwolnionych z obowiązku wizowego

Podczas gdy tożsamość, dane kontaktowe i podstawowe informacje o posiadaczach wiz są zarejestrowane w systemie VIS, jedyne informacje o osobach zwolnionych z obowiązku wizowego pochodzą z ich dokumentów podróży. W przypadku osób podróżujących drogą powietrzną lub morską informacje te mogą zostać uzupełnione danymi API przed ich przybyciem. Zgodnie z zaproponowaną dyrektywą w sprawie PNR dane PNR tych osób będą gromadzone również w sytuacji, gdy będą one przybywać do UE drogą powietrzną. W przypadku osób przybywających do UE przez granice lądowe żadne informacje nie są dostępne przed ich przybyciem na granicę zewnętrzną UE.

Podczas gdy organy ścigania mogą uzyskać informacje dotyczące posiadaczy wiz z systemu VIS, jeśli takie informacje są niezbędne do walki z poważną przestępczością i terroryzmem, porównywalne dane dotyczące osób zwolnionych z obowiązku wizowego w ogóle nie są dostępne. Taki brak informacji ma szczególne znaczenie dla zarządzania lądowymi granicami UE w sytuacji, gdy znacząca liczba osób zwolnionych z obowiązku wizowego przybywa samochodem, autokarem lub pociągiem. Kilka krajów sąsiadujących z UE zniosło już obowiązek wizowy; trwają również dialogi w sprawie liberalizacji systemu wizowego między UE z pozostałymi krajami sąsiadującymi. Prawdopodobnie doprowadzi to w niedalekiej przyszłości do znaczącego wzrostu liczby podróżnych zwolnionych z obowiązku wizowego.

Komisja zbada, czy nowe narzędzie UE, które miałoby rozwiązać tę kwestię, jest konieczne, możliwe do wprowadzenia i proporcjonalne. Można zastanowić się nad wprowadzeniem **unijnego systemu informacji o podróży i zezwoleń na podróż**

(ETIAS), w którym podróżni zwolnieni z obowiązku wizowego rejestrowaliby istotne informacje o swojej planowanej podróży. Automatyczne przetwarzanie tych informacji mogłoby pomóc funkcjonariuszom straży granicznej w ocenie obywateli państw trzecich przybywających na krótki pobyt. Państwa takie jak Stany Zjednoczone, Kanada i Australia już wdrożyły podobne systemy, w tym systemy identyfikacji obywateli UE.

Systemy zezwoleń na podróż opierają się na wnioskach online, w których wnioskodawca musi podać przed planowanym wyjazdem szczegółowe informacje na temat swojej tożsamości, dane kontaktowe, cel i plan podróży. Po uzyskaniu zezwolenia procedury graniczne w momencie przybycia na granicę stają się szybsze i płynniejsze. Oprócz korzyści związanych z bezpieczeństwem i zarządzaniem granicami oraz potencjalnego znaczenia w kontekście wzajemności wizowej system taki jak ETIAS służyłby więc również jako narzędzie ułatwiające podróżowanie.

4. Europejski system przekazywania informacji z akt policyjnych (EPRIS)

Jak określono w Europejskiej agendzie bezpieczeństwa, dostępność istniejących danych policyjnych w czasie rzeczywistym we wszystkich państwach członkowskich jest ważnym obszarem przyszłych działań w zakresie wymiany informacji. Komisja oceni konieczność, wykonalność techniczną i proporcjonalność europejskiego systemu przekazywania informacji z akt policyjnych (EPRIS) w celu ułatwienia transgranicznego dostępu do informacji przechowywanych w krajowych bazach danych organów ścigania. W tym kontekście Komisja wspiera finansowo wdrożenie projektu pilotażowego przez grupę pięciu państw członkowskich w celu ustanowienia mechanizmu zautomatyzowanego transgranicznego przeszukiwania indeksów krajowych na zasadzie trafienie lub braku trafienia[25]. Komisja uwzględni wyniki tego projektu w swojej ocenie.

Działania na rzecz opracowania dodatkowych systemów informacyjnych i wyeliminowania luk informacyjnych

System wjazdu/wyjazdu (EES)

- Parlament Europejski i Rada powinny traktować wnioski legislacyjne dotyczące systemu EES jako sprawę priorytetową oraz dążyć do ich przyjęcia do końca 2016 r.

Dane dotyczące przelotu pasażera (PNR)

- Parlament Europejski i Rada powinny przyjąć dyrektywę w sprawie PNR do kwietnia 2016 r.
- Państwa członkowskie powinny wdrożyć przyjętą dyrektywę w sprawie PNR w trybie pilnym.
- Komisja powinna wesprzeć wymianę danych między jednostkami do spraw informacji o pasażerach (PIU) za pomocą standardowych rozwiązań i procedur.
- Komisja powinna przygotować projekt decyzji wykonawczej dotyczącej wspólnych protokołów i obsługiwanych formatów danych do celów przekazywania danych PNR przez przewoźników lotniczych do jednostek PIU w ciągu trzech miesięcy od przyjęcia dyrektywy w sprawie PNR.

[25] Celem projektu pilotażowego ADEP (proces zautomatyzowanej wymiany danych) jest stworzenie systemu technicznego, który umożliwi sprawdzanie (za pomocą indeksu), czy akta policyjne dotyczące konkretnej osoby lub prowadzonego przez policję dochodzenia w sprawie o przestępstwo istnieją w jednym lub w kilku innych państwach członkowskich. Automatyczna odpowiedź na przeszukanie indeksu wskazywałaby jedynie, czy dane są dostępne: trafienie lub brak trafienia. W przypadku trafienia dodatkowe dane osobowe należałoby podać w drugim kroku za pośrednictwem zwykłych kanałów współpracy policyjnej.

Luka informacyjna przed przybyciem obywateli państw trzecich zwolnionych z obowiązku wizowego

- Komisja powinna ocenić w 2016 r. konieczność, wykonalność techniczną i proporcjonalność ustanowienia nowego narzędzia UE takiego jak unijny system informacji o podróży i zezwoleń na podróż (ETIAS).

Europejski system przekazywania informacji z akt policyjnych (EPRIS)

- Komisja powinna ocenić w 2016 r. konieczność, wykonalność techniczną i proporcjonalność ustanowienia systemu EPRIS.

7. W KIERUNKU INTEROPERACYJNOŚCI SYSTEMÓW INFORMACYJNYCH

Interoperacyjność to zdolność systemów informacyjnych do wymiany danych oraz do umożliwienia dzielenia się informacjami. Można wyróżnić **cztery wymiary interoperacyjności**, z którego każdy obejmuje aspekty prawne[26], techniczne i operacyjne, w tym dotyczące ochrony danych:

- pojedynczy interfejs wyszukiwania umożliwiający jednoczesne przeszukiwanie kilku systemów informacyjnych oraz wyświetlanie łącznych wyników na jednym ekranie;
- wzajemne połączenia między systemami informacyjnymi, dzięki czemu dane zarejestrowane w jednym systemie będą automatycznie sprawdzane przez drugi system;
- stworzenie wspólnej funkcji porównywania danych biometrycznych, która obsługiwałaby różne systemy informacyjne;
- wspólne repozytorium danych dla różnych systemów informacyjnych (moduł główny).

Aby rozpocząć proces wprowadzania interoperacyjności systemów informacyjnych na szczeblu UE, Komisja powoła na wysokim szczeblu **grupę ekspertów ds. systemów informacyjnych i interoperacyjności** z udziałem agencji UE, ekspertów krajowych i zainteresowanych instytucji. Zadaniem grupy ekspertów będzie zajęcie się aspektami prawnymi, technicznymi i operacyjnymi różnych możliwości osiągnięcia interoperacyjności systemów informacyjnych, w tym rozważenie konieczności, wykonalności technicznej i proporcjonalności dostępnych możliwości oraz ich wpływu na ochronę danych. Grupa ekspertów powinna również zająć się obecnym niedociągnięciami i lukami w wiedzy, które wynikają ze złożoności i rozdrobnienia systemów informacyjnych na poziomie europejskim. Grupa ekspertów zajmie się zarządzaniem granicami i egzekwowaniem prawa z szerokiej i wielostronnej perspektywy i uwzględni przy tym również funkcje i obowiązki organów celnych oraz stosowane przez nie odpowiednie systemy. Metodyka pracy grupy ekspertów będzie ukierunkowana na połączenie wszystkich istotnych doświadczeń, które w przeszłości zbyt często nie podlegały wymianie.

Celem tego procesu jest przedstawienie ogólnej strategicznej wizji unijnej architektury zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa oraz zaproponowanie rozwiązań wdrożeniowych.

Procesowi konsultacji winny **przyświecać następujące cele**:

[26] Zgodnie ze szczegółowymi warunkami protokołu nr 22 (w odniesieniu do Danii) oraz protokołów nr 21 i 36 (w odniesieniu do Zjednoczonego Królestwa i Irlandii).

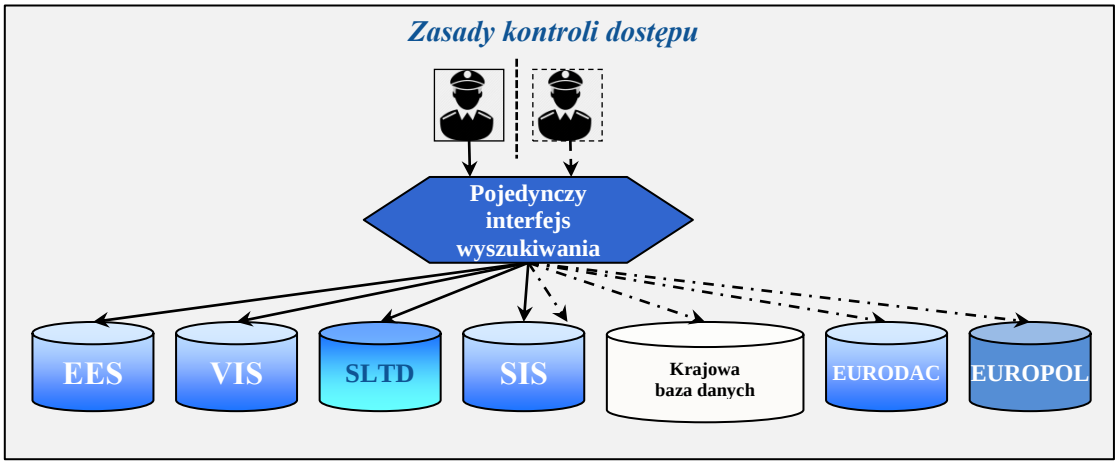
- Systemy informacyjne powinny się uzupełniać. Należy unikać nakładania się tych systemów, a już istniejące przypadki nakładania się należy zlikwidować. Należy odpowiednio zająć się występującymi lukami.
- Należy stosować podejście modułowe, wykorzystując w pełni rozwój technologiczny oraz opierając się na zasadach „uwzględnienia ochrony prywatności już w fazie projektowania".
- Od samego początku należy zapewnić pełne przestrzeganie wszystkich praw podstawowych przysługujących zarówno obywatelom UE, jak i obywatelom państw trzecich na mocy Karty praw podstawowych Unii Europejskiej.
- Tam, gdzie jest to konieczne i możliwe, systemy informacyjne powinny być ze sobą wzajemnie połączone i powinny ze sobą współdziałać. Należy ułatwić jednoczesne przeszukiwanie systemów, aby zagwarantować, że funkcjonariusze straży granicznej i funkcjonariusze policji będą mieli dostęp do wszelkich istotnych informacji wtedy, gdy (i tam, gdzie) będą ich potrzebować do wykonania swoich obowiązków, bez zmiany istniejących praw dostępu.

1. Pojedynczy interfejs wyszukiwania

Pierwszym wymiarem interoperacyjności jest umożliwienie funkcjonariuszom straży granicznej lub funkcjonariuszom policji **jednoczesnego przeszukiwania kilku systemów informacyjnych oraz wyświetlania łącznych wyników na jednym ekranie** przy pełnym poszanowaniu ich praw dostępu oraz odpowiednio do ich właściwych zadań. Wymaga to korzystania z platform z pojedynczym interfejsem wyszukiwania, które są w stanie przeszukiwać kilka systemów informacyjnych w tym samym czasie w ramach pojedynczego zapytania. Na przykład, odczytując układ scalony w dokumencie podróży lub wykorzystując dane biometryczne, taka platforma mogłaby przeszukiwać kilka różnych baz danych w tym samym czasie. Podejście oparte na pojedynczej kwerendzie ma zastosowanie do wszystkich organów, które potrzebują mieć do tych danych i z nich korzystać (tj. funkcjonariuszy straży granicznej, organów ścigania, ośrodków azylowych), zgodnie z zasadą celowości oraz z surowymi zasadami kontroli dostępu. Pojedynczy interfejs wyszukiwania działa również na urządzeniach mobilnych. Ustanowienie pojedynczego interfejsu wyszukiwania przyczyni się do zmniejszenia złożoności systemów informacyjnych na poziomie europejskim, ponieważ taki interfejs umożliwia funkcjonariuszom straży granicznej i funkcjonariuszom policji jednoczesne przeszukiwanie kilku systemów informacyjnych za pomocą jednej procedury oraz zgodnie z ich prawami dostępu.

Kilka państw członkowskich już zainstalowało takie platformy z pojedynczym interfejsem wyszukiwania. Zgodnie z obowiązującą najlepszą praktyką w tym zakresie Komisja wspólnie z eu-LISA podejmie działania na rzecz wypracowania standardowego rozwiązania dla pojedynczego interfejsu wyszukiwania. Państwa członkowskie powinny wykorzystać unijne środki finansowe dostępne w ramach krajowych programów Funduszu Bezpieczeństwa Wewnętrznego do sfinansowania wprowadzenia takiej funkcji. Komisja będzie ściśle monitorować, w jaki sposób państwa członkowskie wykorzystują funkcję pojedynczego interfejsu wyszukiwania na szczeblu krajowym.

***Rysunek 2** Pojedynczy interfejs wyszukiwania*



Przeszukiwanie wielu systemów scentralizowanych lub krajowych (patrz rysunek) jest łatwiejsze do wprowadzenia niż przeszukiwanie systemów zdecentralizowanych. Komisja i eu-LISA zbadają, czy pojedynczy interfejs wyszukiwania można również wykorzystywać do jednoczesnego przeszukiwania systemów zdecentralizowanych takich jak Prüm i ECRIS na zasadzie kompleksowej. Komisja i eu-LISA przeprowadzą taką analizę wspólnie z grupą ekspertów ds. systemów informacyjnych i interoperacyjności bez zmiany istniejących praw dostępu.

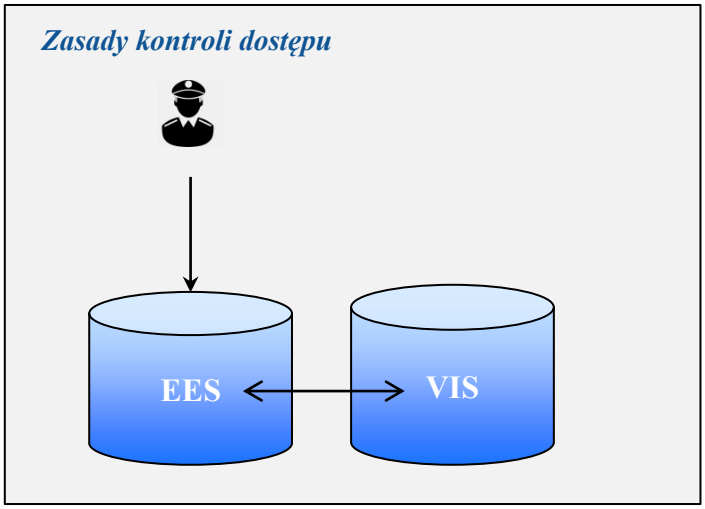
2. Wzajemne połączenia między systemami informacyjnymi

Drugim wymiarem interoperacyjności są wzajemne połączenia między systemami informacyjnymi. Oznacza to, że różne systemy lub bazy danych potrafią ze sobą „rozmawiać” z technicznego punktu widzenia. **Dane zarejestrowane w jednym systemie mogłyby być automatycznie sprawdzane przez drugi system na poziomie centralnym**. Wymaga to technicznej kompatybilności systemów oraz konieczności współdziałania elementów danych przechowywanych w tych systemach (np. odciski palców). Wzajemne połączenia między systemami mogą przyczynić się do zmniejszenia ilości danych krążących w sieciach komunikacyjnych oraz przepływających przez systemy krajowe.

Wzajemne połączenia wymagają odpowiednich zabezpieczeń zapewniających ochronę danych oraz surowych zasad kontroli dostępu. Zgodnie z porozumieniem politycznym osiągniętym przez współustawodawców w grudniu 2015 r. w sprawie reformy ochrony danych w całej UE zostaną wdrożone nowoczesne ramy ochrony danych, które zapewnią wspomniane zabezpieczenia. Ważne jest, aby współustawodawcy niezwłocznie przyjęli ogólne rozporządzenie o ochronie danych oraz dyrektywę o ochronie danych.

Koncepcja wzajemnych połączeń jest nieodłącznym elementem przyszłego systemu EES. Przyszły system EES będzie w stanie komunikować się bezpośrednio z systemem VIS na szczeblu centralnym i na odwrót. Jest to ważny krok w kierunku zaradzenia obecnemu rozdrobnieniu unijnej architektury zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa, a także w kierunku rozwiązania powiązanych problemów. Wprowadzenie automatycznej kontroli krzyżowej zwolni państwa członkowskie z konieczności przeszukiwania systemu VIS podczas kontroli granicznych oraz ograniczy wymogi konserwacyjne i poprawi działanie systemów.

Rysunek 3 *Wzajemne połączenia między systemami: przykład EES/VIS*



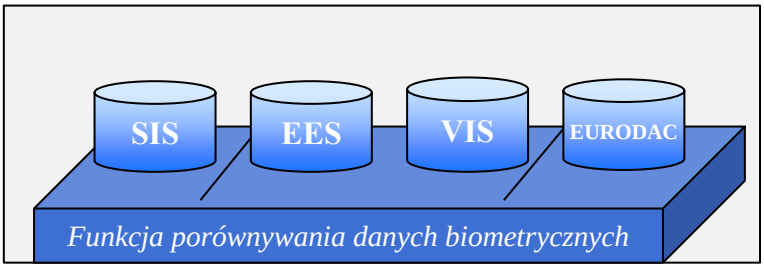
Następnie Komisja i eu-LISA przeanalizują, czy wzajemne połączenia między przyszłym systemem EES i systemem VIS na szczeblu centralnym można rozszerzyć na system SIS oraz czy można połączyć systemy EURODAC i SIS. Komisja i eu-LISA przeprowadzą taką analizę wspólnie z grupą ekspertów ds. systemów informacyjnych i interoperacyjności.

3. Wspólna funkcja porównywania danych biometrycznych

Trzecim wymiarem interoperacyjności jest obszar identyfikatorów biometrycznych. Na przykład, gdy odciski palców są pobierane w konsulacie jednego państwa członkowskiego przy użyciu specjalnego urządzenia, niezwykle ważne jest, aby odciski te można było porównać za pomocą systemu VIS na przejściu granicznym innego państwa członkowskiego przy użyciu sprzętu innego rodzaju. Ten sam wymóg dotyczy kwerend dotyczących porównania odcisków palców w innych systemach: próbki biometryczne muszą spełniać minimalne wymogi w zakresie jakości i formatu, aby bez trudu osiągnąć taki rodzaj interoperacyjności.

Na poziomie systemu interoperacyjność identyfikatorów biometrycznych umożliwia korzystanie ze wspólnej funkcji porównywania danych biometrycznych w odniesieniu do kilku systemów informacyjnych, zgodnie z zasadami ochrony danych osobowych poprzez podział danych oraz zgodnie z oddzielnymi zasadami kontroli dostępu do poszczególnych kategorii danych[27]. Takie wspólne funkcje przynoszą znaczące korzyści finansowe, konserwacyjne i operacyjne.

Rysunek 4 *Wspólna funkcja porównywania danych biometrycznych*



[27] Wspólną funkcję można porównać do korzystania z jednego fizycznego serwera plików przez wielu użytkowników, z których każdy ma specjalne prawa dostępu wyłącznie do określonych folderów.

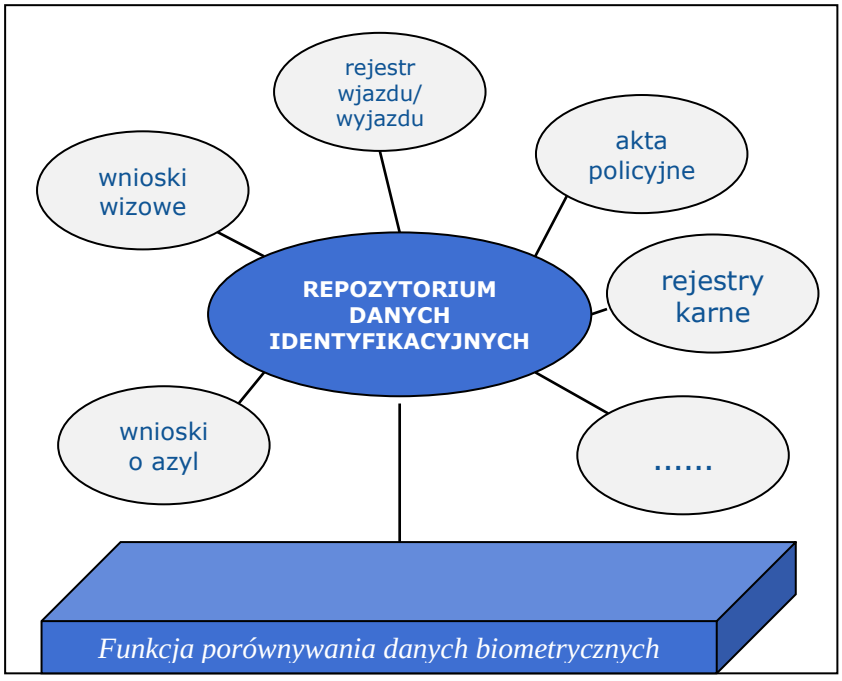
Komisja i eu-LISA przeanalizują, czy opracowanie wspólnej funkcji porównywania danych biometrycznych dla wszystkich właściwych systemów informacyjnych jest konieczne i technicznie wykonalne. Komisja i eu-LISA przeprowadzą taką analizę wspólnie z grupą ekspertów ds. systemów informacyjnych i interoperacyjności.

4. Wspólne repozytorium danych

Najambitniejszym długoterminowym sposobem zapewnienia interoperacyjności byłoby ustanowienie **wspólnego repozytorium danych na szczeblu UE dla różnych systemów informacyjnych**. Wspólne repozytorium stanowiłoby moduł główny, który zawierałby podstawowe dane (dane alfanumeryczne i biometryczne), podczas gdy pozostałe elementy danych i specjalne funkcje różnych systemów informacyjnych (np. dane wizowe) byłyby przechowywane w modułach specjalnych. Moduł główny i moduły specjalne byłyby ze sobą połączone w celu zapewnienia dalszego połączenia odpowiednich zbiorów danych. Takie rozwiązanie umożliwiłoby **modułowe i zintegrowane zarządzanie danymi identyfikacyjnymi do celów zarządzania granicami i zapewnienia bezpieczeństwa**. Należałoby zapewnić zgodność z zasadami ochrony danych, na przykład poprzez podział danych, oraz z oddzielnymi zasadami kontroli dostępu do poszczególnych kategorii danych.

Utworzenie wspólnego repozytorium danych zaradziłoby obecnemu rozdrobnieniu unijnej architektury zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa. Takie rozdrobnienie jest sprzeczne z zasadą minimalizacji danych, ponieważ prowadzi do tego, że te same dane są przechowywane kilkakrotnie. W stosownych przypadkach wspólne repozytorium umożliwiałoby rozpoznawanie powiązań oraz dawałoby ogólny obraz sytuacji poprzez łączenie poszczególnych elementów danych przechowywanych w różnych systemach informacyjnych. Takie repozytorium wypełniłoby tym samym obecne luki w wiedzy oraz rzuciłoby światło na „martwe strefy", z którymi spotykają się funkcjonariusze straży granicznej i funkcjonariusze policji.

Rysunek 5 *Wspólne repozytorium danych*



Utworzenie wspólnego repozytorium danych na szczeblu UE rodzi poważne pytania dotyczące definicji celowości, konieczności, wykonalności technicznej oraz proporcjonalności przetwarzania danych. Takie rozwiązanie wymagałoby całkowitego przeglądu ram prawnych ustanawiających różne systemy informacyjne i stanowiłoby jedynie cel długoterminowy. Grupa ekspertów ds. systemów informacyjnych i interoperacyjności zajmie się kwestiami prawnymi, technicznymi i operacyjnymi dotyczącymi wspólnego repozytorium danych, w tym kwestiami ochrony danych.

W odniesieniu do wszystkich czterech wyżej opisanych wymiarów interoperacyjności (pojedynczy interfejs wyszukiwania, wzajemne połączenia między systemami, funkcja porównywania danych biometrycznych i wspólne repozytorium danych) wymagana jest kompatybilność danych przechowywanych w różnych systemach informacyjnych lub modułach. Aby osiągnąć taką kompatybilność, należy rozpocząć prace nad **jednolitym formatem wiadomości** (UMF) w celu stworzenia wspólnego standardu dla wszystkich właściwych systemów informacyjnych[28].

Działania na rzecz interoperacyjności systemów informacyjnych

- Powołanie przez Komisję **grupy ekspertów ds. systemów informacyjnych i interoperacyjności** z udziałem agencji UE, państw członkowskich i właściwych zainteresowanych stron, do której zadań należałaby analiza prawnych, technicznych i operacyjnych aspektów zwiększenia interoperacyjności systemów informacyjnych, w tym rozważenie konieczności, wykonalności technicznej i proporcjonalności dostępnych możliwości oraz ich wpływu na ochronę danych.

Pojedynczy interfejs wyszukiwania

- Wsparcie przez Komisję i eu-LISA państw członkowskich we wprowadzaniu pojedynczego interfejsu wyszukiwania do przeszukiwania systemów centralnych.
- Przeanalizowanie przez Komisję i eu-LISA, wspólnie z grupą ekspertów, czy pojedyncze interfejsy wyszukiwania można by wykorzystywać do jednoczesnego przeszukiwania wszystkich właściwych systemów na zasadzie kompleksowej, bez zmiany istniejących praw dostępu.

Wzajemne połączenia między systemami informacyjnymi

- Przeanalizowanie przez Komisję i eu-LISA, wspólnie z grupą ekspertów, czy można dalej propagować wzajemne połączenia między scentralizowanymi systemami informacyjnymi poza już zaproponowanym połączeniem systemu wjazdu/wyjazdu i systemu informacji wizowej.

Funkcja porównywania danych biometrycznych

- Przeanalizowanie przez Komisję i eu-LISA, wspólnie z grupą ekspertów, czy opracowanie wspólnej funkcji porównywania danych biometrycznych dla wszystkich właściwych systemów informacyjnych jest konieczne i technicznie wykonalne.

Wspólne repozytorium danych (moduł główny)

[28] Komisja poparła dalsze opracowywanie jednolitego formatu wiadomości (UMF) w komunikacie z 2012 r. dotyczącym europejskiego modelu wymiany informacji (EIXM) i obecnie finansuje trzeci projekt pilotażowy UMF w celu wypracowania wspólnego standardu dla wszystkich właściwych baz danych, który byłby wykorzystywany na szczeblu krajowym (przez państwa członkowskie), unijnym (w odniesieniu do systemów centralnych; i przez agencje) i międzynarodowym (Interpol).

- Przeanalizowanie przez Komisję i eu-LISA, wspólnie z grupą ekspertów, prawnych, technicznych, operacyjnych i finansowych skutków rozwoju wspólnego repozytorium danych w perspektywie długookresowej.
- Zaangażowanie się przez Komisję i eu-LISA w bieżące prace nad stworzeniem globalnego jednolitego formatu wiadomości dla wszystkich właściwych systemów informacyjnych.

8. WNIOSEK

Niniejszy komunikat rozpoczyna dyskusję na temat tego, w jaki sposób systemy informacyjne działające w UE mogą przyczynić się do poprawy zarządzania granicami i zwiększenia bezpieczeństwa wewnętrznego w oparciu o istotne efekty synergii między Europejską agendą bezpieczeństwa a Europejskim programem w zakresie migracji. Szereg systemów informacyjnych już zapewnia funkcjonariuszom straży granicznej i funkcjonariuszom policji dostęp do istotnych informacji, lecz systemy te nie są doskonałe. UE stoi w obliczu wyzwania, jakim jest stworzenie silniejszej i inteligentniejszej architektury zarządzania danymi przy pełnym poszanowaniu praw podstawowch, a w szczególności ochrony danych osobowych i związanej z nią zasady celowości.

Luki, które występują w unijnej architekturze zarządzania danymi, należy zlikwidować. Wraz z niniejszym komunikatem Komisja przedstawiła wniosek dotyczący systemu wjazdu/wyjazdu, który powinien zostać przyjęty w trybie pilnym. Dyrektywę w sprawie danych dotyczących przelotu pasażera również należy przyjąć w najbliższych tygodniach. Wniosek dotyczący Europejskiej Straży Granicznej i Przybrzeżnej należy przyjąć przed początkiem lata. Równocześnie Komisja będzie kontynuować prace nad wzmocnieniem i w razie potrzeby usprawnieniem istniejących systemów, na przykład nad opracowaniem systemu automatycznej identyfikacji daktyloskopijnej do celów Systemu Informacyjnego Schengen.

Państwa członkowskie muszą w pełni wykorzystywać istniejące systemy informacyjne oraz ustanowić niezbędne połączenia techniczne ze wszystkimi systemami informacyjnymi i bazami danych zgodnie ze swoimi zobowiązaniami prawnymi. Istniejące niedociągnięcia, zwłaszcza w ramach z Prüm, należy niezwłocznie wyeliminować. Chociaż niniejszy komunikat otwiera dyskusję i zapoczątkowuje proces likwidacji luk i wad systemowych, to państwa członkowskie muszą niezwłocznie zaradzić uporczywym niedociągnięciom w zakresie dostarczania danych do unijnych baz danych oraz wymiany informacji w całej Unii.

Aby w sposób strukturalny udoskonalić unijną architekturę zarządzania danymi do celów kontroli granic i zapewnienia bezpieczeństwa, niniejszy komunikat przyjęto, aby dać początek procesowi w kierunku zapewnienia interoperacyjności systemów informacyjnych. Komisja powoła grupę ekspertów ds. systemów informacyjnych i interoperacyjności, do której zadań będzie należała analiza prawnych, technicznych i operacyjnych możliwości osiągnięcia interoperacyjności systemów informacyjnych, a także wyeliminowanie wszelkich niedociągnięć i luk. Na podstawie ustaleń grupy ekspertów Komisja Europejska przedstawi Parlamentowi Europejskiemu i Radzie dalsze konkretne pomysły, które będą stanowić podstawę wspólnej dyskusji na temat przyszłych działań. Komisja zwróci się również o opinię Europejskiego Inspektora Ochrony Danych oraz organów krajowych ds. ochrony danych działających w ramach Grupy Roboczej Art. 29.

Celem powinno być opracowanie wspólnej strategii na rzecz zwiększenia skuteczności i efektywności zarządzania danymi w UE, zgodnie z wszelkimi wymogami w zakresie

ochrony danych, aby zapewnić lepszą ochronę granic zewnętrznych UE oraz zwiększyć jej bezpieczeństwo wewnętrzne dla dobra wszystkich obywateli.

ZAŁĄCZNIK 1: INDEKS SKRÓTÓW

API	Dane pasażera przekazywane przed podróżą
AFIS	System automatycznej identyfikacji daktyloskopijnej: system służący do pobierania, przechowywania, porównywania i weryfikacji odcisków palców.
CIS	System informacji celnej
ECRIS	Europejski system przekazywania informacji z rejestrów karnych
EES	System wjazdu/wyjazdu (propozycja)
EIXM	Europejski model wymiany informacji
EIS	System informacyjny Europolu
EPRIS	Europejski system przekazywania informacji z akt policyjnych
EURODAC	Europejski system identyfikacji odcisków palców
EUROPOL	Europejski Urząd Policji (organ ścigania Unii Europejskiej)
ETIAS	Unijny system informacji o podróży i zezwoleń na podróż (propozycja)
eu-LISA	Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości
FIND	System zapewniający dostęp do baz danych Interpolu w trybie online
FRONTEX	Europejska Agencja Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej
iARMS	System Interpolu do zarządzania rejestrowaniem i śledzeniem nielegalnej broni
INTERPOL	Międzynarodowa Organizacja Policji Kryminalnej
MIND	System zapewniający dostęp do baz danych Interpolu w trybie offline
PIU	Jednostka do spraw informacji o pasażerach: jednostka, która ma powstać w każdym państwie członkowskim w celu odbierania danych PNR od przewoźników.
PNR	Dane dotyczące przelotu pasażera
Prüm	Mechanizm współpracy policyjnej służący wymianie informacji dotyczących profili DNA, odcisków palców i danych rejestracyjnych pojazdów
SafeSeaNet	Europejska platforma wymiany danych morskich między organami nadzoru morskiego państw członkowskich
SBC	Kodeks graniczny Schengen
SIENA	Aplikacja sieci bezpiecznej wymiany informacji
SIS	System Informacyjny Schengen (czasami nazywany systemem drugiej generacji – SIS II)
SLTD	Baza Interpolu zawierająca dane skradzionych lub utraconych dokumentów podróży
sTESTA	Bezpieczna transeuropejska telematyczna sieć komunikacyjna między organami administracji (ma zostać zaktualizowana do TESTA-NG (sieci następnej generacji))

UMF	Jednolity format wiadomości: format wiadomości umożliwiający zapewnienie kompatybilności systemów informacyjnych
VIS	Wizowy system informacyjny
VRD	Dane rejestracyjne pojazdów

ZAŁĄCZNIK 2: WYKAZ ISTNIEJĄCYCH SYSTEMÓW INFORMACYJNYCH DO CELÓW ZARZĄDZANIA GRANICAMI I EGZEKWOWANIA PRAWA

1. System Informacyjny Schengen (SIS)

SIS jest największą i najczęściej stosowaną platformą wymiany informacji na temat imigracji i egzekwowania prawa. Jest to system scentralizowany, z którego korzysta 25 państw członkowskich UE[29] oraz cztery państwa stowarzyszone w ramach Schengen[30]; system ten zawiera obecnie 63 mln wpisów. Wpisy wprowadzają i sprawdzają właściwe organy takie jak policja, organy kontroli granicznej i organy imigracyjne. SIS zawiera informacje dotyczące obywateli państw trzecich, którzy mają zakaz wjazdu do strefy Schengen lub przebywania w strefie Schengen, a także informacje dotyczące obywateli UE i obywateli państw trzecich, którzy są poszukiwani lub zaginieni (w tym dzieci), i informacje dotyczące poszukiwanych przedmiotów (broni palnej, pojazdów, dokumentów tożsamości, sprzętu przemysłowego itd.). Wyróżniającą cechą SIS w porównaniu z innymi instrumentami wymiany informacji jest to, że informacjom zawartym w tym systemie towarzyszą instrukcje konkretnego działania, jakie powinni podjąć funkcjonariusze na miejscu, na przykład aresztowanie lub zajęcie.

Kontrole w SIS są obowiązkowe dla wydawania wiz krótkoterminowych oraz kontroli granicznych wobec obywateli państw trzecich i wyrywkowo[31] wobec obywateli UE i innych osób korzystających z prawa do swobodnego przemieszczania się. Ponadto każda kontrola policyjna na danym terytorium powinna obejmować automatyczną kontrolę w SIS.

2. Wizowy system informacyjny (VIS)

VIS jest scentralizowanym systemem wymiany danych dotyczących wiz krótkoterminowych między państwami członkowskimi. Służy on do przetwarzania danych i decyzji dotyczących wniosków o wizy krótkoterminowe zezwalające na pobyt w strefie Schengen lub przejazd przez strefę Schengen. Z systemem VIS są połączone wszystkie konsulaty państw należących do strefy Schengen (około 2 000) oraz wszystkie przejścia graniczne na granicach zewnętrznych tych państw (łącznie około 1 800).

VIS zawiera dane dotyczące wniosków i decyzji wizowych oraz informacje na temat tego, czy wydane wizy zostały cofnięte, unieważnione lub przedłużone. Obecnie zawiera dane dotyczące 20 mln wniosków wizowych i w okresie szczytowym przetwarza ponad 50 000 transakcji na godzinę. Każda osoba ubiegająca się o wizę musi dostarczyć szczegółowe informacje biograficzne, zdjęcie w formacie cyfrowym i dziesięć odcisków palców. Takie dane umożliwiają niezawodną weryfikację tożsamości osób ubiegających się o wizę, ocenę możliwych przypadków nielegalnej migracji i zagrożeń bezpieczeństwa oraz zapobieganie wykorzystywaniu mniej rygorystycznych procedur wizowych, tzw. „visa shopping”.

Na przejściach granicznych lub na terytoriach państw członkowskich system VIS jest wykorzystywany do weryfikacji tożsamości posiadaczy wiz przez porównanie ich odcisków palców z odciskami palców zarejestrowanymi w systemie VIS. Proces ten gwarantuje, że osoba, która wnioskowała o wizę, jest tą samą osobą co osoba przekraczająca granicę. Funkcja wyszukiwania odcisków palców w systemie VIS

[29] Wszystkie państwa członkowskie UE z wyjątkiem Irlandii, Cypru i Chorwacji.
[30] Szwajcaria, Liechtenstein, Norwegia, Islandia.
[31] Zasada ta ma zostać zmieniona, jak przewiduje wniosek Komisji COM/2015/0670 dotyczący zmiany kodeksu granicznego Schengen.

umożliwia również identyfikację osoby, która wnioskowała o wizę w ciągu ostatnich pięciu lat i która może nie mieć przy sobie dokumentów tożsamości.

3. EURODAC

EURODAC (europejski system identyfikacji odcisków palców) zawiera odciski palców osób ubiegających się o azyl i obywateli państw trzecich, którzy nielegalnie przekroczyli granice zewnętrzne strefy Schengen. Jego głównym celem jest obecnie umożliwienia ustalenia, które państwo UE – zgodnie z rozporządzeniem dublińskim – odpowiada za rozpatrzenie wniosku o azyl. System ten jest dostępny na przejściach granicznych, lecz w odróżnieniu od systemów SIS i VIS nie jest systemem służącym do zarządzania granicami.

Odciski palców migrantów o nieuregulowanym statusie bezprawnie przybywających do UE są pobierane na przejściach granicznych. Następnie są one przechowywane w systemie EURODAC w celu weryfikacji tożsamości danej osoby, gdyby w przyszłości ubiegała się ona o azyl. Organy imigracyjne i policyjne również mogą porównywać dane dotyczące odcisków palców migrantów o nieuregulowanym statusie zidentyfikowanych w państwach członkowskich UE w celu weryfikacji, czy osoby te ubiegały się o azyl w innym państwie członkowskim. Organy ścigania i Europol również mogą korzystać z systemu EURODAC do celów zapobiegania poważnym przestępstwom lub atakom terrorystycznym oraz do ich wykrywania lub prowadzenia dochodzeń w ich sprawie.

Rejestracja odcisków palców osób ubiegających się o azyl lub migrantów o nieuregulowanym statusie w scentralizowanym systemie umożliwia wykrywanie i monitorowanie ich wtórnego przemieszczania się[32] po UE, dopóki nie zostanie złożony wniosek o objęcie ochroną międzynarodową lub dopóki nie zostanie wydana decyzja nakazująca powrót (w przyszłości z odpowiednim wpisem do SIS). Ogólnie mówiąc, wykrywanie i monitorowanie migrantów o nieuregulowanym statusie jest wymagane w celu zapewnienia ponownego wydania im dokumentów przez władze w ich krajach pochodzenia i tym samym usprawnia ich powrót.

4. Dane skradzionych lub utraconych dokumentów podróży (SLTD)

Baza danych skradzionych lub utraconych dokumentów podróży (SLTD) jest centralną bazą danych dotyczących paszportów i innych dokumentów podróży, które zostały zgłoszone do Interpolu przez organy je wystawiające jako skradzione lub utracone. Zawiera ona informacje dotyczące skradzionych blankietów paszportowych. Dokumenty podróży, których kradzież lub utratę zgłoszono organom państw uczestniczących w SIS, są rejestrowane zarówno w systemie SLTD, jak i w SIS. SLTD przechowuje również dane dotyczące dokumentów podróży, zarejestrowane przez państwa nieuczestniczące w SIS (Irlandia, Chorwacja, Cypr i państwa trzecie).

Jak określono w konkluzjach Rady z dni 9 i 20 listopada 2015 r. oraz we wniosku Komisji z dnia 15 grudnia 2015 r. dotyczącym rozporządzenia w sprawie ukierunkowanej modyfikacji kodeksu granicznego Schengen[33], dokumenty podróży wszystkich obywateli państw trzecich i osób korzystających z prawa do swobodnego przemieszczania się powinny być sprawdzane w bazie SLTD. Wszystkie punkty kontroli granicznej muszą być połączone z SLTD. Co więcej, wewnątrzkrajowe wyszukiwania w

[32] Na przykład uchodźcy przybywający do Grecji bez zamiaru ubiegania się o azyl w Grecji, lecz chcący podróżować drogą lądową dalej do innych państw członkowskich.

[33] COM(2015) 670 final: wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie nr 562/2006 (WE) w odniesieniu do wzmocnienia kontroli z użyciem odpowiednich baz danych na granicach zewnętrznych.

SLTD na potrzeby ochrony porządku publicznego przyniosłyby dodatkowe korzyści w zakresie bezpieczeństwa.

5. Dane pasażera przekazywane przed podróżą (API)

Celem API jest zebranie informacji dotyczących tożsamości danej osoby przed rozpoczęciem przez nią lotu do UE oraz identyfikacja migrantów o nieuregulowanym statusie w momencie ich przybycia. Dane API obejmują informacje zawarte w dokumencie podróży, takie jak pełne imię i nazwisko osoby podróżującej, datę urodzenia, narodowość, numer i rodzaj dokumentu podróży, oraz informacje dotyczące punktu kontroli granicznej, w którym przekroczono granicę (miejsce wyjazdu i wjazdu), a także informacje transportowe. Dane API odnoszące się do osoby pasażera zazwyczaj są gromadzone podczas odprawy.

W przypadku transportu drogą morską informacje wymagane przed przybyciem muszą zostać dostarczone – zgodnie z Konwencją o ułatwieniu międzynarodowego obrotu morskiego – 24 godziny przed planowanym przybyciem statku. Dyrektywa 2010/65/EU[34] zezwala na elektroniczne przekazywanie danych za pośrednictwem platformy elektronicznej łączącej system SafeSeaNet, e-Cło i inne systemy elektroniczne.

Nie istnieje żaden centralny system UE, który rejestruje dane API.

6. Systemy informacyjne Europolu

System informacyjny Europolu (EIS) jest scentralizowaną bazą danych zawierającą informacje w przestępstwach wykorzystywane do celów prowadzenia dochodzeń. Umożliwia on państwom członkowskim i Europolowi przechowywanie oraz przeszukiwanie danych dotyczących poważnej przestępczości i terroryzmu. Informacje przechowywane w systemie EIS obejmują dane dotyczące osób, dokumentów tożsamości, pojazdów, broni palnej, numerów telefonu, adresów e-mail, odcisków palców i DNA oraz informacje związane z cyberprzestępczością, które można ze sobą łączyć na różne sposoby, aby stworzyć bardziej szczegółową i ustrukturyzowaną charakterystykę przestępstwa. EIS wspomaga współpracę organów ścigania i nie jest dostępny dla organów kontroli granicznej.

Wymiana informacji odbywa się za pośrednictwem platformy SIENA[35], która jest siecią bezpiecznej łączności elektronicznej między Europolem, biurami łącznikowymi, jednostkami krajowymi Europolu, wyznaczonymi właściwymi organami (na przykład urzędami celnymi, biurami ds. odzyskiwania mienia itd.) i powiązanymi osobami trzecimi.

W maju 2017 r. wejdą w życie nowe ramy prawne Europolu. Ramy te przyczynią się do wzmocnienia zdolności operacyjnej Europolu do przeprowadzania analiz oraz lepszego wykrywania powiązań między dostępnymi informacjami.

7. Ramy z Prüm

Ramy z Prüm opierają się na wielostronnej umowie[36] między państwami członkowskimi, która umożliwia porównywanie profili DNA, odcisków palców i danych rejestracyjnych pojazdów (VRD). Koncepcja ta opiera się na możliwości połączenia systemu krajowego

[34] Dyrektywa Parlamentu Europejskiego i Rady 2010/65/UE z dnia 20 października 2010 r. w sprawie formalności sprawozdawczych dla statków wchodzących do lub wychodzących z portów państw członkowskich i uchylająca dyrektywę 2002/6/WE.

[35] Aplikacja sieci bezpiecznej wymiany informacji.

[36] Konwencja z Prüm z 2005 r. Konwencja ta została włączona do prawodawstwa UE w 2008 r. na mocy decyzji Rady 2008/615/WSiSW.

jednego państwa z systemami krajowymi wszystkich pozostałych państw członkowskich UE w celu umożliwienia zdalnej kontroli krzyżowej. W sytuacji, gdy wyszukiwanie daje trafienie w bazie danych innych państw członkowskich, szczegółowe informacje dotyczące tego trafienia są wymieniane za pośrednictwem dwustronnych mechanizmów wymiany.

8. Europejski system przekazywania informacji z rejestrów karnych (ECRIS)

ECRIS jest elektronicznym systemem wymiany informacji na temat wcześniejszych wyroków skazujących wydanych wobec konkretnej osoby przez sądy karne w Unii Europejskiej do celów prowadzenia postępowania karnego wobec tej osoby oraz, jeśli zezwala na to prawo krajowe, również do innych celów. Skazujące państwa członkowskie muszą przekazać państwu członkowskiemu, którego obywatelem jest dana osoba, informacje o wyrokach skazujących wydanych wobec jego obywatela. Państwo członkowskie, którego obywatelem jest dana osoba, musi przechowywać te informacje i tym samym może dostarczać na żądanie aktualne informacje z rejestru karnego swoich obywateli, niezależnie od tego, w którym państwie członkowskim UE wyroki skazujące zostały wydane.

ECRIS umożliwia również wymianę informacji dotyczących wyroków skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców. Organy centralne wyznaczone w każdym państwie członkowskim są punktami kontaktowymi w sieci ECRIS i wykonują zadania takie jak przekazywanie informacji z rejestrów karnych, ich przechowywanie, wnioskowanie o nie oraz ich udostępnianie.