KOMISJA
EUROPEJSKA

Strasburg, dnia 12.12.2017
COM(2017) 793 final

2017/0351 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniające decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399 i rozporządzenie (UE) 2017/2226

{SWD(2017) 473 final} - {SWD(2017) 474 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Kontekst wniosku

W ciągu ostatnich trzech lat UE doświadcza coraz częstszych przypadków nielegalnego przekraczania swojej granicy, a także ewoluujących i wciąż aktualnych zagrożeń dla bezpieczeństwa wewnętrznego, czego dowodem jest seria ataków terrorystycznych. Zgodnie z oczekiwaniami obywateli UE kontrole osób na granicach zewnętrznych i kontrole w ramach strefy Schengen powinny być skuteczne, umożliwiać efektywne zarządzanie migracją oraz przyczyniać się do bezpieczeństwa wewnętrznego. Wyzwania te doprowadziły do zwrócenia szczególnej uwagi na pilną potrzebę połączenia i kompleksowego wzmocnienia unijnych narzędzi informacyjnych służących zarządzaniu granicami i migracją oraz bezpieczeństwu.

Zarządzanie informacjami w UE może i musi stać się skuteczniejsze i wydajniejsze, przy pełnym poszanowaniu praw podstawowych, w szczególności prawa do ochrony danych osobowych, aby lepiej chronić granice zewnętrzne UE, poprawić zarządzanie migracją i zwiększyć bezpieczeństwo wewnętrzne z korzyścią dla wszystkich obywateli. Już obecnie na szczeblu UE funkcjonuje szereg systemów informacyjnych, a kolejne takie systemy są opracowywane, aby dostarczać funkcjonariuszom straży granicznej i organów ścigania oraz urzędnikom imigracyjnym odpowiednich informacji o osobach. Aby to wsparcie było skuteczne, informacje dostarczane za pośrednictwem systemów informacyjnych UE muszą być pełne, dokładne i rzetelne. W unijnej strukturze zarządzania informacją istnieją jednak niedoskonałości strukturalne. Władze krajowe muszą posługiwać się skomplikowanym układem systemów informacyjnych zarządzanych w różny sposób. Ponadto struktura zarządzania danymi dotyczącymi granic i bezpieczeństwa jest fragmentaryczna, gdyż informacje przechowywane są oddzielnie w niepowiązanych systemach. Sprawia to, że pewne dane pozostają nieuwzględnione. W rezultacie **poszczególne systemy informacyjne na szczeblu UE nie są obecnie interoperacyjne**, tzn. zdolne do wymiany danych i dzielenia się informacjami, tak aby władze i właściwi urzędnicy dysponowali informacjami, których potrzebują, w czasie i miejscu, w których ich potrzebują. Interoperacyjność systemów informacyjnych na szczeblu UE może znacznie przyczynić się do eliminacji obecnych niedociągnięć, które sprawiają, że osoby fizyczne, w tym osoby potencjalnie zaangażowane w działalność terrorystyczną, mogą być rejestrowane w różnych, niepowiązanych ze sobą bazach danych pod różnymi pseudonimami.

W kwietniu 2016 r. Komisja przedstawiła **komunikat pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”**[1], w którym wskazano kilka strukturalnych niedociągnięć związanych z systemami informacyjnymi[2]. Celem komunikatu z kwietnia 2016 r. było rozpoczęcie dyskusji na temat tego, jak dzięki systemom informacyjnym w Unii Europejskiej można jeszcze bardziej poprawić zarządzanie granicami i migracją oraz bezpieczeństwo wewnętrzne. Ze swojej strony **Rada** w podobny sposób wskazała na pilną potrzebę działań w tym zakresie. W czerwcu 2016 r. poparła ona **plan działania na rzecz intensyfikacji wymiany informacji**

[1] COM(2016) 205 z dnia 6 kwietnia 2016 r.

[2] (1) Niektóre z istniejących systemów informacyjnych mają nieoptymalne mechanizmy działania; (2) w unijnej strukturze zarządzania danymi istnieją luki informacyjne; (3) systemy informacyjne są zarządzane w różny sposób i tworzą skomplikowany układ; oraz (4) zarządzanie danymi dotyczącymi granic i bezpieczeństwa odbywa się w ramach fragmentarycznych struktur, a informacje przechowywane są oddzielnie w niepowiązanych systemach, co sprawia, że pewne dane pozostają nieuwzględnione.

i udoskonalenia zarządzania nimi, w tym na rzecz rozwiązań interoperacyjnych w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych[3]. Celem tego planu działania było wsparcie dochodzeń międzynarodowych i szybkie zapewnienie grupom zawodowym pierwszego kontaktu — takim jak funkcjonariusze policji i straży granicznej, prokuratorzy, urzędnicy imigracyjni i inni — kompleksowych, aktualnych i rzetelnych informacji umożliwiających efektywne działania i współpracę. **Parlament Europejski** także wezwał do działań w tym obszarze. W swojej rezolucji z lipca 2016 r. w sprawie programu prac Komisji na 2017 r.[4] Parlament Europejski wezwał Komisję do przedstawienia „wniosków dotyczących poprawy i dalszego rozwoju istniejących systemów informacyjnych, zmniejszania luk informacyjnych oraz dążenia do osiągnięcia interoperacyjności, a także wniosków dotyczących obowiązkowej wymiany informacji na szczeblu UE, wraz z niezbędnymi gwarancjami ochrony danych". W orędziu o stanie Unii wygłoszonym przez przewodniczącego Jeana-Claude'a Junckera we wrześniu 2016 r.[5] oraz w konkluzjach Rady Europejskiej z grudnia 2016 r.[6] podkreślono, jak istotna jest likwidacja niedociągnięć w zarządzaniu danymi oraz poprawa interoperacyjności istniejących systemów informacyjnych.

W czerwcu 2016 r. w ramach działań następczych w związku z komunikatem z kwietnia 2016 r. Komisja powołała **grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności**[7] w celu sprostania wyzwaniom prawnym, technicznym i operacyjnym związanym z poprawą interoperacyjności między centralnymi systemami informacyjnymi UE służącymi ochronie granic i zapewnianiu bezpieczeństwa, w tym w zakresie ich niezbędności, wykonalności technicznej, proporcjonalności i konsekwencji dla ochrony danych osobowych. **Sprawozdanie końcowe** wspomnianej grupy ekspertów wysokiego szczebla opublikowano w maju 2017 r.[8]. Określono w nim serię zaleceń mających na celu wzmocnienie i rozwój unijnych systemów informacyjnych i ich interoperacyjności. W pracach grupy ekspertów aktywnie uczestniczyli Agencja Praw Podstawowych Unii Europejskiej, Europejski Inspektor Ochrony Danych i Koordynator UE ds. Zwalczania Terroryzmu. Wszyscy oni wyrazili swoje poparcie, przyznając jednocześnie, że w dalszych pracach należy uwzględnić szersze kwestie związane z ochroną praw podstawowych i danych osobowych. Przedstawiciele Sekretariatu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego oraz Sekretariatu Generalnego Rady uczestniczyli w posiedzeniach grupy w charakterze obserwatorów. Grupa ekspertów stwierdziła, że **prace nad praktycznymi rozwiązaniami służącymi zapewnieniu interoperacyjności systemów informacyjnych są konieczne i wykonalne pod względem technicznym**, a rozwiązania te zasadniczo mogą zarówno przynieść korzyści operacyjne, jak i zostać ustanowione zgodnie z wymogami ochrony danych.

---

[3] Plan działania na rzecz intensyfikacji wymiany informacji i udoskonalenia zarządzania nimi, w tym na rzecz rozwiązań interoperacyjnych w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych z dnia 6 czerwca 2016 r. — 9368/1/16 REV 1.

[4] Rezolucja Parlamentu Europejskiego z dnia 6 lipca 2016 r. w sprawie strategicznych priorytetów programu prac Komisji na 2017 r. (2016/2773(RSP).

[5] Orędzie o stanie Unii (14.9.2016), https://ec.europa.eu/commission/state-union-2016_pl.

[6] Konkluzje Rady Europejskiej (15.12.2016), http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

[7] Decyzja Komisji z dnia 17 czerwca 2016 r. ustanawiająca grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności — 2016/C 257/03.

[8] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

W *siódmym sprawozdaniu z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa*[9], zgodnie ze sprawozdaniem i zaleceniami grupy ekspertów, Komisja określiła **nowe podejście do zarządzania danymi** dotyczącymi ochrony granic, bezpieczeństwa i zarządzania migracją zakładające pełną interoperacyjność wszystkich scentralizowanych systemów informacyjnych UE w dziedzinie bezpieczeństwa oraz zarządzania granicami i przepływami migracyjnymi, przy pełnym poszanowaniu praw podstawowych. Komisja ogłosiła zamiar podejmowania dalszych działań na rzecz stworzenia europejskiego portalu wyszukiwania, który umożliwiałby jednoczesne przeglądanie wszystkich stosownych systemów unijnych w dziedzinach bezpieczeństwa oraz zarządzania granicami i migracją, ewentualnie dzięki uproszczonym przepisom regulującym dostęp organów ścigania, a także opracowania z myślą o tych systemach wspólnego serwisu kojarzenia danych biometrycznych (obejmującego ewentualnie wyszukiwania na zasadzie „wynik/brak wyniku”[10]) i wspólnego repozytorium danych umożliwiających identyfikację. Ogłosiła ona zamiar przedstawienia, w możliwie najkrótszym terminie, wniosku ustawodawczego w sprawie interoperacyjności.

W konkluzjach Rady Europejskiej z czerwca 2017 r.[11] ponownie podkreślono potrzebę działania. Zgodnie z konkluzjami Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych z czerwca 2017 r.[12] Rada Europejska zachęciła Komisję do jak najszybszego sporządzenia projektu aktu ustawodawczego wprowadzającego w życie zalecenia grupy ekspertów wysokiego szczebla. Inicjatywa ta stanowi także odpowiedź na apel Rady o ustanowienie kompleksowych ram regulujących dostęp organów ścigania do różnych baz danych w obszarach sprawiedliwości i spraw wewnętrznych w celu większego uproszczenia tego dostępu oraz zapewnienia spójności, skuteczności i reakcji na potrzeby operacyjne[13]. W kontekście swojego programu prac na 2018 r.[14] Komisja ogłosiła, że do końca 2017 r. przedstawi wniosek w sprawie interoperacyjności systemów informacyjnych, aby wzmocnić działania na rzecz uczynienia społeczeństwa Unii Europejskiej bezpieczniejszym, przy pełnym poszanowaniu praw podstawowych.

- **Cele wniosku**

Zasadnicze cele niniejszej inicjatywy wynikają z określonych w Traktach celów, jakimi jest poprawa zarządzania granicami zewnętrznymi strefy Schengen i wniesienie wkładu w bezpieczeństwo wewnętrzne Unii Europejskiej. Ich podstawą są także strategiczne decyzje Komisji i odpowiednie konkluzje Rady (Europejskiej). Cele te opisano bardziej szczegółowo w Europejskim programie w zakresie migracji i wydanych w jego następstwie komunikatach, w tym w komunikacie dotyczącym utrzymania i wzmocnienia strefy Schengen i w sprawie[15]

---

9 COM(2017) 261 final.

10 Nowa koncepcja uwzględnienia ochrony prywatności już w fazie projektowania zawęża dostęp do wszystkich danych poprzez ograniczanie go do zwykłego powiadomienia „wynik/brak wyniku”, które wskazuje na obecność (lub brak obecności) danych.

11 Konkluzje Rady Europejskiej z dni 22–23 czerwca 2017 r.

12 Wyniki 3546. posiedzenia Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniach 8 i 9 czerwca 2017 r., 10136/17.

13 Komitet Stałych Przedstawicieli (Coreper) Rady po udzieleniu prezydencji Rady w dniu 2 marca 2017 r. mandatu do rozpoczęcia międzyinstytucjonalnych negocjacji w sprawie unijnego systemu wjazdu/wyjazdu uzgodnił projekt oświadczenia Rady wzywającego Komisję do przedstawienia wniosku dotyczącego kompleksowych ram regulujących dostęp organów ścigania do różnych baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych w celu jego większego uproszczenia oraz zapewnienia spójności, skuteczności i reakcji na potrzeby operacyjne (skrócony protokół nr 7177/17 z dnia 21.3.2017 r.).

14 COM(2017) 650 final.

15 COM(2017) 570 final.

Europejskiej agendy bezpieczeństwa[16] oraz w sprawozdaniach Komisji z prac i postępów w zakresie utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa[17].

Cele niniejszego wniosku, oparte w szczególności na komunikacie z kwietnia 2016 r. i ustaleniach grupy ekspertów wysokiego szczebla, są nieodłącznie związane z wymienionymi powyżej aktami.

Szczegółowe cele niniejszego wniosku są następujące:

1) zapewnienie, aby użytkownicy końcowi — a zwłaszcza funkcjonariusze straży granicznej i organów ścigania, urzędnicy imigracyjni i organy wymiaru sprawiedliwości — dysponowali **szybkim, sprawnym, systematycznym i kontrolowanym dostępem** do informacji, których potrzebują do wykonywania swoich zadań;

2) dostarczenie rozwiązania pozwalającego **wykrywać różne tożsamości** powiązane z tymi samymi danymi biometrycznymi, co służyłoby podwójnemu celowi poprawnej identyfikacji osób *podróżujących w dobrej wierze* oraz **zwalczania oszustw dotyczących tożsamości**;

3) ułatwienie **kontroli tożsamości obywateli państw trzecich** na terytorium państw członkowskich przez organy policji; oraz

4) ułatwienie i **usprawnienie dostępu organów ścigania** do systemów informacyjnych niezwiązanych ze ściganiem przestępstw na szczeblu UE, w razie potrzeby, w celach zapobiegania poważnym przestępstwom i terroryzmowi, prowadzenia w ich sprawie dochodzeń, ich wykrywania lub ścigania.

Obok głównych celów operacyjnych niniejszy wniosek przyczyni się także do:

- ułatwienia technicznego i operacyjnego **wdrożenia przez państwa członkowskie** istniejących i przyszłych nowych systemów informacyjnych;
- wzmocnienia i usprawnienia **warunków bezpieczeństwa danych i ochrony danych** regulujących poszczególne systemy; oraz
- poprawy i harmonizacji wymogów dotyczących **jakości danych** w poszczególnych systemach.

Ponadto wniosek obejmuje przepisy dotyczące ustanowienia uniwersalnego formatu wiadomości (UMF) jako standardu UE w zakresie rozwijania systemów informacyjnych w dziedzinach sprawiedliwości i spraw wewnętrznych oraz zarządzania nim, a także przewiduje ustanowienie centralnego repozytorium sprawozdawczo-statystycznego.

- **Zakres wniosku**

Wraz z bliźniaczym wnioskiem przedstawionym tego samego dnia niniejszy wniosek w sprawie interoperacyjności skupia się na systemach informacyjnych UE stworzonych z myślą o zapewnianiu bezpieczeństwa i kontroli granic i migracji, wykorzystywanych na

[16] COM(2015) 185 final.
[17] COM(2016) 230 final.

szczeblu centralnym, spośród których trzy już istnieją, jeden jest bliski opracowania, natomiast dwa pozostałe znajdują się na etapie wniosków będących przedmiotem dyskusji między współustawodawcami. Każdy z tych systemów ma własne cele, zadania, podstawy prawne, zasady, grupy użytkowników i kontekst instytucjonalny.

Trzy istniejące scentralizowane systemy informacyjne to jak dotąd:

- **System Informacyjny Schengen (SIS)**, o szerokim spektrum wpisów dotyczących osób (odmowy wjazdu lub pobytu, europejski nakaz aresztowania, osoby zaginione, pomoc w prowadzeniu postępowań sądowych, kontrole niejawne i kontrole szczególne) oraz przedmiotów (w tym zagubionych, skradzionych lub unieważnionych dokumentów tożsamości lub podróży)[18];
- system **Eurodac** zawierający dane daktyloskopijne osób ubiegających się o azyl oraz obywateli państw trzecich, którzy nielegalnie przekroczyli granicę zewnętrzną lub nielegalnie przebywają w państwie członkowskim; oraz
- **wizowy system informacyjny (VIS)** zawierający dane dotyczące wiz krótkoterminowych.

Oprócz tych istniejących systemów w latach 2016–2017 Komisja wystąpiła o utworzenie trzech nowych scentralizowanych systemów informacyjnych UE:

- **system wjazdu/wyjazdu (EES)**, dla którego właśnie uzgodniono podstawę prawną, który zastąpi obecny system ręcznego umieszczania odcisków pieczęci w paszportach i będzie elektronicznie rejestrować nazwisko, rodzaj dokumentu podróży, dane biometryczne oraz datę i miejsce wjazdu i wyjazdu obywateli państw trzecich odwiedzających strefę Schengen w celu krótkiego pobytu;
- proponowany **europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)**, który po przyjęciu będzie stanowić w znacznej mierze automatyczny system służący gromadzeniu i weryfikacji informacji dostarczanych przez obywateli państw trzecich zwolnionych z obowiązku wizowego przed odbyciem przez nich podróży do strefy Schengen; oraz
- proponowany **europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (system ECRIS-TCN)**, który ma stanowić elektroniczny system wymiany informacji dotyczących wcześniejszych wyroków skazujących wydanych przeciwko obywatelom państw trzecich przez sądy karne w UE.

Wspomnianych sześć systemów wzajemnie się uzupełnia oraz, z wyjątkiem Systemu Informacyjnego Schengen, skupia się wyłącznie na obywatelach państw trzecich. Systemy te wspomagają władze krajowe w zarządzaniu granicami, migracją, rozpatrywaniu wniosków wizowych i o azyl oraz w zwalczaniu przestępczości i terroryzmu. To ostatnie odnosi się przede wszystkim do SIS, który obecnie stanowi najszerzej wykorzystywany instrument dzielenia się informacjami przez organy ścigania.

Oprócz tych systemów informacyjnych, zarządzanych centralnie na szczeblu UE, zakres niniejszego wniosku obejmuje także bazę **Interpolu** zawierającą dane skradzionych lub

[18] W przedstawionych przez Komisję projektach rozporządzeń w sprawie SIS z grudnia 2016 r. zaproponowano dalsze jego rozszerzenie o decyzje nakazujące powrót i rozpytania kontrolne.

utraconych dokumentów podróży (baza danych SLTD), która zgodnie z przepisami kodeksu granicznego Schengen jest systematycznie przeglądana na granicach zewnętrznych UE, a także bazę danych TDAWN Interpolu. Obejmuje on także dane **Europolu**, jeśli są one istotne z punktu widzenia funkcjonowania proponowanego systemu ETIAS oraz pomocy państwom członkowskim w przeglądaniu danych dotyczących poważnych przestępstw i terroryzmu.

Krajowe systemy informacyjne i zdecentralizowane unijne systemy informacyjne pozostają poza zakresem niniejszej inicjatywy. W razie wykazania takiej potrzeby systemy zdecentralizowane, takie jak te działające na mocy ram z Prüm,[19] dyrektywy w sprawie danych dotyczących przelotu pasażera (PNR)[20] i dyrektywy w sprawie danych pasażera przekazywanych przed podróżą[21], mogą w przyszłości zostać powiązane z jednym lub większą liczbą elementów będących przedmiotem niniejszego wniosku[22].

Aby zapewnić poszanowanie rozróżnienia między kwestiami, z jednej strony, stanowiącymi rozwinięcie dorobku Schengen w zakresie granic i przepisów wizowych oraz, z drugiej strony, pozostałymi systemami związanymi z dorobkiem Schengen w zakresie współpracy policyjnej lub niezwiązanymi z dorobkiem Schengen, niniejszy wniosek dotyczy dostępu do wizowego systemu informacyjnego, Systemu Informacyjnego Schengen regulowanego obecnie rozporządzeniem (WE) nr 1987/2006, systemu wjazdu/wyjazdu oraz europejskiego systemu informacji o podróży oraz zezwoleń na podróż.

- **Elementy techniczne konieczne do osiągnięcia interoperacyjności**

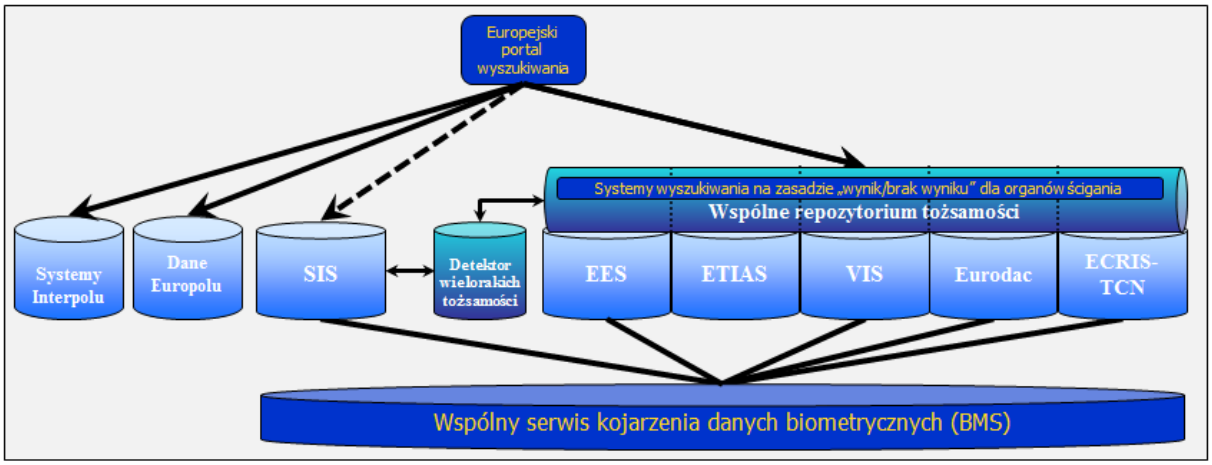
Aby osiągnąć cele niniejszego wniosku, należy ustanowić cztery elementy interoperacyjności:

- europejski portal wyszukiwania
- wspólny serwis kojarzenia danych biometrycznych
- wspólne repozytorium tożsamości
- moduł wykrywający multiplikację tożsamości

Każdy z tych elementów opisano szczegółowo w towarzyszącym niniejszemu wnioskowi dokumencie roboczym służb Komisji w sprawie oceny skutków.

Te cztery elementy wspólnie prowadzą do następującego rozwiązania w zakresie interoperacyjności:

[19] http://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.
[20] http://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1508936384641&uri=CELEX:32016L06 81.
[21] Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów.
[22] Podobnie jak w przypadku systemów celnych w swoich konkluzjach z czerwca 2017 r. Rada zachęciła Komisję do przeprowadzenia studium wykonalności, aby dodatkowo zbadać aspekty techniczne, operacyjne i prawne interoperacyjności między systemami zarządzania bezpieczeństwem i granicami oraz systemami celnymi, a także do przedstawienia swoich ustaleń i przedłożenia ich do dyskusji w Radzie do końca 2018 r.



Cele i funkcjonowanie tych czterech elementów można podsumować następująco:

1) **Europejski portal wyszukiwania** to element, który umożliwiłby jednoczesne przeglądanie różnych systemów (centralnego systemu informacyjnego Schengen (C.SIS), Eurodac, VIS, przyszłego EES, proponowanych systemów ETIAS i ECRIS-TCN, a także odpowiednich systemów Interpolu i danych Europolu) za pomocą danych dotyczących tożsamości (zarówno biograficznych, jak i biometrycznych). Zapewniłoby to użytkownikom systemów informacyjnych UE szybki, sprawny, efektywny, systematyczny i kontrolowany dostęp do wszystkich informacji koniecznych do wykonywania ich zadań.

   Wprowadzenie zapytania w europejskim portalu wyszukiwania niezwłocznie, w ciągu kilku sekund, doprowadziłoby do uzyskania informacji pochodzących z różnych systemów, do których użytkownik zgodnie z prawem ma dostęp. W zależności od celu zapytania i przysługujących praw dostępu europejski portal wyszukiwania byłby wyposażony w szczegółowe konfiguracje.

   Europejski portal wyszukiwania nie przetwarza nowych danych ani nie gromadzi żadnych danych; stanowiłby „pojedyncze okno" lub „pośrednika komunikatów" służącego przeglądaniu różnych systemów centralnych i sprawnemu pozyskiwaniu wymaganych informacji, przy pełnym poszanowaniu wymogów związanych z kontrolą dostępu i ochroną danych obowiązujących w systemach podstawowych. Europejski portal wyszukiwania ułatwiałby poprawne i dozwolone korzystanie z każdego z istniejących systemów informacyjnych, a także uczyniłby przeglądanie i korzystanie z tych systemów łatwiejszymi i tańszymi dla państw członkowskich, zgodnie z instrumentami prawnymi regulującymi te systemy.

2) **Wspólny serwis kojarzenia danych biometrycznych** umożliwiłby konsultację i porównywanie danych biometrycznych (odcisków palców i wizerunków twarzy) z różnych systemów centralnych (zwłaszcza SIS, Eurodac, VIS, przyszłego EES i proponowanego systemu ECRIS-TCN). Proponowany system ETIAS nie będzie zawierać danych biometrycznych, nie będzie zatem powiązany ze wspólnym serwisem kojarzenia danych biometrycznych.

Podczas gdy obecnie każdy istniejący system centralny (SIS, Eurodac, VIS) dysponuje specjalną, zastrzeżoną wyszukiwarką danych biometrycznych[23], wspólny serwis kojarzenia danych biometrycznych zapewniłby wspólną platformę jednoczesnego przeglądania i porównywania danych. Wspólny serwis kojarzenia danych biometrycznych przyniósłby znaczne korzyści w zakresie bezpieczeństwa, kosztów, obsługi technicznej i eksploatacji, ponieważ opierałby się wyłącznie na jednym elemencie technologicznym, nie zaś na pięciu różnych. Dane biometryczne (odciski palców i wizerunki twarzy) są przechowywane wyłącznie w systemach podstawowych. Wspólny serwis kojarzenia danych biometrycznych stwarzałby i zatrzymywał matematyczną reprezentację próbek biometrycznych (wzorzec), usuwałby jednak rzeczywiste dane, które w ten sposób byłyby zapisywane raz i przechowywane w jednej lokalizacji.

Wspólny serwis kojarzenia danych biometrycznych stanowiłby zasadniczy czynnik napędowy pomagający wykrywać powiązania między różnymi zestawami danych i różnymi tożsamościami przyjmowanymi przez tę samą osobę i zarejestrowanymi w różnych systemach centralnych. Bez wspólnego serwisu kojarzenia danych biometrycznych żaden z pozostałych trzech elementów nie będzie mógł funkcjonować.

3) **Wspólne repozytorium tożsamości** stanowiłoby wspólny element służący gromadzeniu danych biograficznych[24] i biometrycznych dotyczących tożsamości obywateli państw trzecich odnotowanych w systemach Eurodac, VIS, przyszłym EES oraz w proponowanych systemach ETIAS i ECRIS-TCN. Każdy z tych pięciu systemów centralnych rejestruje lub będzie rejestrować dane biograficzne konkretnych osób z określonych przyczyn. To się nie zmieni. Odpowiednie dane dotyczące tożsamości byłyby przechowywane we wspólnym repozytorium tożsamości, nadal jednak „należałyby" do odpowiednich systemów podstawowych, w których zostały zarejestrowane.

Wspólne repozytorium tożsamości nie będzie zawierało danych zgromadzonych w SIS. Złożona architektura techniczna SIS zawierająca kopie krajowe, częściowe kopie krajowe i ewentualne krajowe systemy kojarzenia danych biometrycznych sprawiłaby, że wspólne repozytorium tożsamości stałoby się nadmiernie skomplikowane w stopniu niewykonalnym z technicznego i finansowego punktu widzenia.

Zasadniczym celem repozytorium jest ułatwienie identyfikacji biograficznej obywateli państw trzecich. Przyspieszyłoby to operacje, poprawiło ich wydajność i zapewniło korzyści skali. Ustanowienie wspólnego repozytorium tożsamości jest konieczne, aby umożliwić skuteczne kontrole tożsamości obywateli państw trzecich, także na terytorium państw członkowskich. Ponadto dodanie do repozytorium funkcji „wynik/brak wyniku" umożliwiłoby sprawdzenie obecności (lub braku) danych w dowolnym z systemów objętych repozytorium za pomocą prostego powiadomienia o wyniku lub jego braku. W ten sposób wspólne repozytorium tożsamości pomogłoby też usprawnić dostęp organów ścigania do systemów informacyjnych niezwiązanych ze ściganiem przestępstw

[23] Powyższe wyszukiwarki danych biometrycznych są z technicznego punktu widzenia określane jako systemy automatycznej identyfikacji daktyloskopijnej (AFIS) lub systemy automatycznej identyfikacji biometrycznej (ABIS).

[24] Dane biograficzne, które można znaleźć w dokumentach podróży, to m.in.: nazwisko, imię, płeć, data urodzenia i numer dokumentu podróży. Nie obejmują one adresów, poprzednich nazwisk, danych biometrycznych itp.

przy jednoczesnym utrzymaniu wysokiej jakości zabezpieczeń ochrony danych (zob. część poświęconą dwuetapowemu podejściu do dostępu organów ścigania poniżej).

Spośród pięciu systemów, które miałyby zostać objęte wspólnym repozytorium tożsamości, przyszły EES oraz proponowane ETIAS i ECRIS-TCN to nowe systemy, które wciąż wymagają opracowania. Obecnie system Eurodac nie obejmuje danych biograficznych; takie rozszerzenie zostanie opracowane po przyjęciu nowej podstawy prawnej dla tego systemu. Obecnie system VIS zawiera dane biograficzne, jednak konieczne interakcje między VIS a przyszłym EES będą wymagały modernizacji aktualnego systemu VIS. Stworzenie wspólnego repozytorium tożsamości nastąpiłoby zatem we właściwym momencie. Nie będzie to w żaden sposób prowadzić do powielania istniejących danych. Od strony technicznej wspólne repozytorium tożsamości zostanie opracowane na bazie platformy EES/ETIAS.

4) **Moduł wykrywający multiplikację tożsamości** służyłby sprawdzaniu, czy konsultowane dane dotyczące tożsamości są obecne w więcej niż jednym z podłączonych do niego systemów. Moduł obejmuje systemy gromadzące dane dotyczące tożsamości we wspólnym repozytorium tożsamości (Eurodac, VIS, przyszły EES oraz proponowane systemy ETIAS i ECRIS-TCN) oraz SIS. Pozwoliłby on wykrywać multiplikację tożsamości powiązaną z tym samym zestawem danych biometrycznych, co służyłoby podwójnemu celowi poprawnej identyfikacji osób podróżujących w dobrej wierze oraz zwalczania oszustw dotyczących tożsamości.

Moduł wykrywający multiplikację tożsamości umożliwiłby ustalenie, czy różne nazwiska rzeczywiście należą do tej samej osoby. Jest to innowacja niezbędna do skutecznego rozwiązania problemu posługiwania się fałszywymi tożsamościami, który stanowi poważne naruszenie bezpieczeństwa. Moduł pokazywałby tylko te wpisy biograficzne dotyczące tożsamości, do których istnieją powiązania w różnych systemach centralnych. Takie powiązania byłyby wykrywane za pomocą wspólnego serwisu kojarzenia danych biometrycznych na podstawie danych biometrycznych i wymagałyby potwierdzenia lub odrzucenia przez organ, który zarejestrował te dane w systemie informacyjnym, który doprowadził do utworzenia danego powiązania. Aby pomóc uprawnionym użytkownikom modułu wykrywającego multiplikację tożsamości w realizacji tego zadania, system musiałby oznaczać zidentyfikowane powiązania za pomocą jednej z czterech kategorii:

- powiązanie żółte — możliwość istnienia różniących się tożsamości biograficznych należących do tej samej osoby;
- powiązanie białe — potwierdzenie, że różne tożsamości biograficzne należą do tej samej osoby podróżującej w dobrej wierze;
- powiązanie zielone — potwierdzenie, że różne osoby podróżującej w dobrej wierze mają tę samą tożsamość biograficzną;
- powiązanie czerwone — podejrzenie, że ta sama osoba bezprawnie korzysta z różnych tożsamości biograficznych.

Niniejszy wniosek opisuje procedury, które miałyby zostać wprowadzone w odniesieniu do powyższych kategorii. Tożsamość osób podróżujących w dobrej wierze, których sprawa dotyczy, należy jednoznacznie ustalić tak szybko, jak to tylko możliwe,

zmieniając powiązanie żółte w potwierdzone powiązanie białe lub zielone, aby zapewnić uniknięcie niepotrzebnych niedogodności. Jeśli z kolei analiza doprowadzi do potwierdzenia łącza czerwonego bądź zmiany powiązania żółtego w czerwone, należy podjąć odpowiednie działania.

- **Dwuetapowe podejście do dostępu organów ścigania do wspólnego repozytorium tożsamości**

Ściganie przestępstw określono jedynie jako drugorzędny lub pomocniczy cel systemów Eurodac, VIS, przyszłego EES i proponowanego systemu ETIAS. W rezultacie możliwość dostępu do danych przechowywanych w tych systemach na potrzeby ścigania przestępstw jest ograniczona. Organy ścigania mogą bezpośrednio przeglądać te systemy informacyjne niezwiązane ze ściganiem przestępstw jedynie w celach zapobiegania terroryzmowi i innym poważnym przestępstwom, prowadzenia w ich sprawie dochodzeń, ich wykrywania lub ścigania. Ponadto poszczególne systemy podlegają różnym warunkom dostępu i zabezpieczeniom, a niektóre z obecnie obowiązujących przepisów mogłyby spowalniać poparte przepisami korzystanie przez te organy z powyższych systemów. Ogólniej rzecz biorąc, zasada wcześniejszego wyszukiwania ogranicza możliwość przeglądania tych systemów przez organy państw członkowskich w uzasadnionych celach ścigania przestępstw, może zatem prowadzić do straconych szans na wykrycie potrzebnych informacji.

W komunikacie z kwietnia 2016 r. Komisja przyznała, że należy zoptymalizować funkcjonowanie istniejących narzędzi ścigania przestępstw przy jednoczesnym poszanowaniu wymogów w zakresie ochrony danych. Konieczność tę potwierdziły i podkreśliły państwa członkowskie i odpowiednie agencje w ramach grupy ekspertów wysokiego szczebla.

W powyższym kontekście, poprzez utworzenie wspólnego repozytorium tożsamości wyposażonego w tzw. funkcję „wynik/brak wyniku", niniejszy wniosek wprowadza możliwość zapewnienia dostępu do systemów EES, VIS, ETIAS i Eurodac za pomocą **dwuetapowego podejścia do przeglądania danych**. To dwuetapowe podejście nie wpływa na fakt, że ściganie przestępstw stanowi wyłącznie pomocniczy cel tych systemów, musi zatem podlegać rygorystycznym zasadom dostępu.

Na pierwszym etapie funkcjonariusz organu ścigania dokonywałby zapytania dotyczącego poszukiwanej osoby przy wykorzystaniu danych dotyczących jej tożsamości, danych jej dokumentu podróży lub danych biometrycznych, aby sprawdzić, czy jej dane są przechowywane we wspólnym repozytorium tożsamości. Jeśli takie dane byłyby obecne, funkcjonariusz otrzymałby **odpowiedź wskazującą, które systemy informacyjne UE zawierają dane** dotyczące tej osoby (**„wynik/brak wyniku"**). Funkcjonariusz nie miałby rzeczywistego dostępu do danych w żadnym z systemów podstawowych.

Na drugim etapie funkcjonariusz mógłby indywidualnie zwrócić się o dostęp do każdego systemu wskazanego jako zawierający dane, aby uzyskać pełne akta osobowe osoby będącej przedmiotem zapytania **zgodnie z obowiązującymi przepisami i procedurami ustanowionymi dla każdego systemu**. Dostęp w ramach etapu drugiego wymagałby uprzedniej autoryzacji, którą przyznawałby właściwy organ, oraz w dalszym ciągu — posiadania ID użytkownika i zalogowania się do systemu.

To nowe podejście stanowiłoby też wartość dodaną dla organów ścigania ze względu na **istnienie możliwych powiązań** w module wykrywającym multiplikację tożsamości. Moduł wspomagałby wspólne repozytorium tożsamości w identyfikacji istniejących powiązań, co zapewniłoby jeszcze dokładniejsze poszukiwania. Moduł wykrywający multiplikację tożsamości mógłby wskazywać, czy dana osoba jest znana **pod różnymi tożsamościami** w różnych systemach informacyjnych.

Dwuetapowe podejście do przeglądania danych jest szczególnie przydatne w przypadkach, w których osoba podejrzana, sprawca lub domniemana ofiara przestępstwa terrorystycznego **pozostają nieznani**. W istocie w tych przypadkach wspólne repozytorium tożsamości umożliwiłoby identyfikację systemu informacyjnego, w którym zidentyfikowano tę osobę, za pomocą tylko jednego wyszukiwania. W ten sposób obowiązujące obecnie warunki uprzednich wyszukiwań w krajowych bazach danych i wcześniejszego wyszukiwania w systemach automatycznej identyfikacji daktyloskopijnej innych państw członkowskich na mocy decyzji 2008/615/WSiSW („kontrole zgodne z kryteriami z Prüm") stałyby się zbędne.

Nowe dwuetapowe podejście do przeglądania danych **weszłoby w życie dopiero** po pełnym uruchomieniu wymaganych **elementów interoperacyjności**.

- **Dodatkowe elementy niniejszego wniosku wspierające elementy interoperacyjności**

1) Obok powyższych elementów niniejszy projekt rozporządzenia obejmuje też wniosek o ustanowienie **centralnego repozytorium sprawozdawczo-statystycznego**. Repozytorium to jest konieczne do tworzenia i przekazywania sprawozdań zawierających (anonimowe) dane statystyczne w celach związanych ze strategiami politycznymi, jak również w celach operacyjnych i związanych z jakością danych. Obecna praktyka gromadzenia danych statystycznych wyłącznie w pojedynczych systemach informacyjnych jest szkodliwa dla bezpieczeństwa danych i wydajności, nie umożliwia też korelacji danych zgromadzonych w różnych systemach.

   Centralne repozytorium sprawozdawczo-statystyczne zapewniłoby specjalne, oddzielne repozytorium anonimowych statystyk pobranych z systemów SIS, VIS, Eurodac, przyszłego EES, proponowanych systemów ETIAS i ECRIS-TCN, wspólnego repozytorium tożsamości, moduł wykrywający multiplikację tożsamości i wspólnego serwisu kojarzenia danych biometrycznych. Repozytorium zapewniłoby państwom członkowskim, Komisji (w tym Eurostatowi) i agencjom unijnym możliwość bezpiecznego przekazywania sprawozdań (regulowanego odpowiednimi instrumentami prawnymi).

   Opracowanie jednego repozytorium centralnego zamiast odrębnych repozytoriów dla każdego systemu prowadziłoby do obniżenia kosztów i wysiłków koniecznych do jego ustanowienia, funkcjonowania i obsługi technicznej. Zapewniłoby także wyższy poziom bezpieczeństwa danych, ponieważ dane byłyby przechowywane i podlegały kontroli dostępu w ramach jednego repozytorium.

2) Projekt rozporządzenia obejmuje także ustanowienie **uniwersalnego formatu wiadomości (UMF)** jako standardu wykorzystywanego na szczeblu UE, aby zarządzać interakcjami między różnymi systemami w sposób interoperacyjny, w tym systemami

opracowanymi i zarządzanymi przez eu-LISA. Do korzystania z tego standardu zachęca się także Europol i Interpol.

Standard UMF wprowadza wspólny i jednolity język techniczny służący opisywaniu i łączeniu elementów danych, zwłaszcza elementów związanych z osobami i dokumentami (podróży). Korzystanie z UMF przy opracowywaniu nowych systemów informacyjnych gwarantuje łatwiejszą integrację i interoperacyjność z innymi systemami, zwłaszcza w przypadku państw członkowskich, które muszą zbudować nowe interfejsy, aby komunikować się z tymi nowymi systemami. W związku z tym obowiązkowe korzystanie ze standardu UMF przy opracowywaniu nowych systemów można uznać za konieczny warunek wstępny dla wprowadzenia elementów interoperacyjności zaproponowanych w niniejszym rozporządzeniu.

Aby zapewnić pełne wdrożenie standardu UMF w całej UE, zaproponowano odpowiednią strukturę zarządzania. Komisja odpowiada za ustanawianie i opracowywanie standardu UMF w ramach procedury sprawdzającej wraz z państwami członkowskimi. W proces ten będą także zaangażowane agencje unijne i organy międzynarodowe państw stowarzyszonych w ramach Schengen uczestniczące w projektach UMF (takie jak eu-LISA, Europol i Interpol). Proponowana struktura zarządzania ma zasadnicze znaczenie dla UMF, aby umożliwić rozszerzanie i rozbudowę tego standardu przy jednoczesnym zagwarantowaniu maksymalnej użyteczności i stosowalności.

3) Niniejszy projekt rozporządzenia wprowadza ponadto koncepcje **zautomatyzowanych mechanizmów kontroli jakości danych** i wspólnych wskaźników jakości oraz zaznacza, że państwa członkowskie muszą zapewnić najwyższy poziom jakości danych przy przekazywaniu danych do tych systemów i korzystaniu z nich. Konsekwencją nie najwyższej jakości danych może być nie tylko brak możliwości identyfikacji poszukiwanych osób, lecz także naruszanie praw podstawowych niewinnych ludzi. Aby pokonać problemy wynikające z wprowadzania danych przez operatorów-ludzi, można zastosować automatyczne zasady walidacji, aby zapobiegać błędom operatorów. Celem jest automatyczna identyfikacja wprowadzonych danych wyglądających na niespójne lub nieprawidłowe, tak aby państwo członkowskie, z którego te dane pochodzą, mogło je sprawdzić i podjąć wszelkie konieczne środki naprawcze. Działania te będą uzupełniać regularne sprawozdania z jakości danych sporządzane przez eu-LISA.

- **Konsekwencje dla innych instrumentów prawnych**

Wraz z bliźniaczym wnioskiem niniejszy projekt rozporządzenia wprowadza innowacje, które będą wymagały zmian w następujących instrumentach prawnych:

- rozporządzenie (UE) 2016/399 (kodeks graniczny Schengen)
- rozporządzenie (UE) 2017/2226 (rozporządzenie w sprawie EES)
- rozporządzenie (WE) nr 767/2008 (rozporządzenie w sprawie VIS)
- decyzja Rady 2004/512/WE (decyzja w sprawie VIS)
- decyzja Rady 2008/633/WSiSW (decyzja w sprawie dostępu organów ścigania do VIS)
- [rozporządzenie w sprawie ETIAS]
- [rozporządzenie w sprawie Eurodac]

- [rozporządzenia w sprawie SIS]
- [rozporządzenie w sprawie ECRIS-TCN, w tym odpowiednie przepisy rozporządzenia (UE) 2016/1624 (rozporządzenie w sprawie Europejskiej Straży Granicznej i Przybrzeżnej)]
- [rozporządzenie w sprawie eu-LISA]

Niniejszy wniosek i jego bliźniaczy wniosek obejmują szczegółowe przepisy dotyczące koniecznych zmian w instrumentach prawnych, które obecnie stanowią stabilne teksty przyjęte przez współustawodawców: w kodeksie granicznym Schengen, rozporządzeniu w sprawie EES, rozporządzeniu w sprawie VIS, decyzji Rady 2008/633/WSiSW i decyzji Rady 2004/512/WE.

Pozostałe wymienione instrumenty (rozporządzenia w sprawie systemów ETIAS, Eurodac, SIS i ECRIS/TCN oraz eu-LISA) znajdują się obecnie na etapie negocjacji w Parlamencie Europejskim i Radzie. W przypadku tych instrumentów na obecnym etapie nie jest zatem możliwe określenie koniecznych zmian. Komisja przedstawi takie poprawki dla każdego z tych instrumentów w ciągu dwóch tygodni od osiągnięcia porozumienia politycznego w sprawie odpowiednich projektów rozporządzeń.

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

Niniejszy wniosek stanowi część szerszego procesu zapoczątkowanego w kwietniu 2016 r. przez komunikat pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” oraz przez następujące po nim prace grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności. Zmierza on do osiągnięcia następujących trzech celów:

a) wzmocnienia i maksymalizacji korzyści wynikających **z istniejących systemów informacyjnych**;

b) eliminacji luk informacyjnych przez ustanawianie nowych systemów informacyjnych;

c) wzmocnienia interoperacyjności między tymi systemami.

W związku z pierwszym celem Komisja przyjęła w grudniu 2016 r. wnioski w sprawie dalszego wzmocnienia istniejącego Systemu Informacyjnego Schengen (SIS)[25]. Jeśli chodzi o system Eurodac, w następstwie wniosku Komisji z maja 2016 r.[26] przyspieszono negocjacje w sprawie zmienionej podstawy prawnej. Wniosek w sprawie nowej podstawy prawnej wizowego systemu informacyjnego (VIS) także jest w przygotowaniu i zostanie przedłożony w drugim kwartale 2018 r.

Jeśli chodzi o drugi cel, negocjacje w sprawie wniosku Komisji z kwietnia 2016 r. na rzecz ustanowienia systemu wjazdu/wyjazdu (EES)[27] zakończono już w lipcu 2017 r., gdy współustawodawcy osiągnęli porozumienie polityczne, potwierdzone przez Parlament Europejski w październiku 2017 r. i przyjęte formalnie przez Radę w listopadzie 2017 r. Odpowiednia podstawa prawna wejdzie w życie w grudniu 2017 r. Negocjacje dotyczące

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.

wniosku z listopada 2016 r. w sprawie ustanowienia europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)[28] rozpoczęły się i zgodnie z oczekiwaniami mają się zakończyć w nadchodzących miesiącach. W czerwcu 2017 r. Komisja wystąpiła z wnioskiem w sprawie podstawy prawnej w celu eliminacji innej luki informacyjnej: europejskiego systemu przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (system ECRIS-TCN)[29]. Ponownie współustawodawcy wskazali, że zamierzają szybko przyjąć tę podstawę prawną.

Niniejszy wniosek służy także realizacji trzeciego celu wskazanego w komunikacie z kwietnia 2016 r.

- **Spójność z innymi politykami Unii w obszarze wymiaru sprawiedliwości i spraw wewnętrznych**

Niniejszy wniosek wraz z jego bliźniaczym wnioskiem służy realizacji Europejskiego programu w zakresie migracji i wydanych w jego następstwie komunikatów, w tym komunikatu dotyczącego utrzymania i wzmocnienia strefy Schengen[30], Europejskiej agendy bezpieczeństwa[31] i sprawozdań Komisji z prac i postępów w zakresie utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa[32], oraz jest z nimi zgodny. Jest on spójny z pozostałymi politykami Unii, a zwłaszcza z następującymi:

- Bezpieczeństwo wewnętrzne: jak podkreślono w Europejskiej agendzie bezpieczeństwa, wspólne wysokie standardy zarządzania granicami to podstawa zapobiegania przestępczości transgranicznej i terroryzmowi. Niniejszy wniosek przyczynia się do osiągnięcia wysokiego poziomu bezpieczeństwa wewnętrznego poprzez zapewnienie władzom szybkiego, sprawnego, systematycznego i kontrolowanego dostępu do wymaganych przez nie informacji.
- Azyl: wniosek obejmuje system Eurodac jako jeden z unijnych systemów centralnych, które mają zostać objęte interoperacyjnością.
- Zarządzanie granicami zewnętrznymi i bezpieczeństwo: wniosek wzmacnia systemy SIS i VIS, które przyczyniają się do skutecznej kontroli unijnych granic zewnętrznych, a także wspomagają przyszły system EES oraz proponowane systemy ETIAS i ECRIS-TCN.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Główną podstawę prawną wniosku stanowią następujące artykuły Traktatu o funkcjonowaniu Unii Europejskiej: art. 16 ust. 2, art. 74, art. 77 ust. 2 lit. a), b), d) i e).

Zgodnie z art. 16 ust. 2 Unia jest uprawniona do przyjmowania środków na rzecz ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasad dotyczących swobodnego

[28] COM(2016) 731 final.
[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.
[32] COM(2016) 230 final.

przepływu takich danych. Na mocy art. 74 Rada może przyjmować środki w celu zapewnienia współpracy administracyjnej między właściwymi służbami państw członkowskich w dziedzinach wymiaru sprawiedliwości, wolności i bezpieczeństwa. Na mocy art. 77 ust. 2 lit. a), b), d) i e) Parlament Europejski i Rada mogą przyjmować środki dotyczące odpowiednio wspólnej polityki w zakresie wiz i innych dokumentów uprawniających do krótkiego pobytu, kontroli, którym podlegają osoby przekraczające granice zewnętrzne, wszelkich środków niezbędnych dla stopniowego wprowadzania zintegrowanego systemu zarządzania granicami zewnętrznymi oraz braku jakiejkolwiek kontroli osób, niezależnie od ich obywatelstwa, przy przekraczaniu przez nie granic wewnętrznych.

- **Pomocniczość**

Swoboda przemieszczania się w ramach UE wymaga, aby granice zewnętrzne Unii były skutecznie zarządzane w celu zapewniania bezpieczeństwa. Państwa członkowskie uzgodniły zatem, że wspólnie stawią czoła tym wyzwaniom, przede wszystkim poprzez przekazywanie informacji za pośrednictwem scentralizowanych unijnych systemów informacyjnych w dziedzinach wymiaru sprawiedliwości i spraw wewnętrznych. Potwierdzają to liczne konkluzje przyjęte zarówno przez Radę Europejską, jak i Radę, zwłaszcza od 2015 r.

Brak kontroli granic wewnętrznych wymaga racjonalnego zarządzania granicami zewnętrznymi strefy Schengen, w ramach której każde państwo członkowskie lub państwo stowarzyszone w ramach Schengen ma obowiązek kontrolować granicę zewnętrzną w imieniu pozostałych państw strefy Schengen. W rezultacie żadne państwo członkowskie nie może samo rozwiązać problemu nielegalnej migracji i przestępczości transgranicznej. Obywatele państw trzecich, którzy przekraczają granicę strefy bez wewnętrznych kontroli granicznych, mogą swobodnie w ramach niej podróżować. W strefie bez granic wewnętrznych zwalczanie nielegalnej imigracji i przestępczości międzynarodowej oraz terroryzmu, w tym przez wykrywanie oszustw dotyczących tożsamości, należy prowadzić wspólnie i może być z powodzeniem realizowane jedynie na szczeblu UE.

Podstawowe wspólne systemy informacyjne na szczeblu UE już zostały wprowadzone lub są w trakcie wprowadzania. Zwiększenie interoperacyjności między tymi systemami informacyjnymi nieodłącznie wiąże się z działaniami na szczeblu UE. Zasadniczym elementem wniosku jest poprawa wydajności scentralizowanych systemów zarządzanych przez eu-LISA oraz ich wykorzystywanie. Ze względu na skalę, skutki i oddziaływanie przewidywanych działań te podstawowe cele można skutecznie i systematycznie osiągnąć tylko na szczeblu UE.

- **Proporcjonalność**

Jak szczegółowo wyjaśniono w ocenie skutków towarzyszącej proponowanemu rozporządzeniu, decyzje polityczne zawarte w niniejszym wniosku należy uznać za proporcjonalne. Nie wykraczają one poza to, co jest konieczne do osiągnięcia uzgodnionych celów.

Europejski portal wyszukiwania stanowi narzędzie konieczne do wzmocnienia zgodnego z prawem użytkowania istniejących i przyszłych systemów informacyjnych UE. Oddziaływanie portalu w zakresie przetwarzania danych jest bardzo ograniczone. Nie gromadzi on żadnych danych z wyjątkiem informacji o różnych profilach użytkowników portalu oraz o tym, do jakich systemów danych i informacji mają oni dostęp, a także śledzi sposób, w jaki z nich korzystają, za pomocą zapisów w rejestrze. Rola europejskiego portalu wyszukiwania jako pośrednika komunikatów oraz czynnika umożliwiającego i ułatwiającego

korzystanie z systemów jest proporcjonalna, konieczna i ograniczona, jeśli chodzi o wyszukiwania i prawa dostępu na mocy mandatów określonych w podstawach prawnych dotyczących systemów informacyjnych oraz we wniosku dotyczącym rozporządzenia w sprawie interoperacyjności.

Wspólny serwis kojarzenia danych biometrycznych jest konieczny dla funkcjonowania europejskiego portalu wyszukiwania, wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości, a także ułatwia korzystanie z istniejących i przyszłych odpowiednich systemów informacyjnych UE oraz ich obsługę techniczną. Jego funkcje umożliwiają dokonywanie wyszukiwań danych biometrycznych z różnych źródeł w wydajny, sprawny i systematyczny sposób. Dane biometryczne są przechowywane i zatrzymywane w systemach podstawowych. Wspólny serwis kojarzenia danych biometrycznych stwarza wzorce, nie będzie jednak zawierał rzeczywistych wizerunków. Dane będą zatem zapisywane tylko raz i przechowywane w jednej lokalizacji.

Wspólne repozytorium tożsamości jest konieczne do osiągnięcia celu poprawnej identyfikacji obywatela państwa trzeciego, np. podczas kontroli tożsamości w strefie Schengen. Wspiera ono także funkcjonowanie modułu wykrywającego multiplikację tożsamości, stanowi zatem element konieczny do osiągnięcia podwójnego celu ułatwienia kontroli tożsamości osób podróżujących w dobrej wierze i zwalczania oszustw dotyczących tożsamości. Dostęp do repozytorium w tym celu ogranicza się do tych użytkowników, którzy potrzebują tych informacji do wykonywania swoich zadań (co wymaga, aby kontrole te stały się nowym pomocniczym celem systemów Eurodac, VIS, przyszłego systemu EES oraz proponowanych systemów ETIAS i ECRIS-TCN). Przetwarzanie danych ściśle ogranicza się do tego, co jest potrzebne do osiągnięcia tego celu, należy też ustanowić odpowiednie zabezpieczenia, aby zapewnić poszanowanie praw dostępu oraz ograniczenie do minimum danych przechowywanych we wspólnym repozytorium tożsamości. Aby zapewnić minimalizację danych i unikanie nieuzasadnionego ich powielania, w repozytorium znajdują się dane biograficzne z każdego z systemów podstawowych — przechowywane, dodawane, modyfikowane i usuwane zgodnie z odpowiednią podstawą prawną — ale bez ich kopiowania. Warunki zatrzymywania danych są w pełni spójne z przepisami w tym zakresie obowiązującymi wobec podstawowych systemów informacyjnych zawierających dane dotyczące tożsamości.

Moduł wykrywający multiplikację tożsamości jest konieczny, aby zapewnić rozwiązanie służące do wykrywania multiplikacji tożsamości, w podwójnym celu, jakim jest ułatwienie kontroli tożsamości osób podróżujących w dobrej wierze i zwalczanie oszustw dotyczących tożsamości. Będzie on zawierał powiązania między osobami obecnymi w więcej niż jednym centralnym systemie informacyjnym, w zakresie ściśle ograniczonym do danych potrzebnych do weryfikacji, czy dana osoba jest zgodnie lub niezgodnie z prawem zarejestrowana pod różnymi tożsamościami biograficznymi w różnych systemach, a także do wyjaśnienia sytuacji, w których dwie osoby o takich samych danych biograficznych mogą nie być tą samą osobą. Przetwarzanie danych za pomocą modułu wykrywającego multiplikację tożsamości i wspólnego serwisu kojarzenia danych biometrycznych w celu powiązania akt osobowych w poszczególnych systemach ogranicza się do absolutnego minimum. Moduł będzie zawierać zabezpieczenia przed potencjalną dyskryminacją lub nieprzychylnymi decyzjami w sprawie osób posługujących się różnymi tożsamościami w sposób zgodny z prawem.

- **Wybór instrumentu**

Wniosek dotyczy rozporządzenia Parlamentu Europejskiego i Rady. Akt prawny będący przedmiotem wniosku dotyczy bezpośrednio działania centralnych systemów informacyjnych

UE związanych z ochroną granic i bezpieczeństwem, z których każdy został lub zostanie utworzony na mocy rozporządzeń. Podobnie na mocy niniejszego rozporządzenia ustanowiona zostaje agencja eu-LISA, która będzie odpowiadać za projektowanie i rozwój tych elementów, a w przyszłości także za zarządzanie nimi. Rozporządzenie stanowi zatem właściwy instrument w tym celu.

3. WYNIKI KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

• Konsultacje publiczne

W ramach przygotowań do sporządzenia niniejszego wniosku Komisja przeprowadziła w lipcu 2017 r. konsultacje publiczne, aby zebrać opinie zainteresowanych stron na temat interoperacyjności. W ramach tych konsultacji uzyskano 18 odpowiedzi od różnego rodzaju zainteresowanych stron, w tym od rządów państw członkowskich, organizacji sektora prywatnego i innych, np. NGO i ośrodków analitycznych, oraz od obywateli prywatnych[33]. Ogólnie rzecz biorąc, opowiedziano się w nich zasadniczo za podstawowymi zasadami zawartymi w niniejszym wniosku w sprawie interoperacyjności. Znaczna większość respondentów zgodziła się, że w ramach konsultacji poprawnie zidentyfikowano problemy, a cele, do których osiągnięcia dąży pakiet dotyczący interoperacyjności, są właściwe. W szczególności respondenci uznali, że opcje przedstawione w dokumencie konsultacyjnym:

- pomogłyby pracownikom w terenie w uzyskaniu dostępu do potrzebnych im informacji;
- prowadziłyby do uniknięcia powielania danych, ograniczenia zjawiska pokrywania się danych i zwróciły uwagę na niespójności w danych;
- umożliwiłyby rzetelniejszą identyfikację osób, w tym osób o więcej niż jednej tożsamości, oraz ograniczyły oszustwa dotyczące tożsamości.

Wyraźna większość respondentów poparła każdą z proponowanych opcji i uznała je za konieczne do osiągnięcia celów tej inicjatywy, podkreślając w swoich odpowiedziach potrzebę solidnych i jasnych środków ochrony danych, zwłaszcza w związku z dostępem do informacji przechowywanych w systemach i zatrzymywaniem danych, oraz potrzebę, aby dane w systemach były aktualne i wysokiej jakości, a także zapotrzebowanie na środki, które to umożliwią.

Wszystkie zgłoszone uwagi wzięto pod uwagę przy sporządzaniu niniejszego wniosku.

• Badanie Eurobarometru

W czerwcu 2017 r. przeprowadzono specjalne badanie Eurobarometru[34], które wykazało szerokie poparcie społeczeństwa dla unijnej strategii w dziedzinie udostępniania informacji na szczeblu UE w celu zwalczania przestępczości i terroryzmu: niemal wszyscy respondenci (92 %) zgodzili się, że władze krajowe powinny udostępniać informacje władzom innych państw członkowskich, aby wspomagać walkę z przestępczością i terroryzmem.

---

[33] Dalsze szczegóły zawarto streszczeniu sprawozdania załączonym do oceny skutków.

[34] *Sprawozdanie Eurobarometru dotyczące europejskich postaw w stosunku do bezpieczeństwa* analizuje wyniki specjalnego badania opinii publicznej Eurobarometru (464b) dotyczącego ogólnej świadomości, doświadczeń i postrzegania bezpieczeństwa wśród obywateli. Badanie przeprowadziła sieć TNS Political & Social w 28 państwach członkowskich w dniach 13–26 czerwca 2017 r. Przeprowadzono rozmowy z ok. 28 093 obywatelami UE reprezentującymi różne kategorie społeczne i demograficzne.

Zdecydowana większość respondentów (69 %) wyraziła opinię, że policja i inne krajowe organy ścigania powinny udostępniać informacje pozostałym państwom UE w sposób systematyczny. We wszystkich państwach członkowskich większość respondentów uznała, że informacje należy udostępniać we wszystkich przypadkach.

- **Prace grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności**

Jak już wskazano we wstępie, niniejszy wniosek opiera się na zaleceniach **grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności**[35]. Grupę tę powołano w czerwcu 2016 r. w celu sprostania wyzwaniom prawnym, technicznym i operacyjnym związanym z dostępnymi możliwościami służącymi osiągnięciu interoperacyjności między centralnymi systemami UE służącymi ochronie granic i bezpieczeństwa. Grupa przyjęła szeroką i kompleksową perspektywę w odniesieniu do struktury zarządzania danymi na potrzeby zarządzania granicami i ścigania przestępstw, także z uwzględnieniem odpowiednich funkcji, obowiązków i systemów przeznaczonych dla organów celnych.

Grupa składa się z ekspertów z państw członkowskich, państw stowarzyszonych w ramach Schengen oraz ekspertów z agencji unijnych, eu-LISA, Europolu, Europejskiego Urzędu Wsparcia w dziedzinie Azylu, Europejskiej Agencji Straży Granicznej i Przybrzeżnej oraz Agencji Praw Podstawowych UE. W pracach grupy jako pełnoprawni członkowie uczestniczyli również Koordynator UE ds. Zwalczania Terroryzmu oraz Europejski Inspektor Ochrony Danych. Ponadto w posiedzeniach grupy uczestniczyli w charakterze obserwatorów przedstawiciele Sekretariatu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego oraz Sekretariatu Generalnego Rady.

Sprawozdanie końcowe grupy ekspertów wysokiego szczebla opublikowano w maju 2017 r.[36]. Podkreślono w nim potrzebę działania w celu eliminacji niedoskonałości strukturalnych wskazanych w komunikacie z kwietnia 2016 r. Określono serię zaleceń mających na celu wzmocnienie i rozwój unijnych systemów informacyjnych i interoperacyjności. Grupa ta stwierdziła, że **prace nad europejskim portalem wyszukiwania, wspólnym serwisem kojarzenia danych biometrycznych i wspólnym repozytorium tożsamości, jako rozwiązaniami służącymi zapewnieniu interoperacyjności, są konieczne i wykonalne pod względem technicznym** oraz zasadniczo mogą zarówno przynieść korzyści operacyjne, jak i zostać ustanowione zgodnie z wymogami ochrony danych. Grupa zaleciła także rozważenie jako dodatkowej możliwości wprowadzenia dwuetapowego podejścia do dostępu organów ścigania opartego na funkcji „wynik/brak wyniku".

Projekt rozporządzenia stanowi także odpowiedź na zalecenia grupy ekspertów wysokiego szczebla w sprawie jakości danych, uniwersalnego formatu wiadomości (UMF) oraz ustanowienia „hurtowni danych" (przedstawionej tu jako centralne repozytorium sprawozdawczo-statystyczne).

Czwarty element interoperacyjności zaproponowany w niniejszym rozporządzeniu (moduł wykrywający multiplikację tożsamości) nie został wskazany przez grupę ekspertów

[35] Decyzja Komisji z dnia 17 czerwca 2016 r. ustanawiająca grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności — 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

wysokiego szczebla, lecz stanowi wynik dodatkowej analizy technicznej i oceny proporcjonalności przeprowadzonych przez Komisję.

- **Badania techniczne**

W ramach przygotowań do sporządzenia niniejszego wniosku zlecono trzy badania. Na zlecenie Komisji firma Unisys sporządziła sprawozdanie ze studium wykonalności europejskiego portalu wyszukiwania. Agencja eu-LISA zleciła firmie Gartner (we współpracy z firmą Unisys) sporządzenie sprawozdania technicznego mającego ułatwić opracowywanie wspólnego serwisu kojarzenia danych biometrycznych. Firma PWC sporządziła na zlecenie Komisji sprawozdanie techniczne dotyczące wspólnego repozytorium tożsamości.

- **Ocena skutków**

Niniejszy wniosek jest poparty oceną skutków przedstawioną w towarzyszącym dokumencie roboczym służb Komisji SWD(2017) 473.

W dniu 6 grudnia 2017 r. Rada ds. Kontroli Regulacyjnej dokonała przeglądu projektu oceny skutków na posiedzeniu i w dniu 8 grudnia przedstawiła swoją opinię (pozytywną z zastrzeżeniami), podając, że ocena skutków powinna zostać skorygowana w sposób uwzględniający zalecenia Rady w konkretnych sprawach. Te ostatnie wiązały się przede wszystkim z dodatkowymi środkami w ramach preferowanej opcji służącymi usprawnieniu istniejących praw dostępu użytkowników końcowych do danych zawartych w systemach informacyjnych UE oraz zawierały przykłady odpowiednich zabezpieczeń związanych z ochroną danych i praw podstawowych. Druga istotna uwaga dotyczyła objaśnienia włączenia Systemu Informacyjnego Schengen w ramach opcji 2, w tym jego efektywności i kosztów, aby ułatwić porównywanie tej opcji z preferowaną opcją 3. Komisja zaktualizowała swoją ocenę skutków w odpowiedzi na te główne uwagi oraz aby uwzględnić szereg innych uwag wymienionej wyżej rady.

W ocenie skutków oceniono, czy i w jaki sposób każdy ze zidentyfikowanych celów można osiągnąć za pomocą jednego lub większej liczby elementów technicznych zidentyfikowanych przez grupę ekspertów wysokiego szczebla i w późniejszej analizie. Tam gdzie to było konieczne przeanalizowano też warianty potrzebne do spełnienia tych celów, z poszanowaniem ram ochrony danych. Wnioski z oceny skutków były następujące:

- aby osiągnąć cel, jakim jest zapewnienie uprawnionym użytkownikom szybkiego, sprawnego, systematycznego i kontrolowanego dostępu do odpowiednich systemów informacyjnych, należy utworzyć europejski portal wyszukiwania, oparty na wspólnym serwisie kojarzenia danych biometrycznych uwzględniający wszystkie bazy danych;
- aby osiągnąć cel, jakim jest ułatwienie kontroli tożsamości obywateli państw trzecich na terytorium państw członkowskich przez właściwie uprawnionych urzędników, należy utworzyć wspólne repozytorium tożsamości, zawierające minimalny zestaw danych umożliwiających identyfikację i opierające się na tym samym wspólnym serwisie kojarzenia danych biometrycznych;
- aby osiągnąć cel, jakim jest wykrywanie multiplikacji tożsamości powiązanych z tym samym zestawem danych biometrycznych, służący zarówno ułatwieniu kontroli tożsamości osób podróżujących w dobrej wierze, jak i zwalczaniu oszustw dotyczących tożsamości, należy utworzyć moduł wykrywający multiplikację

tożsamości, zawierający powiązania między różnymi tożsamościami zarejestrowanymi w różnych systemach;

- aby osiągnąć cel, jakim jest ułatwienie i usprawnienie dostępu organów ścigania do systemów informacyjnych niezwiązanych ze ściganiem przestępstw w celach zapobiegania poważnym przestępstwom i terroryzmowi, prowadzenia w ich sprawach dochodzeń, wykrywania ich i ścigania, do wspólnego repozytorium tożsamości należy wprowadzić funkcję „wynik/brak wyniku".

Ponieważ wszystkie cele muszą zostać spełnione, **pełnym rozwiązaniem jest połączenie europejskiego portalu wyszukiwania, wspólnego repozytorium tożsamości (z oznaczeniem „wynik/brak wyniku") i modułu wykrywającego multiplikację tożsamości, z których wszystkie opierałyby się na wspólnym serwisie kojarzenia danych biometrycznych**.

Najważniejsze pozytywne oddziaływanie polegałoby na poprawie zarządzania granicami i zwiększeniu bezpieczeństwa wewnętrznego w Unii Europejskiej. Nowe elementy usprawnią i przyspieszą dostęp organów krajowych do wymaganych informacji oraz identyfikację obywateli państw trzecich. Umożliwią one władzom wykrywanie wzajemnych powiązań między już istniejącymi, wymaganymi informacjami o osobach podczas odpraw granicznych, rozpatrywania wniosków o wizy lub azyl oraz w pracy policji. Umożliwi to dostęp do informacji mogących pomagać w podejmowaniu rzetelnych decyzji, czy to w przypadku dochodzeń w sprawie poważnych przestępstw i przestępstw terrorystycznych, czy decyzji w dziedzinie migracji i azylu. Choć wnioski te nie dotyczą bezpośrednio obywateli UE (proponowane środki skupiają się głównie na obywatelach państw trzecich, których dane są zarejestrowane w którymś ze scentralizowanych systemów informacyjnych UE), to oczekuje się, że zwiększą one zaufanie społeczeństwa dzięki zapewnieniu, że ich konstrukcja i stosowanie poprawią bezpieczeństwo obywateli Unii.

Bezpośrednie skutki finansowe i gospodarcze wniosku będą się ograniczać do zaprojektowania, opracowania i funkcjonowania nowych urządzeń. Koszty te zostaną pokryte z budżetu UE i przez organy państw członkowskich korzystające z systemów. Oddziaływanie powyższych środków na turystykę będzie pozytywne, ponieważ poprawią one zarówno bezpieczeństwo w Unii Europejskiej, jak i przyniosą korzyści w postaci przyspieszenia kontroli granicznych. Podobnie oczekuje się, że ich oddziaływanie na lotniska, porty morskie i przewoźników będzie pozytywne, szczególnie ze względu na przyspieszenie kontroli podczas odpraw granicznych.

- **Prawa podstawowe**

W ocenie skutków przeanalizowano szczególnie oddziaływanie proponowanych środków na prawa podstawowe, a zwłaszcza na ochronę danych.

Zgodnie z Kartą praw podstawowych Unii Europejskiej, której instytucje i państwa członkowskie UE mają obowiązek przestrzegać podczas wdrażania prawa Unii (art. 51 ust. 1 Karty), możliwości oferowane przez interoperacyjność jako środek zwiększania bezpieczeństwa i ochrony granic zewnętrznych należy zrównoważyć z obowiązkiem zapewnienia, aby ingerencje w prawa podstawowe mogące wynikać z nowego środowiska interoperacyjności zostały ograniczone do tego, co jest ściśle konieczne, aby rzeczywiście odpowiadały celom interesu ogólnego, z uwzględnieniem zasady proporcjonalności (art. 52 ust. 1 karty).

Proponowane rozwiązania w zakresie interoperacyjności stanowią elementy uzupełniające już istniejące systemy. Jako takie nie zmienią równowagi już zapewnionej przez każdy z istniejących systemów centralnych, jeśli chodzi o ich pozytywne oddziaływanie na przestrzeganie praw podstawowych.

Interoperacyjność ma jednak potencjał wywierania dodatkowego, pośredniego wpływu na przestrzeganie szeregu praw podstawowych. W istocie poprawna identyfikacja osoby wywiera pozytywny wpływ na przestrzeganie prawa do poszanowania życia prywatnego, a zwłaszcza prawa do tożsamości (art. 7 karty), oraz może przyczynić się do uniknięcia pomyłek co do tożsamości danej osoby. Z drugiej strony przeprowadzanie kontroli tożsamości na podstawie danych biometrycznych może być postrzegane jako ingerencja w przysługujące każdej osobie prawo do godności (zwłaszcza jeśli kontrole te są postrzegane jako upokarzające) (art. 1). W badaniu[37] przeprowadzonym przez Agencję Praw Podstawowych Unii Europejskiej respondentów wyraźnie zapytano, czy uważają, że przekazywanie własnych danych biometrycznych w kontekście kontroli granicznej może być upokarzające. Większość respondentów udzieliła negatywnej odpowiedzi na to pytanie.

Proponowane elementy interoperacyjności stwarzają szansę na przyjęcie ukierunkowanych środków zapobiegawczych w celu zwiększenia bezpieczeństwa. Jako takie mogą przyczynić się do ochrony prawa do życia (art. 2 karty), co nakłada także na władze pozytywny obowiązek podjęcia operacyjnych środków zapobiegawczych, aby chronić osobę, której życie jest zagrożone, jeśli wiedzą lub powinny wiedzieć o istnieniu bezpośredniego zagrożenia[38], a także aby stać na straży zakazu niewolnictwa i pracy przymusowej (art. 5). Dzięki rzetelnej, dostępniejszej i łatwiejszej identyfikacji interoperacyjność może przyczynić się do odnajdywania zaginionych dzieci lub dzieci, które padły ofiarą handlu ludźmi, a także ułatwić szybkie i ukierunkowane reagowanie.

Niezawodna, bardziej przystępna i łatwiejsza identyfikacja mogłaby także przyczynić się do skutecznego egzekwowania prawa do azylu (art. 18 karty) i zakazu odsyłania (art. 19 karty). W istocie interoperacyjność może zapobiec sytuacjom, w którym osoby ubiegające się o azyl są bezprawnie aresztowane, zatrzymywane lub poddawane niezgodnemu z prawem wydaleniu. Ponadto dzięki interoperacyjności identyfikacja oszustw dotyczących tożsamości także stanie się łatwiejsza. Zmniejszy się także potrzeba udostępniania danych i informacji dotyczących osób ubiegających się o azyl państwom trzecim (zwłaszcza państwu pochodzenia) w celu ustalenia tożsamości danej osoby i uzyskania dokumentów podróży, co potencjalnie może narazić tę osobę na niebezpieczeństwo.

- **Ochrona danych osobowych**

Z uwagi na wykorzystywane dane osobowe, interoperacyjność będzie wywierać szczególny wpływ na prawo do ochrony danych osobowych. Prawo to zostało ustanowione na mocy art. 8 karty i art. 16 Traktatu o funkcjonowaniu Unii Europejskiej oraz art. 8 europejskiej konwencji praw człowieka. Jak podkreślił Trybunał Sprawiedliwości UE[39], prawo do ochrony

[37] *Badanie Agencji Praw Podstawowych Unii Europejskiej w ramach projektu pilotażowego eu-LISA w sprawie inteligentnych granic — opinie i doświadczenia podróżnych związane z inteligentnymi granicami*, sprawozdanie Agencji Praw Podstawowych Unii Europejskiej: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

[38] Europejski Trybunał Praw Człowieka, Osman przeciwko Zjednoczonemu Królestwu, nr 87/1997/871/1083, 28 października 1998 r., pkt 116.

[39] Trybunał Sprawiedliwości UE, wyrok z dnia 9.11.2010 r.; sprawy połączone C-92/09 i C-93/09 Volker und Markus Schecke oraz Eifert [2010] Zb.Orz. I-0000.

danych osobowych nie jest prawem absolutnym, lecz powinno być rozpatrywane w kontekście funkcji, jaką pełni w społeczeństwie[40]. Ochrona danych jest ściśle powiązana z poszanowaniem życia prywatnego i rodzinnego chronionego przez art. 7 karty.

Zgodnie z ogólnym rozporządzeniem o ochronie danych[41] swobodny przepływ danych wewnątrz UE nie może być ograniczany względami ochrony danych. Należy jednak przestrzegać szeregu zasad w tym zakresie. W istocie aby wszelkie ograniczenie dotyczące wykonywania praw podstawowych chronionych na mocy Karty było zgodne z prawem, musi ono być zgodne z następującymi kryteriami, określonymi w art. 52 ust. 1:

- być przewidziane ustawą;
- szanować istotę tych praw;
- rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób;
- być konieczne; oraz
- być proporcjonalne.

Niniejszy wniosek spełnia wszystkie powyższe zasady dotyczące ochrony danych, jak szczegółowo określono w ocenie skutków towarzyszącej wnioskowi dotyczącemu rozporządzenia. Wniosek opiera się na uwzględnianiu ochrony danych w fazie projektowania oraz na domyślnej ochronie danych. Obejmuje wszystkie odpowiednie przepisy ograniczające przetwarzanie danych do tego, co konieczne do osiągnięcia konkretnego celu, oraz przyznaje dostęp do danych tylko podmiotom, które muszą je znać. Okresy zatrzymywania danych (w stosownych przypadkach) są odpowiednie i ograniczone. Dostęp do danych jest zarezerwowany wyłącznie dla odpowiednio uprawnionego personelu organów państw członkowskich w konkretnych celach określonych dla każdego systemu informacyjnego i jest ograniczony do zakresu, w jakim dane te są konieczne do wykonywania zadań zgodnie z tymi celami.

4. WPŁYW NA BUDŻET

Wpływ na budżet zawarto w załączonym sprawozdaniu finansowym. Obejmuje ono pozostający okres obecnych wieloletnich ram finansowych (do 2020 r.) i siedem lat kolejnego okresu (2021–2027). Proponowany budżet na lata od 2021 r. podano jedynie w celach orientacyjnych i nie przesądza on o kształcie kolejnych wieloletnich ram finansowych.

Wdrożenie wniosku będzie wymagało przydzielenia środków budżetowych na następujące cele:

1) **opracowanie** i integracja przez eu-LISA czterech elementów interoperacyjności i centralnego repozytorium sprawozdawczo-statystycznego oraz ich dalsza **obsługa techniczna i eksploatacja**;

[40] Zgonie z art. 52 ust. 1 karty, można ograniczyć korzystanie z prawa do ochrony danych, o ile takie ograniczenia są przewidziane prawem i respektują istotę praw i wolności, i o ile, zastrzeżeniem zasady proporcjonalności, są one konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób.

[41] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2) **migracja danych** do wspólnego serwisu kojarzenia danych biometrycznych i wspólnego repozytorium tożsamości. W przypadku wspólnego serwisu kojarzenia danych biometrycznych wzorce biometryczne odpowiednich danych z trzech systemów obecnie wykorzystujących dane biometryczne (SIS, VIS i Eurodac) będzie należało odtworzyć w tym serwisie. W przypadku wspólnego repozytorium tożsamości elementy danych osobowych należy przenieść z VIS do repozytorium, a także zatwierdzić ewentualne powiązania wykryte między tożsamościami zawartymi w SIS, VIS i Eurodac. Szczególnie ten ostatni proces będzie się wiązał z dużym nakładem zasobów;

3) dokonana przez eu-LISA aktualizacja **jednolitego interfejsu krajowego**, już przewidziana w rozporządzeniu w sprawie EES, stanie się ogólnie stosowanym elementem umożliwiającym wymianę komunikatów między państwami członkowskimi a systemem(-ami) centralnym(-i);

4) **integracja systemów krajowych państw członkowskich** z jednolitym interfejsem krajowym będzie służyć przekazywaniu komunikatów wymienianych z centralnym repozytorium tożsamości / modułem wykrywającym multiplikację tożsamości za pośrednictwem europejskiego portalu wyszukiwania

5) **szkolenia** z korzystania z elementów interoperacyjności dla użytkowników końcowych, w tym za pośrednictwem Agencji Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL).

Elementy interoperacyjności są tworzone i utrzymywane jako program. Podczas gdy europejski portal wyszukiwania i moduł wykrywający multiplikację tożsamości stanowią całkiem nowe elementy, podobnie jak centralne repozytorium sprawozdawczo-statystyczne, wspólny serwis kojarzenia danych biometrycznych i wspólne repozytorium tożsamości stanowią wspólne elementy łączące istniejące dane przechowywane (lub które będą przechowywane) w istniejących lub nowych systemach, dla których istnieją preliminarze budżetowe.

Europejski portal wyszukiwania wdroży istniejące, znane interfejsy w celu korzystania z SIS, VIS i Eurodac, w przyszłości zostanie także rozszerzony o nowe systemy.

Portal będzie wykorzystywany przez państwa członkowskie i agencje za pomocą interfejsu opartego na uniwersalnym formacie wiadomości (UMF). Nowy interfejs będzie wymagał prac rozwojowych, adaptacji, integracji i badań, których dokonają państwa członkowskie, eu-LISA, Europol oraz Europejska Agencja Straży Granicznej i Przybrzeżnej. Europejski portal wyszukiwania będzie korzystał z koncepcji jednolitego interfejsu krajowego wprowadzonego z myślą o EES, co ułatwi działania związane z integracją.

Portal będzie wiązał się z dodatkowymi kosztami po stronie Europolu w związku z udostępnieniem interfejsu QUEST do korzystania w celach związanych z danymi „poziomu podstawowej ochrony”.

Podstawy **wspólnego serwisu kojarzenia danych biometrycznych** zostaną *de facto* ustanowione wraz ze stworzeniem nowego systemu EES, gdyż zdecydowanie będzie się ono wiązało z największą ilością nowych danych biometrycznych. Wymagany budżet został zarezerwowany w ramach instrumentu prawnego EES. Dodanie do wspólnego serwisu kojarzenia danych biometrycznych dalszych danych biometrycznych z serwisów VIS, SIS i Eurodac stanowi dodatkowy koszt, związany głównie z migracją istniejących danych. Koszty szacuje się na 10 mln EUR dla wszystkich trzech systemów. Dodawanie danych

biometrycznych z proponowanego systemu ECRIS-TCN stanowi ograniczony dodatkowy koszt, który może zostać pokryty ze środków zarezerwowanych w ramach proponowanego instrumentu prawnego ECRIS-TCN, aby ustanowić system automatycznej identyfikacji daktyloskopijnej ECRIS-TCN.

Wspólne repozytorium tożsamości zostanie ustanowione wraz z utworzeniem przyszłego EES i dodatkowo rozszerzone podczas opracowywania proponowanego systemu ETIAS. Silniki baz danych i wyszukiwarki dla tych danych przewidziano w budżecie zarezerwowanym w instrumentach prawnych dotyczących przyszłego systemu EES i proponowanego systemu ETIAS. Dodawanie nowych danych biograficznych zarówno z systemu Eurodac, jak i proponowanego systemu ECRIS-TCN, stanowi mniejszy dodatkowy koszt już zarezerwowany w ramach instrumentów prawnych systemu Eurodac i proponowanego systemu ECRIS-TCN.

Całkowity budżet wymagany w ciągu dziewięciu lat (2019–2027) wynosi 424,7 mln EUR i obejmuje następujące pozycje:

1) budżet wynoszący 225 mln EUR dla eu-LISA, który obejmuje całkowite koszty opracowania programu służącego dostarczeniu pięciu elementów interoperacyjności (68,3 mln EUR), koszty obsługi technicznej od czasu dostarczenia elementów do 2027 r. (56,1 mln EUR), specjalne środki wynoszące 25 mln EUR przeznaczone na migrację danych z istniejących systemów do wspólnego serwisu kojarzenia danych biometrycznych oraz dodatkowe koszty aktualizacji jednolitego interfejsu krajowego, sieci, szkoleń i posiedzeń. Specjalny budżet wynoszący 18,7 mln EUR obejmuje koszty modernizacji i funkcjonowania systemu ECRIS-TCN w trybie wysokiej dostępności od 2022 r.

2) Budżet wynoszący 136,3 mln EUR obejmuje środki dla państw członkowskich na pokrycie kosztów zmian w swoich systemach krajowych, aby mogły korzystać z elementów interoperacyjności i jednolitego interfejsu krajowego dostarczonego przez eu-LISA, oraz środki na szkolenia licznej grupy użytkowników końcowych;

3) budżet wynoszący 48,9 mln EUR będzie przeznaczony na aktualizację systemów informatycznych Europolu, aby przygotować je do obsługi zwiększonej ilości komunikatów oraz podnieść poziom ich wydajności[42]. Elementy interoperacyjności będą wykorzystywane przez system ETIAS w celu przeglądania danych Europolu.

4) budżet wynoszący 4,8 mln EUR będzie przeznaczony dla Europejskiej Agencji Straży Granicznej i Przybrzeżnej na przyjęcie zespołu specjalistów, którzy w ciągu jednego roku będą zatwierdzać powiązania między poszczególnymi tożsamościami w razie uruchomienia się ostrzeżeń w module wykrywającym multiplikację tożsamości;

5) budżet wynoszący 2,0 mln EUR będzie przeznaczony dla Agencji Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL) na pokrycie kosztów przygotowań i przeprowadzenia szkoleń dla pracowników operacyjnych;

6) zapewnienie kwoty w wysokości 7,7 mln EUR dla Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych na pokrycie nieznacznego wzrostu kosztów personelu i kosztów powiązanych w okresie opracowywania poszczególnych elementów,

[42] Aktualne zdolności Europolu do przetwarzania informacji nie odpowiadają znacznym ilościom (średnio 100 000 zapytań dziennie) i skróconemu czasowi udzielenia odpowiedzi, które będą wymagane w ramach systemu ETIAS;

ponieważ Komisja będzie musiała realizować w tym okresie dodatkowe zadania i odpowiadać za prace komitetu pracującego nad uniwersalnym formatem wiadomości.

Instrumentem finansowym, w którym uwzględniono budżet przeznaczony na realizację inicjatywy w sprawie interoperacyjności, jest rozporządzenie w sprawie Funduszu Bezpieczeństwa Wewnętrznego i wsparcia w zakresie granic. Jego art. 5 lit. b) stanowi, że kwota 791 mln EUR ma zostać przeznaczona na program, którego celem jest opracowanie systemów informatycznych, w oparciu o istniejące lub nowe systemy informatyczne, wspierające zarządzanie przepływami migracyjnymi przez granice zewnętrzne, z zastrzeżeniem przyjęcia odpowiednich aktów ustawodawczych Unii i na warunkach określonych w art. 15 ust. 5. W ramach kwoty 791 mln EUR, 480,2 mln EUR jest zarezerwowane na opracowywanie systemu EES, 210 mln EUR — na system ETIAS, a 67,9 mln EUR — na przegląd SIS. Pozostała kwota (32,9 mln EUR) będzie poddana realokacji za pomocą mechanizmów Funduszu Bezpieczeństwa Wewnętrznego ds. Granic i Wiz. Niniejszy wniosek wymaga kwoty 32,1 mln EUR w ramach obecnych WRF (2019/20), mieści się zatem w granicach dostępnego budżetu.

5. INFORMACJE DODATKOWE

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

Agencja eu-LISA odpowiada za zarządzanie operacyjne wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W związku z tym już teraz ma za zadanie eksploatację istniejących systemów oraz wprowadzanie w nich udoskonaleń technicznych i operacyjnych oraz opracowywanie przewidywanych przyszłych systemów. Na mocy niniejszego wniosku dotyczącego rozporządzenia agencja ta będzie projektować fizyczną architekturę elementów interoperacyjności, rozwijać je i wdrażać, a ostatecznie obsługiwać je. Poszczególne elementy będą wdrażane stopniowo, w powiązaniu z opracowywaniem systemów podstawowych.

Komisja zapewni wprowadzenie systemów służących monitorowaniu rozwoju i funkcjonowania czterech elementów (europejski portal wyszukiwania, wspólny serwis kojarzenia danych biometrycznych, wspólne repozytorium tożsamości, moduł wykrywający multiplikację tożsamości) i centralnego repozytorium sprawozdawczo-statystycznego oraz będzie dokonywać ich oceny w stosunku do głównych celów politycznych. Cztery lata po wprowadzeniu i rozpoczęciu działania tych funkcji, a następnie co cztery lata, eu-LISA powinna przedkładać Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie dotyczące technicznego funkcjonowania elementów interoperacyjności. Dodatkowo pięć lat po wprowadzeniu tych funkcji i rozpoczęciu przez nie działania oraz co cztery lata od tego momentu Komisja dokonuje ogólnej oceny tych elementów, w tym ich bezpośredniego lub pośredniego oddziaływania oraz konsekwencji ich stosowania w praktyce dla praw podstawowych. Ocenia wówczas osiągnięte rezultaty pod kątem przyjętych uprzednio celów i analizuje, czy przesłanki dla wprowadzenia tych elementów pozostają aktualne, a także wszelkie konsekwencje dla przyszłych opcji. Komisja powinna przekazywać sprawozdania z oceny Parlamentowi Europejskiemu i Radzie.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Rozdział I opisuje ogólne przepisy niniejszego rozporządzenia. Wyjaśnia: zasady leżące u podstaw niniejszego rozporządzenia; ustanowione w nim elementy; cele, jakim ma służyć interoperacyjność; zakres rozporządzenia; definicje terminów stosowanych w rozporządzeniu; oraz zasadę niedyskryminacji odnoszącą się do przetwarzania danych na mocy niniejszego rozporządzenia.

Rozdział II określa przepisy dotyczące europejskiego portalu wyszukiwania. Rozdział ten dotyczy ustanowienia portalu i jego architektury technicznej, którą ma opracować eu-LISA. Określa cel europejskiego portalu wyszukiwania i wskazuje, kto i w jaki sposób może z niego korzystać zgodnie z istniejącymi prawami dostępu do każdego z systemów centralnych. Zgodnie z obowiązującymi przepisami eu-LISA ma obowiązek tworzenia profili użytkowników dla każdej kategorii użytkownika. Rozdział ten określa, w jaki sposób europejski portal wyszukiwania będzie przeglądać systemy centralne, a także przedstawia treść i format odpowiedzi udzielanych użytkownikom. Rozdział II stanowi także, że eu-LISA będzie prowadzić rejestry dotyczące wszystkich operacji przetwarzania, i przedstawia procedurę awaryjną w sytuacji, w której portal nie będzie mógł uzyskać dostępu do jednego z systemów centralnych lub większej ich liczby.

Rozdział III określa przepisy dotyczące wspólnego serwisu kojarzenia danych biometrycznych. Rozdział ten dotyczy ustanowienia serwisu i jego architektury technicznej, którą ma opracować eu-LISA. Określa jego cel i to, jakie dane będą w nim przechowywane. Wyjaśnia stosunek między wspólnym serwisem kojarzenia danych biometrycznych a pozostałymi elementami. Rozdział III stanowi też, że serwis ten nie będzie przechowywał danych, jeśli zostaną one usunięte z odpowiedniego systemu centralnego, oraz że eu-LISA będzie prowadzić rejestry dotyczące wszystkich operacji przetwarzania.

Rozdział IV określa przepisy dotyczące wspólnego repozytorium tożsamości. Rozdział ten dotyczy ustanowienia repozytorium i jego architektury technicznej, którą ma opracować eu-LISA. Określa jego cel i wyjaśnia, jakie dane i w jaki sposób będą w nim przechowywane, obejmuje też przepisy dotyczące zapewniania jakości przechowywanych danych. Rozdział ten stanowi, że wspólne repozytorium tożsamości będzie tworzyć akta osobowe na podstawie danych przechowywanych w systemach centralnych, a poszczególne akta będą aktualizowane zgodnie ze zmianami wprowadzanymi w odpowiednich systemach centralnych. Rozdział IV określa także, jak repozytorium będzie działać w stosunku do modułu wykrywającego multiplikację tożsamości. W rozdziale tym podano, kto może mieć dostęp do wspólnego repozytorium tożsamości i w jaki sposób może uzyskać dostęp do danych zgodnie z przysługującymi mu prawami dostępu, zawiera także bardziej szczegółowe przepisy zależne od tego, czy celem dostępu jest identyfikacja osoby, czy uzyskanie dostępu do systemów EES, VIS, ETIAS i Eurodac za pośrednictwem repozytorium na potrzeby ścigania przestępstw na pierwszym etapie podejścia dwuetapowego. Rozdział IV stanowi też, że eu-LISA będzie prowadzić rejestry dotyczące wszystkich operacji przetwarzania związanych ze wspólnym repozytorium tożsamości.

Rozdział V zawiera przepisy dotyczące modułu wykrywającego multiplikację tożsamości. Rozdział ten dotyczy ustanowienia modułu i jego architektury technicznej, którą ma opracować eu-LISA. Wyjaśnia jego cel i reguluje korzystanie z niego zgodnie z prawami dostępu do każdego z systemów centralnych. Rozdział V określa, kiedy i jak moduł będzie dokonywać wyszukiwania w celu wykrycia multiplikacji tożsamości należących do jednej osoby oraz jak jego wyniki będą dostarczane i przetwarzane, w tym w razie konieczności w drodze weryfikacji ręcznej. Rozdział V określa klasyfikację rodzajów powiązań, które mogą wyniknąć z wyszukiwania w zależności od tego, czy jego rezultat wykaże istnienie

jednej tożsamości, multiplikacji tożsamości lub wspólnych danych dotyczących tożsamości. Rozdział ten stanowi, że moduł wykrywający multiplikację tożsamości będzie gromadzić dane powiązane przechowywane w systemach centralnych, podczas gdy same dane pozostaną w jednym lub większej liczbie tych systemów centralnych. Rozdział V stanowi też, że eu-LISA będzie prowadzić rejestry dotyczące wszystkich operacji przetwarzania związanych z modułem wykrywającym multiplikację tożsamości.

Rozdział VI określa środki mające na celu wspomaganie interoperacyjności. Wskazuje sposoby udoskonalania jakości danych poprzez ustanowienie uniwersalnego formatu wiadomości jako wspólnego standardu wymiany informacji wspierającego interoperacyjność oraz przewiduje stworzenie centralnego repozytorium sprawozdawczo-statystycznego.

Rozdział VII dotyczy ochrony danych osobowych. Rozdział ten zawiera przepisy zapewniające, aby dane przetwarzane na mocy niniejszego rozporządzenia były przetwarzane zgodnie z prawem i właściwie, w sposób określony w rozporządzeniu nr 45/2001. Wyjaśnia, czym będzie podmiot przetwarzający dane dla każdego ze środków interoperacyjności zaproponowanych w niniejszym rozporządzeniu, określa środki wymagane od eu-LISA i władz państw członkowskich w celu zapewnienia bezpieczeństwa przetwarzania danych, poufności danych, odpowiedniego reagowania na incydenty związane z ich bezpieczeństwem oraz odpowiedniego monitorowania zgodności tych środków z niniejszym rozporządzeniem. Rozdział ten zawiera też przepisy dotyczące praw osób, których dane dotyczą, w tym prawa do informacji o tym, że dane ich dotyczące są przechowywane i przetwarzane na mocy niniejszego rozporządzenia, oraz prawa do dostępu do danych osobowych przechowywanych i przetwarzanych na mocy niniejszego rozporządzenia, ich korekty i usuwania. Rozdział ten precyzuje ponadto zasadę, że dane przetwarzane na mocy niniejszego rozporządzenia nie mogą być przekazywane ani udostępniane do państwa trzeciego, organizacji międzynarodowej lub strony trzeciej, z wyjątkiem, w określonych celach, Interpolu, oraz danych otrzymywanych od Europolu za pośrednictwem europejskiego portalu wyszukiwania, w którym to przypadku obowiązują przepisy rozporządzenia 2016/794 w sprawie późniejszego przetwarzania danych. Na koniec rozdział ten określa przepisy związane z nadzorem i kontrolami w odniesieniu do ochrony danych.

Rozdział VIII określa obowiązki eu-LISA, państw członkowskich, Europolu i jednostki centralnej ETIAS przed wejściem w życie środków przewidzianych w niniejszym rozporządzeniu i po ich wejściu w życie.

Rozdział IX dotyczy zmian w innych aktach unijnych. Rozdział ten wprowadza zmiany do innych aktów prawnych konieczne do pełnego wdrożenia niniejszego wniosku w sprawie interoperacyjności. Niniejszy wniosek obejmuje szczegółowe przepisy dotyczące koniecznych zmian w aktach prawnych, które obecnie stanowią stabilne teksty przyjęte przez współustawodawców: kodeksie granicznym Schengen, rozporządzeniu w sprawie EES, rozporządzeniu (WE) w sprawie VIS, decyzji Rady 2004/512/WE (decyzja w sprawie VIS), decyzji Rady 2008/633/WSiSW (decyzja w sprawie dostępu organów ścigania do VIS).

Rozdział X określa następujące szczegóły: wymogi dotyczące statystyk i sprawozdawczości związane z danymi przetwarzanymi na mocy niniejszego rozporządzenia; środki przejściowe, które będą konieczne; ustalenia dotyczące kosztów wynikających z niniejszego rozporządzenia; wymagania dotyczące powiadomień; proces rozpoczęcia działania środków przewidzianych w niniejszym rozporządzeniu; zasady zarządzania obejmujące utworzenie komitetu i grupy doradczej, obowiązki eu-LISA dotyczące szkoleń oraz praktyczny podręcznik wspierający wdrażanie elementów interoperacyjności i zarządzanie nimi; procedury związane z monitorowaniem i oceną środków zaproponowanych w niniejszym rozporządzeniu; oraz przepis w sprawie wejścia w życie niniejszego rozporządzenia.

2017/0351 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniające decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399 i rozporządzenie (UE) 2017/2226

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 ust. 2, art. 74 i art. 77 ust. 2 lit a), b), d) i e),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[43],

uwzględniając opinię Komitetu Regionów[44],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) W swoim komunikacie z dnia 6 kwietnia 2016 r. zatytułowanym „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”[45] Komisja podkreśliła potrzebę poprawy struktury zarządzania danymi Unii na potrzeby zarządzania granicami i zapewnienia bezpieczeństwa. Komunikat ten zainicjował proces zmierzający do osiągnięcia interoperacyjności między unijnymi systemami informacyjnymi w dziedzinach bezpieczeństwa oraz zarządzania granicami i migracją, aby wyeliminować niedoskonałości strukturalne związane z tymi systemami, które utrudniają pracę władz krajowych, oraz aby zapewnić straży granicznej, organom celnym, funkcjonariuszom policji i organom sądowym dostęp do koniecznych informacji.

(2) W swoim „Planie działania na rzecz intensyfikacji wymiany informacji i udoskonalenia zarządzania nimi, w tym na rzecz rozwiązań interoperacyjnych w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych” z dnia 6 czerwca 2016 r.[46] Rada wskazała liczne wyzwania natury prawnej, technicznej i operacyjnej związane z osiągnięciem interoperacyjności systemów informacyjnych UE oraz wezwała do wprowadzenia w życie rozwiązań w tym zakresie.

---

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

[44]

[45] COM(2016) 205 z 6.4.2016.

[46] Plan działania na rzecz intensyfikacji wymiany informacji i udoskonalenia zarządzania nimi, w tym na rzecz rozwiązań interoperacyjnych w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych z dnia 6 czerwca 2016 r. — 9368/1/16 REV 1.

(3) W swojej rezolucji z dnia 6 lipca 2016 r. w sprawie strategicznych priorytetów programu prac Komisji na 2017 r.[47] Parlament Europejski wezwał Komisję do przedstawienia wniosków dotyczących poprawy i dalszego rozwoju istniejących systemów informacyjnych UE, zmniejszania luk informacyjnych oraz dążenia do osiągnięcia interoperacyjności, a także wniosków dotyczących obowiązkowej wymiany informacji na szczeblu UE, wraz z niezbędnymi gwarancjami ochrony danych.

(4) W dniu 15 grudnia 2016 r. Rada Europejska[48] zaapelowała o dalsze efekty prac nad interoperacyjnością unijnych systemów informacyjnych i baz danych.

(5) W swoim sprawozdaniu końcowym z dnia 11 maja 2017 r.[49] grupa ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności stwierdziła, że prace w kierunku praktycznych rozwiązań służących zapewnieniu interoperacyjności systemów informacyjnych są konieczne i wykonalne pod względem technicznym, zaś rozwiązania te mogą zasadniczo zarówno przynieść korzyści operacyjne, jak i zostać ustanowione zgodnie z wymogami ochrony danych.

(6) W swoim komunikacie z dnia 16 maja 2017 r. zatytułowanym „Siódme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa”[50] Komisja określiła, zgodnie ze swoim komunikatem z dnia 6 kwietnia 2016 r. oraz z wnioskami i zaleceniami grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, nowe podejście do zarządzania danymi dotyczącymi ochrony granic, bezpieczeństwa i migracji zakładające pełną interoperacyjność wszystkich systemów informacyjnych UE w dziedzinie bezpieczeństwa, zarządzania granicami i zarządzania przepływami migracyjnymi, przy pełnym poszanowaniu praw podstawowych.

(7) W swoich konkluzjach z dnia 9 czerwca 2017 r.[51] w sprawie dalszych prac nad usprawnieniem wymiany informacji i zapewnieniem interoperacyjności unijnych systemów informacyjnych Rada zachęciła Komisję do dążenia do realizacji rozwiązań w zakresie interoperacyjności zaproponowanych przez grupę ekspertów wysokiego szczebla.

(8) W dniu 23 czerwca 2017 r. Rada Europejska[52] podkreśliła potrzebę poprawy interoperacyjności pomiędzy bazami danych i zachęciła Komisję do jak najszybszego sporządzenia projektu przepisów opartego na propozycjach grupy ekspertów wysokiego szczebla ds. systemów informatycznych i interoperacyjności.

(9) Należy ustanowić interoperacyjność między systemami informacyjnymi UE — a mianowicie [systemem wjazdu/wyjazdu (EES)], wizowym systemem informacyjnym (VIS), [europejskim systemem informacji o podróży oraz zezwoleń na podróż (ETIAS)], systemem Eurodac, Systemem Informacyjnym Schengen (SIS) oraz [europejskim systemem przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN)], aby poprawić zarządzanie granicami zewnętrznymi, przyczynić się do zapobiegania nielegalnej migracji i jej zwalczania oraz wnieść wkład w zapewnienie wysokiego poziomu bezpieczeństwa w ramach unijnej

---

47 Rezolucja Parlamentu Europejskiego z dnia 6 lipca 2016 r. w sprawie strategicznych priorytetów programu prac Komisji na 2017 r. (2016/2773(RSP).

48 http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/.

49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

50 COM(2017) 261 final z 16.5.2017.

51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.

52 Konkluzje Rady Europejskiej z dni 22–23 czerwca 2017 r.

przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w tym w utrzymanie bezpieczeństwa publicznego i polityki publicznej, oraz aby chronić bezpieczeństwo na terytoriach państw członkowskich, tak aby te unijne systemy informacyjne i zawarte w nich dane mogły się wzajemnie uzupełniać. W tym celu jako elementy interoperacyjności należy ustanowić europejski portal wyszukiwania, wspólny serwis kojarzenia danych biometrycznych, wspólne repozytorium tożsamości i moduł wykrywający multiplikację tożsamości.

(10) Interoperacyjność między unijnymi systemami informacyjnymi powinna umożliwiać tym systemom wzajemne uzupełnianie i ułatwić w ten sposób poprawną identyfikację osób, przyczynić się do zwalczania oszustw dotyczących tożsamości, poprawić i zharmonizować wymagania dotyczące jakości danych w odpowiednich unijnych systemach informacyjnych, ułatwić wdrożenie istniejących i przyszłych unijnych systemów informacyjnych przez państwa członkowskie od strony technicznej i operacyjnej, wzmocnić i uprościć gwarancje bezpieczeństwa danych i ochrony danych regulujące odpowiednie systemy informacyjne UE, usprawnić dostęp organów ścigania do systemów EES, VIS, [ETIAS] i Eurodac oraz wspierać realizację celów systemów EES, VIS, [ETIAS], Eurodac, SIS i [ECRIS-TCN].

(11) Elementy interoperacyjności powinny obejmować systemy EES, VIS, [ETIAS], Eurodac, SIS i [ECRIS-TCN]. Powinny one obejmować dane Europolu w zakresie umożliwiającym ich przeglądanie jednocześnie z systemami informacyjnymi UE.

(12) Elementy interoperacyjności powinny dotyczyć osób, których dane osobowe mogą być przetwarzane w systemach informacyjnych UE i przez Europol, a mianowicie obywateli państw trzecich, których dane osobowe są przetwarzane w systemach informacyjnych UE i przez Europol, oraz obywateli Unii, których dane osobowe są przetwarzane w SIS i przez Europol.

(13) Należy ustanowić europejski portal wyszukiwania, aby technicznie wspomagać władze państw członkowskich i organy UE w uzyskiwaniu szybkiego, sprawnego, wydajnego, systematycznego i kontrolowanego dostępu do systemów informacyjnych UE, danych Europolu i baz danych Interpolu koniecznych do pełnienia przez nie swoich funkcji, zgodnie z własnymi prawami dostępu, a także aby wspierać realizację celów systemów EES, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN] i danych Europolu. Poprzez umożliwienie jednoczesnego, równoległego przeszukiwania wszystkich istotnych systemów informacyjnych, a także danych Europolu i baz danych Interpolu, europejski portal wyszukiwania powinien działać jako pojedynczy punkt kontaktowy lub „pośrednik komunikatów” oraz służyć sprawnemu przeszukiwaniu różnych systemów centralnych i uzyskiwaniu koniecznych informacji, przy pełnym poszanowaniu zasad kontroli dostępu i wymogów dotyczących ochrony danych regulujących systemy podstawowe.

(14) Baza zawierająca dane skradzionych lub utraconych dokumentów podróży (SLTD) Międzynarodowej Organizacji Policji Kryminalnej (Interpolu) umożliwia uprawnionym organom ścigania państw członkowskich, w tym urzędnikom imigracyjnym i funkcjonariuszom straży granicznej, ustalenie, czy dany dokument podróży jest ważny. [System ETIAS] przeszukuje bazy danych SLTD i TDAWN Interpolu w kontekście oceny, czy istnieje ryzyko, że osoba ubiegająca się o zezwolenie na podróż migruje nielegalnie lub może stwarzać zagrożenie dla bezpieczeństwa. Scentralizowany europejski portal wyszukiwania powinien umożliwiać przeszukiwanie baz danych SLTD i TDAWN za pomocą danych dotyczących tożsamości danej osoby. W przypadku przekazywania danych osobowych

z Unii do Interpolu za pośrednictwem europejskiego portalu wyszukiwania obowiązują przepisy w sprawie międzynarodowego przekazywania danych określone w rozdziale V rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[53] lub przepisy krajowe stanowiące transpozycję rozdziału V dyrektywy (UE) 2016/680 Parlamentu Europejskiego i Rady[54]. Nie powinno to naruszać przepisów szczegółowych określonych we wspólnym stanowisku Rady 2005/69/WSiSW[55] oraz w decyzji Rady 2007/533/WSiSW[56].

(15) Europejski portal wyszukiwania powinien zostać opracowany i skonfigurowany tak, aby uniemożliwiał wykorzystywanie podczas wyszukiwania pól danych niezwiązanych z osobami lub dokumentami podróży lub które nie są obecne w systemach informacyjnych UE, danych Europolu lub bazie danych Interpolu.

(16) Aby umożliwić szybkie i systematyczne wykorzystywanie wszystkich systemów informacyjnych UE, należy korzystać z europejskiego portalu wyszukiwania w celu konsultowania wspólnego repozytorium tożsamości oraz systemów EES, VIS, [ETIAS], Eurodac i [ECRIS-TCN]. Należy jednak pozostawić krajowe połączenia z różnymi systemami informacyjnymi UE, aby zapewnić techniczną opcję awaryjną. Organy Unii powinny też korzystać z europejskiego portalu wyszukiwania, aby przeszukiwać system centralny Systemu Informacyjnego Schengen (C.SIS) zgodnie z posiadanymi prawami dostępu w celu pełnienia swoich funkcji. Europejski portal wyszukiwania powinien stanowić dodatkowy środek konsultacji C.SIS, danych Europolu i systemów Interpolu, uzupełniając istniejące dedykowane interfejsy.

(17) Dane biometryczne, takie jak odciski palców i wizerunki twarzy, są unikalne, a zatem znacznie bardziej niezawodne w identyfikacji osób niż dane alfanumeryczne. Wspólny serwis kojarzenia danych biometrycznych powinien stanowić narzędzie techniczne służące wzmacnianiu i ułatwianiu prac odpowiednich unijnych systemów informacyjnych i pozostałych elementów interoperacyjności. Głównym celem wspólnego serwisu kojarzenia danych biometrycznych powinno być ułatwienie identyfikacji osób, które mogą być zarejestrowane w różnych bazach danych, poprzez skojarzenie ich danych biometrycznych w różnych systemach oraz poprzez poleganie na jednym, unikalnym elemencie technologicznym zamiast pięciu różnych w każdym z systemów podstawowych. Wspólny serwis kojarzenia danych biometrycznych powinien przyczynić się do poprawy bezpieczeństwa oraz przynieść korzyści finansowe i związane z obsługą techniczną i funkcjonowaniem, ponieważ polega tylko na jednym, unikalnym elemencie technologicznym, nie zaś na pięciu różnych w każdym z systemów podstawowych. Wszystkie zautomatyzowane systemy identyfikacji daktyloskopijnej, w tym te obecnie wykorzystywane na potrzeby systemów Eurodac, VIS i SIS, korzystają ze wzorców biometrycznych składających

---

[53] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

[54] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

[55] Wspólne stanowisko Rady 2005/69/WSiSW z dnia 24 stycznia 2005 r. w sprawie wymiany niektórych danych z Interpolem (Dz.U. L 27 z 29.1.2005, s. 61).

[56] Decyzja 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 205 z 7.8.2007, s. 63).

się z danych uzyskanych w wyniku ekstrakcji cech z rzeczywistych próbek biometrycznych. Wspólny serwis kojarzenia danych biometrycznych powinien przegrupować i gromadzić wszystkie te wzorce biometryczne w jednej lokalizacji, ułatwiając porównania międzysystemowe i umożliwiając korzyści skali w zakresie rozwoju i utrzymywania unijnych systemów centralnych.

(18) Dane biometryczne stanowią wrażliwe dane osobowe. Niniejsze rozporządzenie ma za zadanie określić podstawy i zabezpieczenia związane z przetwarzaniem takich danych w celu jednostkowej identyfikacji osób.

(19) Systemy ustanowione na mocy rozporządzenia (UE) 2017/2226 Parlamentu Europejskiego i Rady[57], rozporządzenia (WE) nr 767/2008 Parlamentu Europejskiego i Rady[58], [rozporządzenia w sprawie systemu ETIAS] na rzecz zarządzania granicami Unii, system ustanowiony na mocy [rozporządzenia w sprawie Eurodac] na rzecz identyfikacji osób ubiegających się o ochronę międzynarodową i zwalczania nielegalnej migracji oraz system ustanowiony na mocy [rozporządzenia w sprawie ECRIS-TCN], aby były skuteczne, muszą polegać na poprawnej identyfikacji obywateli państw trzecich, których dane osobowe są w nich przechowywane.

(20) Wspólne repozytorium tożsamości powinno zatem ułatwiać i wspomagać poprawną identyfikację osób zarejestrowanych w systemach EES, VIS, [ETIAS], Eurodac i [ECRIS-TCN].

(21) Dane osobowe przechowywane w tych systemach informacyjnych UE mogą dotyczyć tych samych osób, zidentyfikowanych jednak za pomocą różnych lub niekompletnych tożsamości. Państwa członkowskie dysponują skutecznymi sposobami identyfikacji swoich obywateli lub zarejestrowanych stałych rezydentów na swoim terytorium, w przypadku obywateli państw trzecich jest jednak inaczej. Interoperacyjność między systemami informacyjnymi UE powinna przyczyniać się do poprawnej identyfikacji obywateli państw trzecich. Wspólne repozytorium tożsamości powinno przechowywać dane osobowe dotyczące obywateli państw trzecich obecne w systemach i konieczne do ich dokładniejszej identyfikacji, powinno zatem obejmować ich tożsamość, dokument podróży i dane biometryczne, bez względu na system, z którego zostały pierwotnie pobrane. W repozytorium przechowywane są jedynie dane osobowe ściśle konieczne do przeprowadzenia dokładnej kontroli tożsamości. Zarejestrowane w nim dane osobowe powinny być przechowywane nie dłużej niż jest to absolutnie konieczne na potrzeby systemów podstawowych i automatycznie usuwane wraz z usunięciem tych danych z systemów podstawowych, zgodnie z logicznym rozdzieleniem danych.

(22) Nowa operacja przetwarzania danych polegająca na przechowywaniu takich danych we wspólnym repozytorium tożsamości zamiast w każdym z odrębnych systemów jest konieczna do zwiększenia dokładności identyfikacji poprzez automatyczne porównywanie i kojarzenie takich danych. Fakt, że dane potwierdzające tożsamość

---

[57] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen oraz rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (rozporządzenie w sprawie systemu EES) (Dz.U. L 327 z 9.12.2017, s. 20–82).

[58] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie wizowego systemu informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) (Dz.U. L 218 z 13.8.2008, s. 60).

i dane biometryczne obywateli państw trzecich są przechowywane w repozytorium, nie powinien w żaden sposób negatywnie wpływać na przetwarzanie danych na potrzeby rozporządzeń w sprawie systemów EES, VIS, ETIAS, Eurodac czy ECRIS-TCN, ponieważ repozytorium będzie stanowić nowy wspólny element tych systemów podstawowych.

(23) W związku z tym stworzenie w nim akt osobowych dla każdej osoby odnotowanej w systemach EES, VIS, ETIAS, Eurodac lub ECRIS-TCN jest konieczne do osiągnięcia celu poprawnej identyfikacji obywateli państw trzecich w granicach strefy Schengen oraz wspierania modułu wykrywającego multiplikację tożsamości, w podwójnym celu ułatwienia kontroli tożsamości osób podróżujących w dobrej wierze i zwalczania oszustw dotyczących tożsamości. Te akta osobowe powinny gromadzić w jednej lokalizacji wszystkie możliwe tożsamości powiązane z daną osobą i udostępniać je właściwie uprawnionym użytkownikom końcowym.

(24) Wspólne repozytorium tożsamości powinno zatem wspierać funkcjonowanie modułu wykrywającego multiplikację tożsamości oraz ułatwiać i usprawniać dostęp organów ścigania do tych systemów informacyjnych UE, które nie zostały ustanowione wyłącznie w celach zapobiegania poważnym przestępstwom, prowadzenia w ich sprawie dochodzeń, ich wykrywania i ścigania.

(25) Repozytorium powinno stanowić wspólny zbiór danych potwierdzających tożsamość i danych biometrycznych obywateli państw trzecich zarejestrowanych w systemach EES, VIS, [ETIAS], Eurodac i [ECRIS-TCN], służąc jako wspólny element łączący powyższe systemy przechowujące te dane i umożliwiający ich konsultację.

(26) Wszystkie wpisy we wspólnym repozytorium tożsamości powinny być logicznie oddzielone poprzez automatyczne oznakowanie każdego wpisu ze wskazaniem systemu podstawowego, do którego on należy. Oznaczenia te powinny być wykorzystywane w ramach kontroli dostępu do repozytorium, aby umożliwić lub uniemożliwić dostęp do niego.

(27) W celu zapewnienia poprawnej identyfikacji danej osoby właściwe organy państw członkowskich odpowiedzialne za zapobieganie nielegalnej migracji i jej zwalczanie oraz właściwe organy państw członkowskich w rozumieniu art 3 ust. 7 dyrektywy 2016/680 powinny być uprawnione do przeszukiwania wspólnego repozytorium tożsamości za pomocą danych biometrycznych tej osoby pobranych podczas kontroli tożsamości.

(28) Jeśli nie można użyć danych biometrycznych danej osoby lub jeśli zapytanie przy użyciu tych danych zakończy się niepowodzeniem, wyszukiwanie należy przeprowadzić za pomocą danych dotyczących tożsamości tej osoby w połączeniu z danymi z dokumentu podróży. Jeśli wynik zapytania wskaże, że dane tej osoby są przechowywane we wspólnym repozytorium tożsamości, organy państwa członkowskiego powinny mieć możliwość wglądu do danych dotyczących tożsamości tej osoby przechowywanych w repozytorium, bez wskazania w jakikolwiek sposób, do którego systemu informacyjnego UE dane te należą.

(29) Państwa członkowskie powinny przyjąć krajowe środki ustawodawcze wyznaczające właściwe organy odpowiedzialne za przeprowadzanie kontroli tożsamości za pomocą wspólnego repozytorium tożsamości oraz określające procedury, warunki i kryteria, jakim podlegają takie kontrole, zgodnie z zasadą proporcjonalności. W szczególności krajowe środki ustawodawcze powinny określać uprawnienia do pobierania danych

biometrycznych podczas kontroli tożsamości danej osoby przez przedstawicieli tych organów.

(30) Rozporządzenie powinno także wprowadzić nową możliwość usprawnienia dostępu do danych wykraczających poza dane dotyczące tożsamości zawarte w systemach EES, VIS, [ETIAS] lub Eurodac przez organy ścigania wyznaczone przez państwa członkowskie i Europol. Dane, w tym dane inne niż te dotyczące tożsamości zawarte w powyższych systemach, mogą być konieczne do zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania, prowadzenia w ich sprawie dochodzeń i ścigania sprawców w konkretnych sprawach.

(31) Pełen dostęp do wymaganych danych zawartych w systemach informacyjnych UE koniecznych do zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie dochodzeń, wykraczających poza odpowiednie dane dotyczące tożsamości zawarte we wspólnym repozytorium tożsamości, uzyskanych w wyniku użycia danych biometrycznych określonej osoby pobranych podczas kontroli tożsamości, powinien nadal podlegać przepisom odpowiednich aktów prawnych. Wyznaczone organy ścigania i Europol nie wiedzą z góry, który system informacyjny UE zawiera dane osób będących przedmiotem zapytania. Prowadzi to do opóźnień i osłabia efektywność wykonywania przez nie swoich zadań. Użytkownik końcowy uprawniony przez wyznaczony organ powinien móc zatem widzieć, w którym z systemów informacyjnych UE zarejestrowano dane odpowiadające zapytaniu. Dany system zostałby zatem odpowiednio oznaczony w wyniku automatycznej weryfikacji obecności trafienia w danym systemie (tzw. funkcja „wynik/brak wyniku”).

(32) Rejestry tych wyszukiwań we wspólnym repozytorium tożsamości powinny podawać cel wyszukiwania. Jeśli wyszukiwania dokonano w ramach dwuetapowego podejścia do przeglądania danych, rejestry powinny zawierać odniesienie do akt krajowych związanych z danym dochodzeniem lub sprawą, wskazując w ten sposób, że danego zapytania dokonano w celach zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie dochodzeń.

(33) Dokonanie przez organy wyznaczone przez państwo członkowskie i Europol wyszukiwania we wspólnym repozytorium tożsamości w celu uzyskania odpowiedzi typu „wynik/brak wyniku” wskazującej, czy dane zostały zarejestrowane w systemach EES, VIS, [ETIAS] lub Eurodac, wymaga automatycznego przetwarzania danych osobowych. Trafienie nie będzie wiązało się z ujawnianiem danych osobowych osoby, której dotyczy wyszukiwanie, innych niż wskazanie, że pewne jej dane znajdują się w jednym z systemów. Uprawniony użytkownik nie ma prawa podejmować żadnej nieprzychylnej decyzji w stosunku do osoby, której dotyczy wyszukiwanie, jedynie na podstawie samego wystąpienia trafienia. Dostęp użytkownika do trafienia stanowiłby zatem jedynie bardzo ograniczoną ingerencję w prawo do ochrony danych osobowych osoby, której dotyczy wyszukiwanie, przy czym konieczne będzie umożliwienie wyznaczonemu organowi i Europolowi rozpatrzenia jego wniosku o dostęp do danych osobowych w bardziej efektywny sposób, bezpośrednio w systemie oznaczonym jako zawierający trafienie.

(34) Dwuetapowe podejście do przeglądania danych jest szczególnie przydatne w przypadkach, w których osoba podejrzana, sprawca lub domniemana ofiara przestępstwa terrorystycznego pozostają nieznani. W tych przypadkach wspólne repozytorium tożsamości umożliwiłoby identyfikację systemu informacyjnego, w którym zidentyfikowano tę osobę, już za pomocą jednego wyszukiwania. Poprzez

stworzenie obowiązku stosowania tego nowego podejścia, dostęp przez organy ścigania do danych osobowych przechowywanych w systemach EES, VIS, [ETIAS] i Eurodac powinien mieć miejsce bez wymogu wcześniejszego przeszukania krajowych baz danych i uruchomienia wcześniejszego wyszukiwania w zautomatyzowanym systemie identyfikacji daktyloskopijnej pozostałych państw członkowskich zgodnie z decyzją 2008/615/WSiSW. Zasada wcześniejszego wyszukiwania skutecznie ogranicza możliwość korzystania z tych systemów przez organy państw członkowskich w uzasadnionych celach ścigania przestępstw, może zatem prowadzić do straconych szans na odnalezienie potrzebnych informacji. Wymogi wcześniejszego przeszukania krajowych baz danych i uruchomienia wcześniejszego wyszukiwania w zautomatyzowanym systemie identyfikacji daktyloskopijnej pozostałych państw członkowskich zgodnie z decyzją 2008/615/WSiSW powinny przestać obowiązywać dopiero wówczas, gdy wejdzie w życie alternatywne zabezpieczenie w postaci dwuetapowego podejścia do dostępu organów ścigania za pośrednictwem wspólnego repozytorium tożsamości.

(35) Należy ustanowić moduł wykrywający multiplikację, aby wspierać funkcjonowanie wspólnego repozytorium tożsamości oraz osiągnięcie celów systemów EES, VIS, [ETIAS], Eurodac, SIS i [ECRIS-TCN]. Aby skutecznie osiągnąć ich cele, wszystkie te systemy informacyjne UE wymagają dokładnej identyfikacji osób, których dane są w nich przechowywane.

(36) Możliwość osiągnięcia celów systemów informacyjnych UE podważa aktualna niezdolność władz do korzystania z tych systemów w celu przeprowadzania wystarczająco rzetelnej weryfikacji tożsamości obywateli państw trzecich, których dane są przechowywane w różnych systemach. O tej niezdolności decyduje fakt, że zestaw danych dotyczących tożsamości przechowywanych w danym systemie może być fałszywy, niepoprawny lub niepełny, obecnie natomiast brakuje możliwości wykrycia takich fałszywych, niepoprawnych lub niepełnych danych dotyczących tożsamości poprzez porównywanie ich z danymi przechowywanymi w innym systemie. Aby zaradzić tej sytuacji, konieczne jest dysponowanie instrumentem technicznym na szczeblu Unii, który umożliwiałby dokładną identyfikację obywateli państw trzecich w tych celach.

(37) Moduł wykrywający multiplikację tożsamości powinien stworzyć i przechowywać powiązania między danymi w różnych systemach informacyjnych UE, aby wykrywać multiplikację tożsamości, w podwójnym celu ułatwienia kontroli tożsamości osób podróżujących w dobrej wierze i zwalczania oszustw dotyczących tożsamości. Będzie on zawierał jedynie powiązania między osobami obecnymi w więcej niż jednym systemie informacyjnym UE, w zakresie ściśle ograniczonym do danych potrzebnych do weryfikacji, czy dana osoba została zgodnie lub niezgodnie z prawem zarejestrowana pod różnymi tożsamościami biograficznymi w różnych systemach, lub wyjaśnienia sytuacji, w których dwie osoby o podobnych danych biograficznych mogą nie być tą samą osobą. Przetwarzanie danych za pośrednictwem europejskiego portalu wyszukiwania i serwisu kojarzenia danych biometrycznych w celu powiązania akt osobowych w poszczególnych systemach należy sprowadzić do absolutnego minimum, ogranicza się ono zatem do wykrywania multiplikacji tożsamości w chwili dodawania nowych danych do jednego z systemów informacyjnych włączonych do wspólnego repozytorium tożsamości i SIS. Moduł wykrywający multiplikację tożsamości powinien zawierać zabezpieczenia przed potencjalną dyskryminacją lub nieprzychylnymi decyzjami wobec osób posługujących się różnymi tożsamościami w sposób zgodny z prawem.

(38) Niniejsze rozporządzenie przewiduje nowe operacje przetwarzania danych mające na celu poprawną identyfikację osób, których to dotyczy. Stanowi to ingerencję w ich prawa podstawowe chronione na mocy art. 7 i 8 Karty praw podstawowych Unii Europejskiej. Ponieważ skuteczne wdrożenie systemów informacyjnych UE zależy od poprawnej identyfikacji odpowiednich osób, taka ingerencja jest uzasadniona tymi samymi celami, dla których ustanowiono każdy z tych systemów, a mianowicie celami skutecznego zarządzania granicami Unii, bezpieczeństwa wewnętrznego Unii oraz skutecznego wdrażania polityk Unii w zakresie wiz i azylu oraz zwalczania nielegalnej migracji.

(39) Europejski portal wyszukiwania i wspólny serwis kojarzenia danych biometrycznych powinny porównywać dane dotyczące osób we wspólnym repozytorium tożsamości i w SIS przy tworzeniu nowych wpisów przez władze krajowe lub organy UE. Takie porównywanie powinno odbywać się automatycznie. Wspólne repozytorium tożsamości i SIS powinny korzystać ze wspólnego serwisu kojarzenia danych biometrycznych, aby wykrywać możliwe powiązania na podstawie danych biometrycznych. Wspólne repozytorium tożsamości i SIS powinny korzystać z europejskiego portalu wyszukiwania, aby wykrywać możliwe powiązania na podstawie danych alfanumerycznych. Wspólne repozytorium tożsamości i SIS powinny móc identyfikować identyczne lub podobne dane dotyczące obywatela państwa trzeciego przechowywane w różnych systemach. W takich przypadkach należy ustanowić powiązanie wskazujące, że jest to ta sama osoba. Wspólne repozytorium tożsamości i SIS powinny być tak skonfigurowane, aby wykrywały drobne błędy transliteracji lub zapisu w sposób, który nie przysparzałby danemu obywatelowi państwa trzeciego nieuzasadnionych trudności.

(40) Organ krajowy lub unijny, który zarejestrował dane w odpowiednim systemie informacyjnym UE, powinien potwierdzić takie powiązania lub wprowadzić w nim zmiany. Organ ten powinien mieć dostęp do danych przechowywanych we wspólnym repozytorium tożsamości lub w SIS oraz w module wykrywającym multiplikację tożsamości w celu ręcznej weryfikacji tożsamości.

(41) Dostęp do modułu wykrywającego multiplikację tożsamości dla organów państw członkowskich i unijnych, które mają dostęp do co najmniej jednego systemu informacyjnego UE objętego wspólnym repozytorium tożsamości lub do SIS, powinien ograniczać się do tzw. powiązań czerwonych, w których powiązane ze sobą dane wskazują na obecność takich samych danych biometrycznych, lecz różnych danych dotyczących tożsamości, a organ odpowiedzialny za weryfikację różniących się tożsamości stwierdzi, że odnoszą się one do tej samej osoby z naruszeniem prawa, lub w przypadkach, w których powiązane ze sobą dane wykażą obecność podobnych danych dotyczących tożsamości i organ odpowiedzialny za weryfikację różniących się tożsamości stwierdzi, że odnoszą się one do tej samej osoby z naruszeniem prawa. Jeśli powiązane ze sobą dane dotyczące tożsamości nie są podobne, należy ustanowić powiązanie żółte i przeprowadzić weryfikację ręczną, aby potwierdzić to powiązanie lub odpowiednio zmienić jego kolor.

(42) Organ odpowiedzialny za tworzenie lub aktualizację danych, które spowodowały trafienie prowadzące do ustanowienia powiązania do danych już przechowywanych w innym systemie informacyjnym UE, zapewnia przeprowadzenie ręcznej weryfikacji multiplikacji tożsamości. Organ odpowiedzialny za wykrywanie różniących się tożsamości powinien ocenić, czy te różne tożsamości są zgodne z prawem, czy nie. Oceny tej w miarę możliwości należy dokonać w obecności danego obywatela państwa trzeciego, w stosownych przypadkach zwracając się o dodatkowe wyjaśnienia

lub informacje. Oceny takiej należy dokonać niezwłocznie, zgodnie z wymogami prawnymi dotyczącymi dokładności informacji na mocy prawa Unii i prawa krajowego.

(43) W przypadku powiązań uzyskanych w związku z Systemem Informacyjnym Schengen (SIS) odnoszących się do wpisów dotyczących osób poszukiwanych w celu aresztowania i wydania lub ekstradycji, osobami zaginionymi lub narażonymi na zagrożenia, osobami, których obecność jest wymagana do celów postępowania sądowego, osobami poddawanymi kontrolom niejawnym lub kontrolom szczególnym lub nieznanymi osobami poszukiwanymi organem odpowiedzialnym za weryfikację multiplikacji tożsamości powinno być biuro Sirene państwa członkowskiego, które dokonało wpisu. W istocie powyższe kategorie wpisów w SIS mają charakter wrażliwy i nie muszą być przekazywane organom tworzącym lub aktualizującym dane w którymś z pozostałych systemów informacyjnych UE. Utworzenie powiązania do danych SIS nie powinno wpływać na działania podejmowane zgodnie z [rozporządzeniami w sprawie SIS].

(44) Agencja eu-LISA powinna ustanowić mechanizmy automatycznej kontroli jakości danych i wspólne wskaźniki jakości danych. Agencja ta powinna odpowiadać za rozwinięcie centralnych zdolności monitorowania jakości danych oraz sporządzać regularne sprawozdania z analizy danych, aby poprawić kontrolę wdrażania i stosowania systemów informacyjnych UE przez państwa członkowskie. Wspólne wskaźniki jakości powinny obejmować minimalne normy jakości w zakresie przechowywania danych w systemach informacyjnych UE lub elementach interoperacyjności. Celem takich norm kontroli jakości danych powinna być automatyczna identyfikacja przez systemy informacyjne UE i elementy interoperacyjności wprowadzonych danych wyglądających na niespójne lub nieprawidłowe, tak aby państwo członkowskie, z którego te dane pochodzą, mogło je sprawdzić i podjąć wszelkie konieczne środki naprawcze.

(45) Komisja powinna dokonywać oceny sprawozdań z jakości przedkładanych przez eu-LISA i w razie potrzeby wydawać zalecenia dla państw członkowskich. Państwa członkowskie powinny odpowiadać za sporządzenie planu działania opisującego czynności mające zaradzić wszelkim niedoskonałościom jakości danych oraz przedstawiać regularne sprawozdania z postępów w jego realizacji.

(46) Uniwersalny format wiadomości (UMF) powinien stanowić standard dla uporządkowanej, transgranicznej wymiany informacji między systemami informacyjnymi, organami lub organizacjami działającymi w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych. Powinien on określać wspólny język i struktury logiczne wzajemnie wymienianych informacji, aby ułatwić interoperacyjność poprzez umożliwienie tworzenia i odczytywania wymienianych treści w sposób spójny i semantycznie równoważny.

(47) Należy ustanowić centralne repozytorium sprawozdawczo-statystyczne, aby generować międzysystemowe dane statystyczne i sprawozdania analityczne na potrzeby strategii politycznych, działań operacyjnych i zapewniania jakości danych. Agencja eu-LISA powinna ustanowić, wdrożyć i obsługiwać to repozytorium w swoich witrynach technicznych zawierających anonimowe dane statystyczne z powyższych systemów, wspólne repozytorium tożsamości, moduł wykrywający multiplikację tożsamości i wspólny serwis kojarzenia danych biometrycznych. Dane zawarte w centralnym repozytorium sprawozdawczo-statystycznym nie powinny umożliwiać identyfikacji osób fizycznych. Agencja eu-LISA ma obowiązek

anonimizacji danych i gromadzenia takich anonimowych danych w tym repozytorium. Proces anonimizacji danych powinien przebiegać automatycznie, a pracownicy eu-LISA nie powinni otrzymywać bezpośredniego dostępu do żadnych danych osobowych przechowywanych w systemach informacyjnych UE lub w elementach interoperacyjności.

(48) W stosunku do przetwarzania danych osobowych przez władze krajowe na mocy niniejszego rozporządzenia obowiązują przepisy rozporządzenia (UE) 2016/679, z wyjątkiem sytuacji, gdy takiego przetwarzania dokonują wyznaczone organy lub centralne punkty dostępu państw członkowskich w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie dochodzeń, kiedy to obowiązują przepisy dyrektywy (UE) 2016/680 Parlamentu Europejskiego i Rady.

(49) W stosunku do przetwarzania danych osobowych przez odpowiednie powyższe systemy obowiązują szczegółowe przepisy dotyczące ochrony danych [rozporządzenia w sprawie EES], rozporządzenia nr 767/2008, [rozporządzenia w sprawie ETIAS] i [rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych].

(50) W stosunku do przetwarzania danych osobowych przez eu-LISA oraz pozostałe instytucje i organy Unii przy wykonywaniu ich obowiązków na mocy niniejszego rozporządzenia obowiązują przepisy rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady[59], nie naruszając przepisów rozporządzenia (UE) 2016/794, które obowiązują w stosunku do przetwarzania danych osobowych przez Europol.

(51) Krajowe organy nadzoru ustanowione zgodnie z [rozporządzeniem (UE) 2016/679] powinny kontrolować zgodność z prawem przetwarzania danych osobowych przez państwa członkowskie, natomiast Europejski Inspektor Ochrony Danych ustanowiony rozporządzeniem (WE) nr 45/2001 powinien monitorować działalność instytucji i organów UE w odniesieniu do przetwarzania danych osobowych. Europejski Inspektor Ochrony Danych i organy nadzorcze powinny współpracować ze sobą w zakresie monitorowania przetwarzania danych osobowych przez elementy interoperacyjności.

(52) „(...) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu ...".

(53) Odpowiednie przepisy Regulaminu pracowniczego urzędników i warunków zatrudnienia innych pracowników Unii Europejskiej dotyczące poufności powinny mieć zastosowanie do urzędników lub innych pracowników, którzy są zatrudnieni i pracują przy SIS.

(54) Zarówno państwa członkowskie, jak i eu-LISA powinny utrzymywać plany ochrony, aby ułatwić wdrożenie obowiązków w zakresie bezpieczeństwa, oraz współpracować ze sobą w celu rozwiązywania problemów związanych z bezpieczeństwem. Agencja eu-LISA powinna też zapewniać stałe wprowadzanie najnowszych rozwiązań technologicznych, aby zapewnić integralność danych w ramach rozwoju i projektowania elementów interoperacyjności oraz zarządzania nimi.

(55) Wdrożenie elementów interoperacyjności, o których mowa w niniejszym rozporządzeniu, będzie mieć wpływ na sposób przeprowadzania kontroli na przejściach granicznych. Oddziaływanie to będzie wynikać z łącznego stosowania

[59] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

aktualnych przepisów rozporządzenia (UE) 2016/399 Parlamentu Europejskiego i Rady[60] oraz przepisów w sprawie interoperacyjności zawartych w niniejszym rozporządzeniu.

(56) W wyniku takiego łącznego stosowania przepisów to europejski portal wyszukiwania powinien stanowić główny punkt dostępu służący przeprowadzaniu obowiązkowego i systematycznego przeglądania baz danych przewidzianych w kodeksie granicznym Schengen w stosunku do obywateli państw trzecich na przejściach granicznych. Dodatkowo dane dotyczące tożsamości, które doprowadziły do ustalenia klasyfikacji powiązania w module wykrywającym multiplikację tożsamości jako powiązania czerwonego, powinny być brane pod uwagę przez funkcjonariuszy straży granicznej przy ocenie, czy dana osoba spełnia warunki wjazdu określone w kodeksie granicznym Schengen. Obecność powiązania czerwonego sama w sobie nie powinna jednak stanowić przyczyny odmowy wjazdu, a istniejący wykaz warunków odmowy wjazdu zawarty w kodeksie granicznym Schengen nie powinien zatem ulec zmianie.

(57) Należałoby zaktualizować Praktyczny podręcznik dla straży granicznej, aby to jasno sprecyzować.

(58) Konieczna będzie jednak zmiana rozporządzenia (UE) 2016/399, aby dodać spoczywający na funkcjonariuszu straży granicznej obowiązek skierowania obywatela państwa trzeciego do kontroli drugiej linii w wypadku, gdyby użycie modułu wykrywającego multiplikację tożsamości za pośrednictwem europejskiego portalu wyszukiwania wykazało obecność powiązania żółtego lub czerwonego, aby nie przedłużać czasu oczekiwania w kontroli pierwszej linii.

(59) Jeśli użycie modułu wykrywającego multiplikację tożsamości za pośrednictwem europejskiego portalu wyszukiwania wykaże obecność powiązania żółtego lub czerwonego, funkcjonariusz straży granicznej dokonujący kontroli drugiej linii powinien wprowadzić zapytanie do wspólnego repozytorium tożsamości lub Systemu Informacyjnego Schengen lub do obu, aby uzyskać dostęp do informacji o kontrolowanej osobie, ręcznie zweryfikować jej odmienną tożsamość i w razie potrzeby odpowiednio dostosować kolor powiązania.

(60) Na potrzeby statystyk i sprawozdawczości konieczne jest przyznanie dostępu uprawnionym pracownikom właściwych władz, instytucji i organów wskazanych w niniejszym rozporządzeniu, aby mogli przeglądać niektóre dane związane z pewnymi elementami interoperacyjności bez umożliwiania im identyfikacji osoby fizycznej.

(61) Aby umożliwić właściwym organom i organom unijnym dostosowanie się do nowych wymogów w zakresie korzystania z europejskiego portalu wyszukiwania, konieczne jest ustanowienie okresu przejściowego. Podobnie aby umożliwić spójne i optymalne funkcjonowanie modułu wykrywającego multiplikację tożsamości należy, na początku jego działania, ustanowić środki przejściowe.

(62) Koszty opracowania elementów interoperacyjności przewidzianych w obecnych wieloletnich ramach finansowych są niższe niż pozostała kwota przeznaczona w budżecie na inteligentne granice zgodnie z rozporządzeniem (UE) nr 515/2014 Parlamentu Europejskiego i Rady[61]. W związku z powyższym zgodnie z art. 5 ust. 5

[60] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice, Dz.U. L 77 z 23.3.2016, s. 1.

[61] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 515/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia

lit. b) rozporządzenia (UE) nr 515/2014 w niniejszym rozporządzeniu powinno się ponownie przydzielić kwotę przewidzianą obecnie na rozwijanie systemów informatycznych wspomagających zarządzanie przepływami migracyjnymi przez granice zewnętrzne.

(63) Aby uzupełnić pewne szczegółowe aspekty techniczne niniejszego rozporządzenia należy delegować Komisji uprawnienia do przyjmowania aktów ustawodawczych zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w zakresie profili użytkowników europejskiego portalu wyszukiwania oraz treści i formatu odpowiedzi udzielanych przez ten portal. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.[62]. W szczególności aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te powinny otrzymywać wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji powinni systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(64) Aby zapewnić jednolite warunki wykonania niniejszego rozporządzenia, należy przyznać Komisji uprawnienia wykonawcze obejmujące przyjmowanie szczegółowych przepisów w zakresie: mechanizmów, procedur i wskaźników związanych z automatyczną kontrolą jakości danych; rozwijania standardu uniwersalnego formatu wiadomości (UMF); procedur ustalania przypadków podobieństwa tożsamości; prowadzenia centralnego repozytorium sprawozdawczo-statystycznego; oraz procedury współpracy na wypadek incydentów bezpieczeństwa. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[63].

(65) W stosunku do wszelkiego przetwarzania danych Europolu na potrzeby niniejszego rozporządzenia obowiązują przepisy rozporządzenia 2016/794.

(66) Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2004/38/WE.

(67) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen.

(68) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje. Ponieważ niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, zgodnie z art. 4 tego protokołu Dania — w terminie sześciu miesięcy po przyjęciu niniejszego rozporządzenia — podejmie decyzję, czy dokona jego transpozycji do prawa krajowego.

(69) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Zjednoczonego Królestwa, zgodnie z decyzją Rady

---

finansowego w zakresie granic zewnętrznych i wiz oraz uchylające decyzję nr 574/2007/WE (Dz.U. L 150 z 20.5.2014, s. 143).

[62] http://eur-lex.europa.eu/legal-content/EN-PL/TXT/?uri=CELEX:32016Q0512(01)&from=PL.

[63] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

2000/365/WE[64]; Zjednoczone Królestwo nie uczestniczy zatem w przyjęciu niniejszego rozporządzenia, nie jest nim związane ani go nie stosuje.

(70) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Irlandii zgodnie z decyzją Rady 2002/192/WE[65]; Irlandia nie uczestniczy w związku z tym w przyjęciu niniejszego rozporządzenia, nie jest nim związana ani go nie stosuje.

(71) W odniesieniu do Islandii i Norwegii niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, w rozumieniu umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii, dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[66], który należy do dziedziny, o której mowa w art. 1 pkt A, B i G decyzji Rady 1999/437/WE z dnia 17 maja 1999 r. w sprawie niektórych warunków stosowania tej umowy[67].

(72) W odniesieniu do Szwajcarii niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[68], które wchodzą w zakres obszaru, o którym mowa w art. 1 pkt A, B i G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2008/146/WE[69].

(73) W odniesieniu do Liechtensteinu niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu o przystąpieniu Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku[70] Schengen, które wchodzą w zakres obszaru, o którym mowa w art. 1 pkt A, B i G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2011/350/UE[71].

(74) W odniesieniu do Cypru przepisy związane z systemami SIS i VIS stanowią akty oparte na dorobku Schengen lub w inny sposób z nim związane w rozumieniu art. 3 ust. 2 Aktu przystąpienia z 2003 r.

(75) W odniesieniu do Bułgarii i Rumunii przepisy związane z systemami SIS i VIS stanowią akty oparte na dorobku Schengen lub w inny sposób z nim związane w rozumieniu art. 4 ust. 2 Aktu przystąpienia z 2005 r., w związku z decyzją Rady 2010/365/UE[72] i decyzją Rady (UE) 2017/1908[73].

---

[64] Decyzja Rady 2000/365/WE z dnia 29 maja 2000 r. dotycząca wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowanie wobec niego niektórych przepisów dorobku Schengen (Dz.U. L 131 z 1.6.2000, s. 43).

[65] Decyzja Rady 2002/192/WE z dnia 28 lutego 2002 r. dotycząca wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen (Dz.U. L 64 z 7.3.2002, s. 20).

[66] Dz.U. L 176 z 10.7.1999, s. 36.

[67] Dz.U. L 176 z 10.7.1999, s. 31.

[68] Dz.U. L 53 z 27.2.2008, s. 52.

[69] Dz.U. L 53 z 27.2.2008, s. 1.

[70] Dz.U. L 160 z 18.6.2011, s. 21.

[71] Dz.U. L 160 z 18.6.2011, s. 19.

[72] Decyzja Rady 2010/365/UE z dnia 29 czerwca 2010 r. w sprawie stosowania w Republice Bułgarii i w Rumunii przepisów dorobku Schengen związanych z systemem informacyjnym Schengen (Dz.U. L 166 z 1.7.2010, s. 17).

(76) W odniesieniu do Chorwacji przepisy związane z systemami SIS i VIS stanowią akty oparte na dorobku Schengen lub w inny sposób z nim związane w rozumieniu art. 4 ust. 2 Aktu przystąpienia z 2011 r., w związku z decyzją Rady (UE) 2017/733[74].

(77) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej oraz powinno być stosowane zgodnie z tymi prawami i zasadami.

(78) Aby niniejsze rozporządzenie było spójne z obowiązującymi ramami prawnymi, rozporządzenie (UE) 2016/399, rozporządzenie (UE) 2017/2226, decyzja Rady 2008/633/WSiSW, rozporządzenie (WE) nr 767/2008 i decyzja Rady 2004/512/WE powinny zostać odpowiednio zmienione,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I
Przepisy ogólne

Artykuł 1
Przedmiot

1. Niniejsze rozporządzenie, wraz z [rozporządzeniem 2018/xx w sprawie interoperacyjności w zakresie współpracy policyjnej i sądowej, azylu i migracji], ustanawia ramy zapewniające interoperacyjność między systemem wjazdu/wyjazdu (EES), wizowym systemem informacyjnym (VIS), [europejskim systemem informacji o podróży oraz zezwoleń na podróż (ETIAS)], systemem Eurodac, Systemem Informacyjnym Schengen (SIS) oraz [europejskim systemem przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN)], aby te systemy i dane mogły się wzajemnie uzupełniać.

2. Ramy te obejmują następujące elementy interoperacyjności:

   a) europejski portal wyszukiwania;

   b) wspólny serwis kojarzenia danych biometrycznych;

   c) wspólne repozytorium tożsamości;

   d) moduł wykrywający multiplikację tożsamości.

3. Niniejsze rozporządzenie określa także przepisy dotyczące wymogów jakości danych, uniwersalnego formatu wiadomości (UMF) oraz centralnego repozytorium sprawozdawczo-statystycznego, a także określa obowiązki państw członkowskich i Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) w odniesieniu do projektowania i działania elementów interoperacyjności.

---

[73] Decyzja Rady (UE) 2017/1908 z dnia 12 października 2017 r. w sprawie wprowadzenia w życie w Republice Bułgarii i w Rumunii niektórych przepisów dorobku Schengen dotyczących wizowego systemu informacyjnego (Dz.U. L 269 z 19.10.2017, s. 39).

[74] Decyzja Rady (UE) 2017/733 z dnia 25 kwietnia 2017 r. w sprawie stosowania w Republice Chorwacji przepisów dorobku Schengen dotyczących Systemu Informacyjnego Schengen (Dz.U. L 108 z 26.4.2017, s. 31).

4. Rozporządzenie dostosowuje także procedury i warunki dostępu organów ścigania państw członkowskich i Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) do systemu wjazdu/wyjazdu (EES), wizowego systemu informacyjnego (VIS), [europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)] oraz systemu Eurodac na potrzeby działań związanych z zapobieganiem przestępstwom terrorystycznym lub innym poważnym przestępstwom oraz ich wykrywaniem i prowadzeniem w ich sprawie dochodzeń, leżących w granicach ich kompetencji.

Artykuł 2
Cele interoperacyjności

5. Poprzez zapewnienie interoperacyjności niniejsze rozporządzenie służy następującym celom:

   a) usprawnieniu zarządzania granicami zewnętrznymi;

   b) przyczynieniu się do zapobiegania nielegalnej migracji i jej zwalczania;

   c) zapewnianiu wysokiego poziomu bezpieczeństwa w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej, w tym utrzymania bezpieczeństwa publicznego i polityki publicznej oraz zagwarantowania bezpieczeństwa na terytoriach państw członkowskich;

   d) poprawie wdrażania wspólnej polityki wizowej; oraz

   e) pomocy w rozpatrywaniu wniosków o udzielenie ochrony międzynarodowej.

6. Cele zapewnienia interoperacyjności są osiągane poprzez:

   a) zapewnienie poprawnej identyfikacji osób;

   b) wspieranie walki z oszustwami dotyczącymi tożsamości;

   c) poprawę i harmonizację wymogów dotyczących jakości danych w poszczególnych systemach informacyjnych UE;

   d) ułatwienie technicznego i operacyjnego wdrożenia przez państwa członkowskie istniejących i przyszłych systemów informacyjnych UE;

   e) wzmocnienie i uproszczenie oraz ujednolicenie warunków bezpieczeństwa danych i ochrony danych regulujących odpowiednie systemy informacyjne UE;

   f) usprawnienie warunków dostępu organów ścigania do systemów EES, VIS, [ETIAS] i Eurodac;

   g) wspieranie realizacji celów systemów EES, VIS, [ETIAS], Eurodac, SIS i [ECRIS-TCN].

Artykuł 3
Zakres

7. Niniejsze rozporządzenie stosuje się do [systemu wjazdu/wyjazdu (EES)], wizowego systemu informacyjnego (VIS), [europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)] i Systemu Informacyjnego Schengen.

8. Rozporządzenie obowiązuje w stosunku do osób, których dane osobowe mogą być przetwarzane za pomocą systemów informacyjnych UE, o których mowa w ust. 1.

Artykuł 4
Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „granice zewnętrzne” oznaczają granice zewnętrzne zgodnie z definicją zawartą w art. 2 ust. 2 rozporządzenia (UE) 2016/399;

2) „odprawa graniczna” oznacza czynności kontrolne przeprowadzane na przejściach granicznych zgodnie z definicją zawartą w art. 2 ust. 11 rozporządzenia (UE) 2016/399;

3) „służba graniczna” oznacza straż graniczną wyznaczoną zgodnie z przepisami prawa krajowego do przeprowadzania odpraw granicznych;

4) „organy nadzorcze” oznaczają organ nadzorczy ustanowiony zgodnie z art. 51 ust. 1 rozporządzenia (UE) 2016/679 oraz organ nadzorczy ustanowiony zgodnie z art. 41 ust. 1 dyrektywy (UE) 2016/680;

5) „weryfikacja” oznacza proces porównywania zestawów danych w celu ustalenia autentyczności podawanej tożsamości (kontrola jeden do jednego);

6) „identyfikacja” oznacza proces ustalania tożsamości osoby poprzez przeszukiwanie bazy danych w oparciu o różne zestawy danych (kontrola jeden do wielu);

7) „obywatel państwa trzeciego” oznacza osobę niebędącą obywatelem Unii w rozumieniu art. 20 ust. 1 Traktatu lub bezpaństwowca lub osobę o nieznanym obywatelstwie;

8) „dane alfanumeryczne” oznaczają dane wyrażone literami, cyframi, znakami specjalnymi, odstępami i znakami przestankowymi;

9) „dane dotyczące tożsamości” oznaczają dane, o których mowa w art. 27 ust. 3, lit. a)–h);

10) „dane daktyloskopijne” oznaczają dane dotyczące odcisków palców osoby fizycznej;

11) „wizerunek twarzy” oznacza cyfrowe wizerunki twarzy;

12) „dane biometryczne” oznaczają dane daktyloskopijne lub wizerunek twarzy;

13) „wzorzec biometryczny” oznacza matematyczną reprezentację uzyskaną przez ekstrakcję cech z danych biometrycznych ograniczoną do właściwości koniecznych do dokonywania identyfikacji i weryfikacji;

14) „dokument podróży” oznacza paszport lub inny równoważny dokument, który upoważnia jego posiadacza do przekraczania granic zewnętrznych i w którym może być umieszczona wiza;

15) „dane dokumentu podróży” oznaczają rodzaj, numer i państwo wydania dokumentu podróży, datę upływu ważności dokumentu podróży i trzyliterowy kod państwa wydającego dokument podróży;

16) „zezwolenie na podróż” oznacza zezwolenie na podróż określone w art. 3 [rozporządzenia w sprawie ETIAS];

17) „wiza krótkoterminowa” oznacza wizę określoną w art. 2 ust. 2 lit. a) rozporządzenia (WE) nr 810/2009;

18) „systemy informacyjne UE” oznaczają wielkoskalowe systemy informatyczne zarządzane przez eu-LISA;

19) „dane Europolu” oznaczają dane osobowe przekazane Europolowi w celu, o którym mowa w art. 18 ust. 2 lit. a) rozporządzenia (UE) 2016/794;

20) „bazy danych Interpolu” oznaczają bazę Interpolu zawierającą dane skradzionych lub utraconych dokumentów podróży (SLTD) i bazę danych TDAWN Interpolu;

21) „dopasowanie” oznacza istnienie zgodności ustalone w wyniku porównania dwóch lub większej liczby wystąpień danych osobowych zarejestrowanych lub będących w trakcie rejestrowania w systemie informacyjnym lub bazie danych;

22) „trafienie” oznacza potwierdzenie jednego dopasowania lub większej ich liczby;

23) „organ policji” oznacza „właściwy organ” zgodnie z definicją określoną w art. 3 ust. 7 dyrektywy 2016/680;

24) „wyznaczone organy” oznaczają wyznaczone przez państwo członkowskie organy, o których mowa w art. 29 ust. 1 rozporządzenia (UE) 2017/2226, art. 3 ust. 1 decyzji Rady 2008/633/WSiSW, [art. 43 rozporządzenia w sprawie ETIAS] i [art. 6 rozporządzenia w sprawie Eurodac];

25) „przestępstwo terrorystyczne” oznacza określone w prawie krajowym przestępstwo odpowiadające lub równoważne jednemu z przestępstw, o których mowa w dyrektywie (UE) 2017/541;

26) „poważne przestępstwo” oznacza przestępstwo odpowiadające lub równoważne jednemu z przestępstw, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW, jeżeli zgodnie z prawem krajowym podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat;

27) „EES” oznacza system wjazdu/wyjazdu, o którym mowa w rozporządzeniu (UE) 2017/2226;

28) „VIS” oznacza wizowy system informacyjny, o którym mowa w rozporządzeniu (WE) nr 767/2008;

29) [„ETIAS” oznacza europejski system informacji o podróży oraz zezwoleń na podróż, o którym mowa w rozporządzeniu w sprawie ETIAS];

30) „Eurodac” oznacza system Eurodac, o którym mowa w [rozporządzeniu w sprawie Eurodac];

31) „SIS” oznacza System Informacyjny Schengen, o którym mowa [w rozporządzeniu w sprawie SIS w odniesieniu do odpraw granicznych, rozporządzeniu w sprawie SIS w odniesieniu do ścigania przestępstw i rozporządzeniu w sprawie SIS w odniesieniu do nielegalnych powrotów];

32) [„system ECRIS-TCN” oznacza europejski system przekazywania informacji z rejestrów karnych zawierający informacje o wyrokach skazujących w odniesieniu do obywateli państw trzecich i bezpaństwowców, o którym mowa w rozporządzeniu w sprawie ECRIS-TCN];

33) „ESP” oznacza europejski portal wyszukiwania, o którym mowa w art. 6;

34) „wspólny serwis kojarzenia danych biometrycznych” oznacza wspólny serwis kojarzenia danych biometrycznych, o którym mowa w art. 15;

35) „wspólne repozytorium tożsamości” oznacza wspólne repozytorium tożsamości, o którym mowa w art. 17;

36) „moduł wykrywający multiplikację tożsamości” oznacza moduł wykrywający multiplikację tożsamości, o którym mowa w art. 25;

37) „centralne repozytorium sprawozdawczo-statystyczne” oznacza centralne repozytorium sprawozdawczo-statystyczne, o którym mowa w art. 39.

Artykuł 5
Zakaz dyskryminacji

Przetwarzanie danych osobowych do celów niniejszego rozporządzenia nie może prowadzić do dyskryminacji z jakichkolwiek względów takich jak płeć, pochodzenie rasowe lub etniczne, religia lub przekonania, niepełnosprawność, wiek lub orientacja seksualna. Odbywa się ono z pełnym poszanowaniem godności ludzkiej i integralności osoby. Szczególną uwagę poświęca się dzieciom, osobom starszym i niepełnosprawnym.

ROZDZIAŁ II
Europejski portal wyszukiwania

Artykuł 6
Europejski portal wyszukiwania

9. Europejski portal wyszukiwania ustanawia się, aby zapewnić władzom państw członkowskich i organom UE uzyskiwanie szybkiego, sprawnego, wydajnego, systematycznego i kontrolowanego dostępu do systemów informacyjnych UE, danych Europolu i baz danych Interpolu koniecznych do pełnienia przez nie swoich funkcji, zgodnie z przysługującymi im prawami dostępu, a także aby wspierać realizację celów systemów EES, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN] i danych Europolu.

10. ESP składa się z:

a) infrastruktury centralnej obejmującej portal wyszukiwania umożliwiający jednoczesną konsultację systemów EES, VIS, [ETIAS], Eurodac, SIS, [ECRIS-TCN] oraz danych Europolu i baz danych Interpolu;

b) bezpiecznego kanału komunikacji między ESP a państwami członkowskimi i organami UE uprawnionymi do korzystania z portalu zgodnie z prawem Unii;

c) bezpiecznej infrastruktury komunikacyjnej między ESP a systemami EES, VIS, [ETIAS], Eurodac, systemem centralnym Systemu Informacyjnego Schengen (C.SIS), [systemem ECRIS-TCN], danymi Europolu i bazami danych Interpolu, a także między ESP a infrastrukturą centralną wspólnego repozytorium tożsamości i modułem wykrywającym multiplikację tożsamości.

11. Europejski portal wyszukiwania opracowuje agencja eu-LISA, która zarządza nim również od strony technicznej.

Artykuł 7
Korzystanie z europejskiego portalu wyszukiwania

12. Korzystanie z europejskiego portalu wyszukiwania jest zarezerwowane dla organów państw członkowskich i organów UE mających dostęp do systemów EES, [ETIAS], VIS, SIS, Eurodac i [systemu ECRIS-TCN], wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości oraz do danych Europolu i baz danych Interpolu, zgodnie z prawem Unii i przepisami krajowymi regulującymi ten dostęp.

13. Organy, o których mowa w ust. 1, korzystają z europejskiego portalu wyszukiwania, aby wyszukiwać dane dotyczące osób lub ich dokumentów podróży przechowywane w systemach centralnych EES, VIS i [ETIAS] zgodnie z prawami dostępu przysługującymi im na mocy prawa Unii i przepisów prawa krajowego. Korzystają one także z portalu, aby konsultować wspólne repozytorium tożsamości zgodnie z prawami dostępu przysługującymi im na mocy niniejszego rozporządzenia w celach, o których mowa w art. 20, 21 i 22.

14. Organy państw członkowskich, o których mowa w ust. 1, mogą z niego korzystać, aby wyszukiwać dane dotyczące osób lub ich dokumentów podróży w C.SIS zgodnie z [rozporządzeniem w sprawie SIS w odniesieniu do odpraw granicznych i rozporządzeniem w sprawie SIS w odniesieniu do ścigania przestępstw]. Dostęp do C.SIS za pośrednictwem europejskiego portalu wyszukiwania odbywa się za pomocą systemu krajowego (N.SIS) każdego państwa członkowskiego zgodnie z [art. 4 ust. 2 rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych i rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw].

15. Organy UE korzystają z europejskiego portalu wyszukiwania, aby wyszukiwać dane dotyczące osób lub ich dokumentów podróży w C.SIS.

16. Organy, o których mowa w ust. 1, mogą korzystać z europejskiego portalu wyszukiwania, aby wyszukiwać dane dotyczące osób lub ich dokumentów podróży przechowywane w bazach danych Interpolu zgodnie z prawami dostępu przysługującymi im na mocy prawa Unii i przepisów prawa krajowego.

Artykuł 8
Profile użytkowników europejskiego portalu wyszukiwania

17. Aby umożliwić korzystanie z europejskiego portalu wyszukiwania eu-LISA opracowuje odrębny profil dla każdej kategorii użytkownika portalu zgodnie ze szczegółowymi informacjami technicznymi i prawami dostępu, o których mowa w ust. 2, który zgodnie z przepisami prawa Unii i prawa krajowego obejmuje:

    a) pola danych wykorzystywane w zapytaniach;

    b) systemy informacyjne UE, dane Europolu i bazy danych Interpolu, które są i mogą być przeglądane oraz w których użytkownik znajduje odpowiedź; oraz

    c) dane przekazywane w każdej odpowiedzi.

18. Komisja przyjmuje akty delegowane zgodnie z art. 63, aby określić szczegóły techniczne profili, o których mowa w ust. 1, dla użytkowników europejskiego portalu wyszukiwania określonych w art. 7 ust. 1, zgodnie z przysługującymi im prawami dostępu.

Artykuł 9
Zapytania

19. Użytkownicy europejskiego portalu wyszukiwania mogą dokonywać zapytania poprzez wprowadzenie danych w portalu zgodnie ze swoim profilem użytkownika i przysługującymi im prawami dostępu. Po dokonaniu zapytania portal jednocześnie przeszukuje, za pomocą danych wprowadzonych przez użytkownika, systemy EES, [ETIAS], VIS, SIS, Eurodac, [system ECRIS-TCN] i wspólne repozytorium tożsamości oraz dane Europolu i bazy danych Interpolu.

20. Pola danych stosowane w celu dokonania zapytania za pośrednictwem europejskiego portalu wyszukiwania odpowiadają polom danych związanych z osobami fizycznymi lub dokumentami podróży, których można użyć, aby dokonać zapytania w różnych systemach informacyjnych UE, danych Europolu i bazach danych Interpolu, zgodnie z instrumentami prawnymi, którym te podlegają.

21. Agencja eu-LISA wdraża dokument kontroli interfejsu (DKI) oparty na uniwersalnym formacie wiadomości, o którym mowa w art. 38, w odniesieniu do europejskiego portalu wyszukiwania.

22. Systemy EES, [ETIAS], VIS, SIS, Eurodac, [system ECRIS-TCN], wspólne repozytorium tożsamości i moduł wykrywający multiplikację tożsamości oraz dane Europolu i bazy danych Interpolu dostarczają przechowywanych w nich danych w wyniku zapytania dokonanego za pośrednictwem europejskiego portalu wyszukiwania.

23. Projekt europejskiego portalu wyszukiwania powinien zapewniać, aby podczas przeszukiwania baz danych Interpolu dane użyte przez użytkownika portalu w celu dokonania zapytania nie były przekazywane właścicielom danych Interpolu.

24. Odpowiedź udzielana użytkownikowi europejskiego portalu wyszukiwania jest unikalna i zawiera wszystkie dane, do których użytkownik ten ma dostęp na mocy prawa Unii. W stosownych przypadkach odpowiedź udzielana przez portal wskazuje, do którego systemu informacyjnego lub do której bazy należą dane.

25. Komisja przyjmuje akt delegowany zgodnie z art. 63, w którym szczegółowo określa treść i format odpowiedzi udzielanych przez europejski portal wyszukiwania.

Artykuł 10
Prowadzenie zapisów w rejestrze

26. Nie naruszając przepisów [art. 46 rozporządzenia w sprawie EES], art. 34 rozporządzenia (WE) nr 767/2008, [art. 59 wniosku dotyczącego rozporządzenia w sprawie ETIAS] oraz art. 12 i 18 rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych, eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach europejskiego portalu wyszukiwania. Rejestry te obejmują w szczególności następujące elementy:

a) organ państwa członkowskiego i indywidualnego użytkownika europejskiego portalu wyszukiwania, w tym zastosowany profil użytkownika portalu, o którym mowa w art. 8;

b) datę i godzinę zapytania;

c) przeszukiwane systemy informacyjne UE i bazy danych Interpolu;

d) zgodnie z przepisami krajowymi lub, w stosownych przypadkach, rozporządzeniem (UE) nr 45/2001, identyfikator osoby, która dokonała zapytania.

27. Rejestry można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności zapytania i zgodności przetwarzania danych z prawem, oraz w celu zapewniania bezpieczeństwa danych zgodnie z art. 42. Rejestry są chronione za pomocą odpowiednich środków przed nieuprawnionym dostępem i usuwane jeden rok po ich utworzeniu, chyba że są konieczne do prowadzenia już rozpoczętych procedur monitorowania.

Artykuł 11
Procedury awaryjne w razie braku technicznej możliwości korzystania z europejskiego portalu wyszukiwania

28. Jeśli korzystanie z europejskiego portalu wyszukiwania w celu przeszukania jednego lub większej liczby systemów informacyjnych UE, o których mowa w art. 9 ust. 1, lub wspólnego repozytorium tożsamości nie jest technicznie możliwe z powodu awarii portalu, eu-LISA powiadamia o tym fakcie użytkowników.

29. Jeśli korzystanie z europejskiego portalu wyszukiwania w celu przeszukiwania jednego lub większej liczby systemów informacyjnych UE, o których mowa w art. 9 ust. 1, lub wspólnego repozytorium tożsamości, nie jest technicznie możliwe z powodu awarii infrastruktury krajowej w jednym z państw członkowskich, właściwy organ tego państwa członkowskiego powiadamia o tym fakcie eu-LISA i Komisję.

30. W obu przypadkach, do czasu rozwiązania problemu technicznego obowiązek, o którym mowa w art. 7 ust. 2 i 4, nie obowiązuje, a państwa członkowskie mogą uzyskać dostęp do systemów informacyjnych, o których mowa w art. 9 ust. 1, lub do wspólnego repozytorium tożsamości, za pomocą odpowiedniego jednolitego interfejsu krajowego lub krajowej infrastruktury komunikacyjnej.

ROZDZIAŁ III
Wspólny serwis kojarzenia danych biometrycznych

Artykuł 12
Wspólny serwis kojarzenia danych biometrycznych

31. Wspólny serwis kojarzenia danych biometrycznych gromadzący wzorce biometryczne i umożliwiający jednoczesne wyszukiwanie za pomocą danych biometrycznych w różnych systemach informacyjnych UE ustanawia się, aby wspierać wspólne repozytorium tożsamości i moduł wykrywający multiplikację tożsamości oraz realizację celów systemów EES, VIS, Eurodac, SIS i [systemu ECRIS-TCN].

32. Wspólny serwis kojarzenia danych biometrycznych składa się z następujących elementów:

a) infrastruktury centralnej, w tym wyszukiwarki i pamięci danych, o których mowa w art. 13;

b) bezpiecznej infrastruktury komunikacyjnej między wspólnym serwisem kojarzenia danych biometrycznych, C.SIS i wspólnym repozytorium tożsamości.

33. Wspólny serwis kojarzenia danych biometrycznych opracowuje agencja eu-LISA, która zarządzani nim też od strony technicznej.

Artykuł 13

Dane przechowywane we wspólnym serwisie kojarzenia danych biometrycznych

34. Wspólny serwis kojarzenia danych biometrycznych przechowuje wzorce biometryczne, które uzyskuje na podstawie następujących danych biometrycznych:

a) dane, o których mowa w art. 16 ust. 1 lit. d) i w art. 17 ust. 1 lit. b) i c) rozporządzenia (UE) 2017/2226;

b) dane, o których mowa w art. 9 ust. 6 rozporządzenia (WE) nr 767/2008;

c) [dane, o których mowa w art. 20 ust. 2 lit. w) i x) rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych;

d) dane, o których mowa w art. 20 ust. 3 lit. w) i x) rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw;

e) dane, o których mowa w art. 4 ust. 3 lit. t) i u) rozporządzenia w sprawie SIS w odniesieniu do nielegalnego powrotu];

f) [dane, o których mowa w art. 13 lit. a) rozporządzenia w sprawie Eurodac];

g) [dane, o których mowa w art. 5 ust. 1 lit. b) i w art. 5 ust. 2 rozporządzenia w sprawie ECRIS-TCN].

35. Wspólny serwis kojarzenia danych biometrycznych zawiera w każdym wzorcu biometrycznym odniesienie do systemów informacyjnych, w których przechowywane są powiązane dane biometryczne.

36. Wzorce biometryczne są wprowadzane do serwisu dopiero po przeprowadzeniu automatycznej kontroli jakości danych biometrycznych dodanych do jednego z systemów informacyjnych, której dokonuje wspólny serwis kojarzenia danych biometrycznych, aby zapewnić spełnienie minimalnych norm jakości danych.

37. Przechowywanie danych, o których mowa w ust. 1, jest zgodne z normami jakości określonymi w art. 37 ust. 2.

Artykuł 14

Przeszukiwanie danych biometrycznych za pomocą wspólnego serwisu kojarzenia danych biometrycznych

Aby przeszukiwać dane biometryczne zgromadzone we wspólnym repozytorium tożsamości i w SIS, wspólne repozytorium tożsamości i SIS korzystają ze wzorców biometrycznych przechowywanych we wspólnym serwisie kojarzenia danych biometrycznych. Zapytań zawierających dane biometryczne dokonuje się zgodnie z celami określonymi w niniejszym rozporządzeniu i w rozporządzeniu w sprawie EES, rozporządzeniu w sprawie VIS, rozporządzeniu w sprawie Eurodac, [rozporządzeniach w sprawie SIS] i [rozporządzeniu w sprawie ECRIS-TCN].

Artykuł 15
Zatrzymywanie danych we wspólnym serwisie kojarzenia danych biometrycznych

Dane, o których mowa w art. 13, są przechowywane we wspólnym serwisie kojarzenia danych biometrycznych tak długo, jak długo odpowiadające im dane biometryczne są przechowywane we wspólnym repozytorium tożsamości lub w SIS.

Artykuł 16
Prowadzenie zapisów w rejestrze

38. Nie naruszając przepisów [art. 46 rozporządzenia w sprawie EES], art. 34 rozporządzenia (WE) nr 767/2008 oraz [art. 12 i 18 rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw], eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach wspólnego serwisu kojarzenia danych biometrycznych. Zawierają one w szczególności:

    a) historię związaną z tworzeniem i przechowywaniem wzorców biometrycznych;

    b) odniesienie do systemów informacyjnych UE przeszukiwanych za pomocą wzorców biometrycznych przechowywanych we wspólnym serwisie kojarzenia danych biometrycznych;

    c) datę i godzinę zapytania;

    d) rodzaj danych biometrycznych użytych przy dokonywaniu zapytania;

    e) długość zapytania;

    f) wyniki zapytania oraz datę i godzinę ich uzyskania;

    g) zgodnie z przepisami krajowymi lub, w stosownych przypadkach, rozporządzeniem (UE) nr 45/2001, identyfikator osoby, która dokonała zapytania.

39. Rejestry można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności wniosku i zgodności przetwarzania danych z prawem, oraz w celu zapewniania bezpieczeństwa danych zgodnie z art. 42. Rejestry są chronione za pomocą odpowiednich środków przed nieuprawnionym dostępem i usuwane jeden rok po utworzeniu, chyba że są konieczne do prowadzenia już rozpoczętych procedur monitorowania. Rejestry, o których mowa w ust. 1 lit. a), są usuwane po usunięciu odpowiadających im danych.

ROZDZIAŁ IV
Wspólne repozytorium tożsamości

Artykuł 17
Wspólne repozytorium tożsamości

40. Wspólne repozytorium tożsamości, tworzące indywidualne akta osobowe dla każdej osoby zarejestrowanej w systemach EES, VIS, [ETIAS], Eurodac lub [systemie ECRIS-TCN], zawierające dane, o których mowa w art. 18, ustanawia się po to, aby ułatwiać i wspomagać poprawną identyfikację osób zarejestrowanych w systemach EES, VIS, [ETIAS], Eurodac i [systemie ECRIS-TCN], wspierać funkcjonowanie modułu wykrywającego multiplikację tożsamości oraz, w stosownych przypadkach,

ułatwiać i usprawniać dostęp organów ścigania do systemów informacyjnych niezwiązanych ze ściganiem przestępstw na szczeblu UE w celu zapobiegania poważnym przestępstwom, prowadzenia w ich sprawie dochodzeń, ich wykrywania i ścigania.

41. Wspólne repozytorium tożsamości składa się z:

a) infrastruktury centralnej, która zastępuje systemy centralne, odpowiednio, systemów EES, VIS, [ETIAS], Eurodac i [systemu ECRIS-TCN] w zakresie przechowywania danych, o których mowa w art. 18;

b) bezpiecznego kanału komunikacji między wspólnym repozytorium tożsamości, państwami członkowskimi i organami UE uprawnionymi do korzystania z europejskiego portalu wyszukiwania zgodnie z przepisami prawa Unii;

c) bezpiecznej infrastruktury komunikacyjnej między wspólnym repozytorium tożsamości a systemami EES, VIS, [ETIAS], Eurodac i [systemem ECRIS-TCN] oraz wspólną infrastrukturą europejskiego portalu wyszukiwania, wspólnego serwisu kojarzenia danych biometrycznych i modułu wykrywającego multiplikację tożsamości.

42. Wspólne repozytorium tożsamości opracowuje eu-LISA, która zarządzani nim też od strony technicznej.

Artykuł 18
Dane wspólnego repozytorium tożsamości

43. Wspólne repozytorium tożsamości przechowuje następujące, oddzielone logicznie, dane, według systemu informacyjnego, z którego dane te pierwotnie pochodzą:

a) dane, o których mowa w [art. 16 ust. 1 lit. a)–d) oraz art. 17 ust. 1 lit. a)–c) rozporządzenia w sprawie EES];

b) dane, o których mowa w art. 9 ust. 4 lit. a)–c), ust. 5 i ust. 6 rozporządzenia (WE) nr 767/2008;

c) [dane, o których mowa w art. 15 ust. 2 lit. a)–e) rozporządzenia w sprawie ETIAS];

d) – (nie dotyczy)

e) – (nie dotyczy)

44. Dla każdego zestawu danych, o których mowa w ust. 1, wspólne repozytorium tożsamości zawiera odniesienie do systemów informacyjnych, z których dane te pochodzą.

45. Przechowywanie danych, o których mowa w ust. 1, jest zgodne z normami jakości określonymi w art. 37 ust. 2.

Artykuł 19
Dodawanie, zmiana i usuwanie danych we wspólnym repozytorium tożsamości

46. W przypadku dodawania, zmiany lub usuwania danych w systemach EES, VIS i [ETIAS] dane, o których mowa w art. 18, przechowywane w aktach osobowych wspólnego repozytorium tożsamości są odpowiednio dodawane, zmieniane lub usuwane w sposób automatyczny.

47. W wypadku stworzenia przez moduł wykrywający multiplikację tożsamości powiązania białego lub czerwonego zgodnie z art. 32 i 33 między danymi z dwóch lub większej liczby systemów informacyjnych UE składających się na wspólne repozytorium tożsamości, zamiast tworzyć nowe akta osobowe, repozytorium dodaje nowe dane do akt osobowych, z których pochodzą powiązane dane.

Artykuł 20

Dostęp do wspólnego repozytorium tożsamości w celu identyfikacji

48. W sytuacji, w której organ policyjny państwa członkowskiego został do tego upoważniony na mocy krajowych środków ustawodawczych, o których mowa w ust. 2, może on, wyłącznie w celu identyfikacji osoby fizycznej, dokonać zapytania we wspólnym repozytorium tożsamości, posługując się danymi biometrycznymi tej osoby pobranymi podczas kontroli tożsamości.

Jeśli wynik zapytania wskaże, że dane tej osoby są przechowywane we wspólnym repozytorium tożsamości, organ państwa członkowskiego powinien mieć możliwość przeglądania danych, o których mowa w art. 18 ust. 1.

Jeśli nie można użyć danych biometrycznych danej osoby lub jeśli zapytanie przy użyciu tych danych zakończy się niepowodzeniem, wyszukiwanie należy przeprowadzić za pomocą danych dotyczących tożsamości tej osoby w połączeniu z danymi dokumentu podróży lub danymi dotyczącymi tożsamości podanymi przez tę osobę.

49. Państwa członkowskie, które pragną skorzystać z możliwości przewidzianej w niniejszym artykule, przyjmują odpowiednie krajowe środki ustawodawcze. Takie środki ustawodawcze precyzują cele kontroli tożsamości na potrzeby określone w art. 2 ust. 1 lit. b) i c). Wyznaczają one właściwe organy policji i określają procedury, warunki i kryteria takich kontroli.

Artykuł 21

Dostęp do wspólnego repozytorium tożsamości w celu wykrywania multiplikacji tożsamości

50. Jeśli wynikiem zapytania we wspólnym repozytorium tożsamości jest powiązanie żółte określone w art. 28 ust. 4 organ odpowiedzialny za weryfikację różniących się tożsamości ustalonych zgodnie z art. 29 ma dostęp, wyłącznie w celu przeprowadzenia tej weryfikacji, do danych dotyczących tożsamości przechowywanych w repozytorium, należących do różnych systemów informacyjnych odnoszących się do powiązania żółtego.

51. Jeśli wynikiem zapytania we wspólnym repozytorium tożsamości jest powiązanie czerwone określone w art. 32 organy, o których mowa w art. 26 ust. 2, mają dostęp, wyłącznie w celu zwalczania oszustw dotyczących tożsamości, do danych dotyczących tożsamości przechowywanych w repozytorium, należących do różnych systemów informacyjnych odnoszących się do powiązania czerwonego.

Artykuł 22

Przeszukiwanie wspólnego repozytorium tożsamości w celu ścigania przestępstw

52. W celach zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie dochodzeń

w konkretnych sprawach oraz w celu uzyskania informacji o tym, czy dane określonej osoby znajdują się w systemach EES, VIS i [ETIAS], wyznaczone organy państw członkowskich i Europol mogą dokonać zapytania we wspólnym repozytorium tożsamości.

53. Wyznaczone organy państw członkowskich i Europol nie mają prawa do przeglądania danych należących do [ECRIS-TCN] podczas przeglądania wspólnego repozytorium tożsamości w celach wymienionych w ust. 1.

54. Jeśli odpowiedź na zapytanie we wspólnym repozytorium tożsamości wskaże, że dane przedmiotowej osoby są obecne w EES, VIS i [ETIAS], wspólne repozytorium tożsamości udziela odpowiedzi wyznaczonym organom państwa członkowskiego i Europolowi w postaci odniesienia wskazującego, który z systemów informacyjnych zawiera dane odpowiadające zapytaniu zgodnie z art. 18 ust. 2. Wspólne repozytorium tożsamości udziela odpowiedzi w sposób nienaruszający bezpieczeństwa danych.

55. Pełen dostęp do danych zawartych w systemach informacyjnych UE w celach zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie dochodzeń nadal podlega warunkom i procedurom określonym w odpowiednich instrumentach ustawodawczych regulujących taki dostęp.

Artykuł 23
Zatrzymywanie danych we wspólnym repozytorium tożsamości

56. Dane, o których mowa w art. 18 ust. 1 i 2, są usuwane ze wspólnego repozytorium tożsamości zgodnie z przepisami dotyczącymi zatrzymywania danych, odpowiednio, [rozporządzenia w sprawie EES], rozporządzenia w sprawie VIS i [rozporządzenia w sprawie ETIAS].

57. Akta osobowe są przechowywane we wspólnym repozytorium tożsamości tak długo, jak długo są one przechowywane w co najmniej jednym systemie informacyjnym, którego dane są zawarte w repozytorium. Stworzenie powiązania nie wpływa na okres zatrzymywania żadnej z pozycji wchodzącej w skład powiązanych danych.

Artykuł 24
Prowadzenie zapisów w rejestrze

58. Nie naruszając przepisów [art. 46 rozporządzenia w sprawie EES], art. 34 rozporządzenia (WE) nr 767/2008 oraz [art. 59 wniosku dotyczącego rozporządzenia w sprawie ETIAS], eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach wspólnego repozytorium tożsamości zgodnie z ust. 2, 3 i 4.

59. Jeśli chodzi o dostęp do wspólnego repozytorium tożsamości na mocy art. 20, eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach wspólnego repozytorium tożsamości. Rejestry te obejmują w szczególności:

a) cel dostępu użytkownika dokonującego zapytania za pośrednictwem wspólnego repozytorium tożsamości;

b) datę i godzinę zapytania;

c) rodzaj danych użytych przy dokonywaniu zapytania;

d) wyniki zapytania;

e) zgodnie z przepisami krajowymi lub rozporządzeniem (UE) 2016/794 lub, w stosownych przypadkach, rozporządzeniem (UE) nr 45/2001, identyfikator osoby, która dokonała zapytania.

60. Jeśli chodzi o dostęp do wspólnego repozytorium tożsamości na mocy art. 21, eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach wspólnego repozytorium tożsamości. Rejestry te obejmują w szczególności:

a) cel dostępu użytkownika dokonującego zapytania za pośrednictwem wspólnego repozytorium tożsamości;

b) datę i godzinę zapytania;

c) w stosownych przypadkach dane użyte w zapytaniu;

d) w stosownych przypadkach wyniki zapytania;

e) zgodnie z przepisami krajowymi lub rozporządzeniem (UE) 2016/794 lub, w stosownych przypadkach, rozporządzeniem (UE) nr 45/2001, identyfikator osoby, która dokonała zapytania.

61. Jeśli chodzi o dostęp do wspólnego repozytorium tożsamości na mocy art. 22, eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach wspólnego repozytorium tożsamości. Rejestry te obejmują w szczególności:

a) dane referencyjne rejestru krajowego;

b) datę i godzinę zapytania;

c) rodzaj danych użytych przy dokonywaniu zapytania;

d) wyniki zapytania;

e) nazwę organu przeglądającego wspólne repozytorium tożsamości;

f) zgodnie z przepisami krajowymi lub rozporządzeniem (UE) 2016/794 lub, w stosownych przypadkach, rozporządzeniem (UE) nr 45/2001, identyfikator urzędnika, który dokonał zapytania, i urzędnika, który je zlecił.

Rejestry dostępu podlegają regularnej weryfikacji przez właściwy organ nadzorczy ustanowiony zgodnie z art. 51 rozporządzenia (UE) 2016/679 lub zgodnie z art. 41 dyrektywy 2016/680, w odstępach czasowych nieprzekraczających sześć miesięcy, w celu sprawdzenia, czy procedury i warunki określone w art. 22 ust. 1–3 zostały spełnione.

62. Każde państwo członkowskie prowadzi rejestry zapytań dokonanych przez pracowników uprawnionych do korzystania ze wspólnego repozytorium tożsamości na mocy art. 20, 21 i 22.

63. Rejestry, o których mowa w ust. 1 i 5, można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności wniosku i zgodności z prawem przetwarzania danych, oraz w celu zapewniania bezpieczeństwa danych zgodnie z art. 42. Zapisy w rejestrze są chronione za pomocą odpowiednich środków przed nieuprawnionym dostępem i usuwane jeden rok po utworzeniu, chyba że są konieczne do prowadzenia już rozpoczętych procedur monitorowania.

64. Agencja eu-LISA prowadzi rejestry dotyczące historii danych przechowywanych w aktach osobowych w celach określonych w ust. 6. Rejestry dotyczące historii przechowywanych danych są usuwane po usunięciu tych danych.

ROZDZIAŁ V
Moduł wykrywający multiplikację tożsamości

Artykuł 25
Moduł wykrywający multiplikację tożsamości

65. Moduł wykrywający multiplikację tożsamości, tworzący i przechowujący powiązania między danymi zgromadzonymi w systemach informacyjnych UE objętych wspólnym repozytorium tożsamości i SIS oraz wykrywający w ten sposób multiplikację tożsamości tej samej osoby, co służy podwójnemu celowi ułatwienia kontroli tożsamości i zwalczania oszustw dotyczących tożsamości, ustanawia się po to, aby wspierać funkcjonowanie wspólnego repozytorium tożsamości i realizację celów systemów EES, VIS, [ETIAS], Eurodac, SIS i [systemu ECRIS-TCN].

66. Moduł wykrywający multiplikację tożsamości składa się z:

a) infrastruktury centralnej, przechowującej powiązania i odniesienia do systemów informacyjnych;

b) bezpiecznej infrastruktury komunikacyjnej łączącej moduł wykrywający multiplikację tożsamości z SIS i infrastrukturą centralną europejskiego portalu wyszukiwania i wspólnego repozytorium tożsamości.

67. Moduł wykrywający multiplikację tożsamości opracowuje agencja eu-LISA, która zarządza nim też od strony technicznej.

Artykuł 26
Dostęp do modułu wykrywającego multiplikację tożsamości

68. W celu ręcznej weryfikacji tożsamości, o której mowa w art. 29, dostęp do danych określonych w art. 34 przechowywanych w module wykrywającym multiplikację tożsamości mają:

a) organy graniczne, podczas tworzenia lub aktualizacji akt osobowych, o których mowa w art. 14 [rozporządzenia w sprawie EES];

b) właściwe organy, o których mowa w art. 6 ust. 1 i 2 rozporządzenia 767/2008, podczas tworzenia lub aktualizacji pliku danych dotyczących wniosku w systemie VIS zgodnie z art. 8 rozporządzenia (WE) nr 767/2008;

c) [jednostka centralna ETIAS i jednostki krajowe ETIAS, podczas dokonywania oceny, o której mowa w art. 20 i 22 rozporządzenia w sprawie ETIAS];

d) – (nie dotyczy);

e) biuro Sirene państwa członkowskiego, które utworzyło [wpis w SIS zgodnie z rozporządzeniem w sprawie SIS w odniesieniu do odpraw granicznych];

f) – (nie dotyczy).

69. Organy państw członkowskich i UE mające dostęp do co najmniej jednego systemu informacyjnego UE objętego *wspólnym repozytorium tożsamości lub SIS* mają dostęp do danych, o których mowa w art. 34 lit. a) i b), w odniesieniu do wszelkich powiązań czerwonych określonych w art. 32.

Artykuł 27
Wykrywanie multiplikacji tożsamości

70. Proces wykrywania multiplikacji tożsamości we wspólnym repozytorium tożsamości i SIS należy uruchomić w następujących sytuacjach:

a) tworzenie lub aktualizacja akt osobowych w [EES zgodnie z art. 14 rozporządzenia w sprawie EES];

b) tworzenie lub aktualizacja pliku danych dotyczących wniosku w systemie VIS zgodnie z art. 8 rozporządzenia (WE) nr 767/2008;

c) [tworzenie lub aktualizacja pliku danych dotyczących wniosku w systemie ETIAS zgodnie z art. 17 rozporządzenia w sprawie ETIAS];

d) – (nie dotyczy);

e) [tworzenie lub aktualizacja wpisu dotyczącego danej osoby w SIS zgodnie z rozdziałem V rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych];

f) – (nie dotyczy).

71. Jeśli dane zawarte w systemie informacyjnym, o którym mowa w ust. 1, zawierają dane biometryczne, wspólne repozytorium tożsamości i C.SIS korzystają ze wspólnego serwisu kojarzenia danych biometrycznych w celu wykrycia multiplikacji tożsamości. Wspólny serwis kojarzenia danych biometrycznych porównuje wzorce biometryczne pochodzące z wszelkich nowych danych biometrycznych ze wzorcami biometrycznymi już znajdującymi się we wspólnym serwisie kojarzenia danych biometrycznych, aby sprawdzić, czy dane należące do tego samego obywatela państwa trzeciego już znajdują się we wspólnym repozytorium tożsamości i w C.SIS.

72. Obok procesu, o którym mowa w ust. 2, wspólne repozytorium tożsamości i C.SIS korzystają z europejskiego portalu wyszukiwania, aby przeszukiwać dane przechowywane we wspólnym repozytorium tożsamości i w C.SIS, posługując się następującymi danymi:

a) nazwisko; imię (imiona); data urodzenia, płeć i obywatelstwo (obywatelstwa), zgodnie z art. 16 ust. 1 lit. a) [rozporządzenia w sprawie EES];

b) nazwisko; imię (imiona); data urodzenia, płeć i obywatelstwo (obywatelstwa), zgodnie z art. 9 ust. 4 lit. a) rozporządzenia (WE) nr 767/2008;

c) [nazwisko; imię (imiona); nazwisko rodowe; data urodzenia, miejsce urodzenia, płeć i obywatelstwo (obywatelstwa), zgodnie z art. 15 ust. 2 rozporządzenia w sprawie ETIAS];

d) – (nie dotyczy);

e) [nazwisko (nazwiska); imię (imiona); nazwisko (nazwiska) rodowe, wcześniej używane nazwiska i pseudonimy; data urodzenia, miejsce urodzenia, obywatelstwo (obywatelstwa) i płeć zgodnie z art. 20 ust. 2 rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych;]

f) – (nie dotyczy);

g) – (nie dotyczy);

h) – (nie dotyczy).

73. Wykrywanie multiplikacji tożsamości należy przeprowadzić wyłącznie w celu porównania danych dostępnych w jednym systemie informacyjnym z danymi dostępnymi w pozostałych systemach.

Artykuł 28
Wyniki wykrywania multiplikacji tożsamości

74. Jeśli zapytania, o których mowa w art. 27 ust. 2 i 3, nie wykażą żadnego trafienia, procedury określone w art. 27 ust. 1 są prowadzone dalej zgodnie z odpowiednimi rozporządzeniami, którym podlegają.

75. Jeśli zapytanie, o którym mowa w art. 27 ust. 2 i 3, wykaże jedno lub kilka trafień, we wspólnym repozytorium tożsamości oraz, w stosownych przypadkach, w SIS tworzone jest powiązanie między danymi użytymi w zapytaniu a danymi, które doprowadziły do wystąpienia trafienia.

W wypadku wystąpienia kilku trafień tworzone jest powiązanie między wszystkimi danymi, które doprowadziły do trafienia. Jeśli dane te już uprzednio były powiązane, istniejące powiązanie należy rozszerzyć o dane użyte w zapytaniu.

76. Jeśli zapytanie, o którym mowa w art. 27 ust. 2 lub 3, wykaże jedno lub kilka trafień, a dane dotyczące tożsamości zawarte w powiązanych ze sobą aktach indywidualnych są identyczne lub podobne, tworzone jest powiązanie białe zgodnie z art. 33.

77. Jeśli zapytanie, o którym mowa w art. 27 ust. 2 lub 3, wykaże jedno lub kilka trafień, a danych dotyczących tożsamości zawartych w powiązanych ze sobą aktach indywidualnych nie można uznać za podobne, ustanawiane jest powiązanie żółte zgodnie z art. 30; obowiązuje wówczas procedura, o której mowa w art. 29.

78. Komisja określa za pomocą aktów wykonawczych procedury ustalania, w jakich przypadkach dane dotyczące tożsamości można uznać za identyczne lub podobne. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 64 ust. 2.

79. Powiązania te są zapisywane w plikach potwierdzających tożsamość, o których mowa w art. 34.

Komisja określa za pomocą aktów wykonawczych zasady techniczne łączenia ze sobą danych z różnych systemów informacyjnych. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 64 ust. 2.

Artykuł 29
Ręczna weryfikacja różnych tożsamości

80. Nie naruszając przepisów ust. 2, organem odpowiedzialnym za weryfikację różniących się tożsamości jest:

a) służba graniczna — w przypadku trafień, które wystąpiły przy tworzeniu lub aktualizacji danych dotyczących osoby fizycznej w [systemie EES zgodnie z art. 14 rozporządzenia w sprawie EES];

b) właściwe organy, o których mowa w art. 6 ust. 1 i 2 rozporządzenia 767/2008, w przypadku trafień, które wystąpiły podczas tworzenia lub aktualizacji pliku

danych dotyczących wniosku w systemie VIS zgodnie z art. 8 rozporządzenia (WE) nr 767/2008;

c) [jednostka centralna ETIAS i jednostki krajowe ETIAS, w przypadku trafień, o których mowa w art. 18, 20 i 22 rozporządzenia w sprawie ETIAS];

d) – (nie dotyczy);

e) biuro Sirene państwa członkowskiego, w przypadku trafień, które wystąpiły podczas tworzenia [wpisu w SIS zgodnie z rozporządzeniem w sprawie SIS w odniesieniu do odpraw granicznych];

f) – (nie dotyczy).

Moduł wykrywający multiplikację tożsamości wskazuje organ odpowiedzialny za weryfikację różniących się tożsamości w pliku potwierdzającym tożsamość.

81. Organem odpowiedzialnym za weryfikację różniących się tożsamości w pliku potwierdzającym tożsamość jest biuro Sirene państwa członkowskiego, które stworzyło wpis, jeśli utworzono powiązanie do danych zawartych we:

a) wpisie dotyczącym osób poszukiwanych w celu aresztowania i wydania lub ekstradycji, zgodnie z art. 26 [rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw];

b) wpisie dotyczącym osób zaginionych lub narażonych na zagrożenia zgodnie z art. 32 [rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw];

c) wpisie dotyczącym osób, których obecność jest wymagana do celów postępowania sądowego zgodnie z art. 34 [rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw];

d) [wpisie dotyczącym powrotu zgodnie z rozporządzeniem w sprawie SIS w odniesieniu do nielegalnych powrotów];

e) wpisie dotyczącym osób, wobec których prowadzone są kontrole niejawne, rozpytania kontrolne lub kontrole szczegółowe zgodnie z art. 36 [rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw];

f) wpisie dotyczącym nieznanych osób poszukiwanych, których identyfikacja jest wymagana na mocy prawa krajowego i w związku z poszukiwaniami opartymi na danych biometrycznych, zgodnie z art. 40 [rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw].

82. Nie naruszając przepisów ust. 4, organ odpowiedzialny za weryfikację różniących się tożsamości ma dostęp do powiązanych danych zawartych w odpowiednich plikach potwierdzających tożsamość i w danych dotyczących tożsamości powiązanych we wspólnym repozytorium tożsamości oraz, w stosownych przypadkach, w SIS, oraz ocenia różne tożsamości i aktualizuje powiązanie zgodnie z art. 31, 32 i 33, a także niezwłocznie dodaje je do pliku potwierdzającego tożsamość.

83. Jeśli organem odpowiedzialnym za weryfikację różnych tożsamości w pliku potwierdzającym tożsamość jest służba graniczna, która tworzy lub aktualizuje akta osobowe w EES zgodnie z art. 14 rozporządzenia w sprawie EES, a także w razie uzyskania powiązania żółtego, ta służba graniczna przeprowadza dodatkowe weryfikacje w ramach kontroli drugiej linii. W czasie tej kontroli drugiej linii służby graniczne mają dostęp do powiązanych danych zawartych w odpowiednim pliku

potwierdzającym tożsamość i analizują różne tożsamości oraz aktualizują powiązanie zgodnie z art. 31–33 i niezwłocznie dodają je do pliku potwierdzającego tożsamość.

84. W razie uzyskania więcej niż jednego powiązania organ odpowiedzialny za weryfikację różnych tożsamości ocenia każde powiązanie oddzielnie.

85. Jeśli dane prowadzące do wystąpienia trafienia już uprzednio były ze sobą powiązane, organ odpowiedzialny za weryfikację różniących się tożsamości uwzględnia istniejące powiązania podczas oceny, czy należy utworzyć nowe powiązania.

Artykuł 30
Powiązanie żółte

86. Powiązanie między danymi z dwóch lub większej liczby systemów informacyjnych klasyfikuje się jako powiązanie żółte w każdym z poniższych przypadków:

a) powiązane ze sobą dane zawierają takie same dane biometryczne, lecz różne dane dotyczące tożsamości i nie przeprowadzono ręcznej weryfikacji różniących się tożsamości;

b) powiązane ze sobą dane zawierają różne dane dotyczące tożsamości i nie przeprowadzono ręcznej weryfikacji różniących się tożsamości.

87. W razie sklasyfikowania powiązania jako żółtego zgodnie z ust. 1 obowiązuje procedura opisana w art. 29.

Artykuł 31
Powiązanie zielone

88. Powiązanie między danymi zawartymi w dwóch lub większej liczbie systemów informacyjnych klasyfikuje się jako zielone, jeśli powiązane ze sobą dane nie zawierają takich samych danych biometrycznych, lecz podobne dane dotyczące tożsamości, a organ odpowiedzialny za weryfikację różniących się tożsamości stwierdzi, że odnoszą się one do dwóch różnych osób.

89. Jeśli po przeszukaniu wspólnego repozytorium tożsamości lub SIS stwierdzone zostanie istnienie powiązania zielonego między dwoma systemami informacyjnymi składającymi się na wspólne repozytorium tożsamości lub z SIS, moduł wykrywający multiplikację tożsamości wskazuje, że dane dotyczące tożsamości stanowiące część powiązanych danych nie należą do tej samej osoby. Przeszukiwany system informacyjny udziela odpowiedzi, podając jedynie dane osoby, której danych użyto w zapytaniu, nie prowadząc jednak do trafienia w stosunku do danych powiązanych powiązaniem zielonym.

Artykuł 32
Powiązanie czerwone

90. Powiązanie między danymi z dwóch lub większej liczby systemów informacyjnych klasyfikuje się jako powiązanie czerwone w każdym z poniższych przypadków:

a) powiązane dane zawierają takie same dane biometryczne, lecz różne dane dotyczące tożsamości, a organ odpowiedzialny za weryfikację różniących się tożsamości stwierdził, że bezprawnie odnoszą się one do tej samej osoby;

b) powiązane dane zawierają podobne dane dotyczące tożsamości, a organ odpowiedzialny za weryfikację poszczególnych tożsamości stwierdził, że bezprawnie odnoszą się one do tej samej osoby.

91. Jeśli w wyniku przeszukania wspólnego repozytorium tożsamości stwierdzona zostanie obecność powiązania czerwonego między dwoma lub większą liczbą systemów informacyjnych składających się na wspólne repozytorium tożsamości lub z SIS, moduł wykrywający multiplikację tożsamości udziela odpowiedzi, wskazując dane, o których mowa w art. 34. Działania następcze w związku z wystąpieniem powiązania czerwonego są prowadzone zgodnie z przepisami prawa Unii i prawa krajowego.

92. W razie utworzenia powiązania czerwonego między danymi z systemów EES, VIS, [ETIAS], Eurodac lub [ECRIS-TCN], akta osobowe przechowywane we wspólnym repozytorium tożsamości są aktualizowane zgodnie z art. 19 ust. 1.

93. Bez uszczerbku dla przepisów związanych z rozpatrywaniem wpisów w SIS, o których mowa w [rozporządzeniach w sprawie SIS w odniesieniu do odpraw granicznych, SIS w odniesieniu do ścigania przestępstw i SIS w odniesieniu do nielegalnych powrotów], oraz bez uszczerbku dla ograniczeń koniecznych do ochrony bezpieczeństwa i porządku publicznego, zapobiegania przestępstwom i zagwarantowania, aby prowadzone śledztwa krajowe nie były zagrożone, w razie utworzenia powiązania czerwonego organ odpowiedzialny za weryfikację różniących się tożsamości powiadamia osobę, której to dotyczy, o stwierdzeniu obecności niezgodnych z prawem różnych tożsamości.

94. W razie utworzenia powiązania czerwonego organ odpowiedzialny za weryfikację różniących się tożsamości przesyła odpowiednie odniesienie organom odpowiedzialnym za powiązane dane.

Artykuł 33
Powiązanie białe

95. Powiązanie między danymi z dwóch lub większej liczby systemów informacyjnych klasyfikuje się jako powiązanie białe w każdym z poniższych przypadków:

a) powiązane ze sobą dane zawierają takie same dane biometryczne i takie same lub podobne dane dotyczące tożsamości;

b) powiązane ze sobą dane zawierają takie same lub podobne dane dotyczące tożsamości, a co najmniej jeden z systemów informacyjnych nie zawiera danych biometrycznych osoby, której to dotyczy;

c) powiązane dane zawierają takie same dane biometryczne, lecz różne dane dotyczące tożsamości, a organ odpowiedzialny za weryfikację różniących się tożsamości stwierdził, że odnoszą się one do tej samej osoby, która w sposób zgodny z prawem posiada różne dane dotyczące tożsamości.

96. Jeśli po przeszukaniu wspólnego repozytorium tożsamości lub SIS stwierdzone zostanie istnienie powiązania białego między dwoma systemami informacyjnymi składającymi się na wspólne repozytorium tożsamości lub z SIS, moduł wykrywający multiplikację tożsamości wskazuje, że powiązane dane dotyczące tożsamości należą do tej samej osoby. Wynikiem przeszukiwania systemów

informacyjnych jest odpowiedź, która w stosownych przypadkach wskazuje wszystkie powiązane ze sobą dane dotyczące danej osoby, co powoduje powstanie trafienia w stosunku do danych objętych powiązaniem białym, jeśli organ, który dokonał zapytania, ma dostęp do tych powiązanych danych na mocy prawa Unii lub prawa krajowego.

97. W razie utworzenia powiązanie białego między danymi z systemów EES, VIS, [ETIAS], Eurodac lub [ECRIS-TCN] akta osobowe przechowywane we wspólnym repozytorium tożsamości są aktualizowane zgodnie z art. 19 ust. 1.

98. Bez uszczerbku dla przepisów związanych z rozpatrywaniem wpisów w SIS, o których mowa w [rozporządzeniach w sprawie SIS w odniesieniu do odpraw granicznych, SIS w odniesieniu do ścigania przestępstw i SIS w odniesieniu do nielegalnych powrotów], w razie utworzenia powiązania białego w wyniku ręcznej weryfikacji multiplikacji tożsamości, organ odpowiedzialny za weryfikację różniących się tożsamości powiadamia zainteresowaną osobę o rozbieżnościach między jej danymi osobowymi w różnych systemach oraz przekazuje odpowiednie odniesienie organom odpowiedzialnym za te powiązane dane.

Artykuł 34
Plik potwierdzający tożsamość

Plik potwierdzający tożsamość zawiera następujące dane:

a) powiązania, w tym ich opis w formie kolorów, zgodnie z art. 30–33;

b) odniesienie do systemów informacyjnych zawierających powiązane ze sobą dane;

c) pojedynczy numer identyfikacyjny umożliwiający pobranie danych z systemów informacyjnych zawierających odpowiednie powiązane ze sobą pliki;

d) w razie potrzeby organ odpowiedzialny za weryfikację różniących się tożsamości.

Artykuł 35
Zatrzymywanie danych w module wykrywającym multiplikację tożsamości

Pliki potwierdzające tożsamość i zawarte w nich dane, w tym powiązania, są przechowywane w module wykrywającym multiplikację tożsamości tylko tak długo, jak długo powiązane ze sobą dane są przechowywane w dwóch lub większej liczbie systemów informacyjnych UE.

Artykuł 36
Prowadzenie rejestrów

99. Agencja eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w module wykrywającym multiplikację tożsamości. Zawierają one w szczególności:

a) cel dostępu użytkownika i przysługujące mu prawa dostępu;

b) datę i godzinę zapytania;

c) rodzaj danych użytych w zapytaniu lub zapytaniach;

d) odniesienie do powiązanych ze sobą danych;

e) historię pliku potwierdzającego tożsamość;

f) identyfikator osoby, która dokonała zapytania.

100. Każde państwo członkowskie prowadzi rejestry pracowników uprawnionych do korzystania z modułu wykrywającego multiplikację tożsamości.

101. Rejestry można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności wniosku i zgodności przetwarzania danych z prawem, oraz w celu zapewniania bezpieczeństwa danych zgodnie z art. 42. Rejestry są chronione za pomocą odpowiednich środków przed nieuprawnionym dostępem i usuwane jeden rok po utworzeniu, chyba że są konieczne do prowadzenia już rozpoczętych procedur monitorowania. Rejestry związane z historią pliku potwierdzającego tożsamość są usuwane niezwłocznie po usunięciu tego pliku.

ROZDZIAŁ VI
Środki wspierające interoperacyjność

Artykuł 37
Jakość danych

102. Agencja eu-LISA ustanawia automatyczne mechanizmy i procedury kontroli jakości danych przechowywanych w systemach EES, [ETIAS], VIS, SIS, wspólnym serwisie kojarzenia danych biometrycznych, wspólnym repozytorium tożsamości i module wykrywającym multiplikację tożsamości.

103. Agencja eu-LISA ustanawia wspólne wskaźniki jakości danych i minimalne normy jakości przechowywania danych w systemach EES, [ETIAS], VIS, SIS, wspólnym serwisie kojarzenia danych biometrycznych, wspólnym repozytorium tożsamości i w module wykrywającym multiplikację tożsamości.

104. Agencja eu-LISA regularnie przedstawia państwom członkowskim sprawozdania z mechanizmów i procedur automatycznej kontroli jakości danych oraz wspólnych wskaźników jakości danych. Agencja eu-LISA regularnie przedstawia też Komisji sprawozdania ze zidentyfikowanych problemów i tego, których państw członkowskich dotyczą.

105. Szczegóły tych mechanizmów i procedur automatycznej kontroli jakości danych, wspólnych wskaźników jakości danych oraz minimalnych norm jakości przechowywania danych w systemach EES, [ETIAS], VIS, SIS, wspólnym serwisie kojarzenia danych biometrycznych i module wykrywającym multiplikację tożsamości, zwłaszcza w odniesieniu do danych biometrycznych, określają akty wykonawcze. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 64 ust. 2.

106. Jeden rok po ustanowieniu mechanizmów i procedur automatycznej kontroli jakości danych i wspólnych wskaźników jakości danych oraz co roku od tej daty Komisja ocenia wdrożenie jakości danych w państwach członkowskich i sporządza odpowiednie zalecenia. Państwa członkowskie przedstawiają Komisji plan działania mający na celu rozwiązanie wszelkich problemów zidentyfikowanych w sprawozdaniu oceniającym oraz zdają sprawę z postępów w realizacji tego planu działania do czasu jego pełnego wdrożenia. Komisja przekazuje powyższe

sprawozdanie oceniające Parlamentowi Europejskiemu, Radzie, Europejskiemu Inspektorowi Danych Osobowych i Agencji Praw Podstawowych Unii Europejskiej ustanowionej na mocy rozporządzenia Rady (WE) nr 168/2007[75].

Artykuł 38
Uniwersalny format wiadomości

107. Niniejszym ustanawia się uniwersalny format wiadomości (UMF). Uniwersalny format wiadomości określa standardy dla niektórych elementów treści transgranicznej wymiany informacji między systemami informacyjnymi, organami lub organizacjami działającymi w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych.

108. Standard UMF jest stosowany przy opracowywaniu systemów EES, [ETIAS], europejskiego portalu wyszukiwania, wspólnego repozytorium tożsamości, modułu wykrywającego multiplikację tożsamości oraz, w stosownych przypadkach, przy opracowywaniu przez eu-LISA lub inny organ UE nowych modeli wymiany informacji i systemów informacyjnych w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych.

109. Wdrożenie standardu UMF można rozważyć w przypadku systemów VIS, SIS oraz wszelkich istniejących lub nowych modeli transgranicznej wymiany informacji i systemów informacyjnych w dziedzinie wymiaru sprawiedliwości i bezpieczeństwa opracowywanych przez państwa członkowskie lub państwa stowarzyszone.

110. Komisja przyjmuje akt wykonawczy, aby określić i rozwijać standard UMF, o którym mowa w ust. 1. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 64 ust. 2.

Artykuł 39
Centralne repozytorium sprawozdawczo-statystyczne

111. Centralne repozytorium sprawozdawczo-statystyczne ustanawia się po to, aby wspierać realizację celów systemów EES, VIS, [ETIAS] i SIS oraz generować międzysystemowe dane statystyczne i sprawozdania analityczne służące strategiom politycznym, celom operacyjnym i związanym z jakością danych.

112. Agencja eu-LISA ustanawia, wdraża i obsługuje to repozytorium w swoich witrynach technicznych zawierających dane, o których mowa w [art. 63 rozporządzenia w sprawie EES], art. 17 rozporządzenia (WE) nr 767/2008, [art. 73 rozporządzenia w sprawie ETIAS] i [art. 54 rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych], logicznie oddzielone. Dane zawarte w centralnym repozytorium sprawozdawczo-statystycznym nie umożliwiają identyfikacji osób fizycznych. Dostęp do repozytorium w postaci bezpiecznego dostępu za pośrednictwem zabezpieczonej transeuropejskiej telematycznej sieci komunikacyjnej między administracjami (TESTA) i przy zastosowaniu kontroli dostępu i określonych profili użytkowników przyznaje się – wyłącznie w celach sprawozdawczo-statystycznych – organom, o których mowa w [art. 63 rozporządzenia w sprawie EES], art. 17 rozporządzenia (WE) nr 767/2008, [art. 73

[75] Rozporządzenie Rady (WE) nr 168/2007 z dnia 15 lutego 2007 r. ustanawiające Agencję Praw Podstawowych Unii Europejskiej (Dz.U. L 53 z 22.2.2007, s. 1).

rozporządzenia w sprawie ETIAS] i [art. 54 rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych].

113. Agencja eu-LISA poddaje dane anonimizacji i rejestruje takie anonimowe dane w repozytorium. Proces anonimizacji danych odbywa się automatycznie.

114. Centralne repozytorium sprawozdawczo-statystyczne składa się z:

a) infrastruktury centralnej, obejmującej repozytorium danych umożliwiające udostępnianie anonimowych danych;

b) bezpiecznej infrastruktury komunikacyjnej łączącej repozytorium z systemami EES, [ETIAS], VIS i SIS oraz z infrastrukturą centralną wspólnego serwisu kojarzenia danych biometrycznych, wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości.

115. Komisja określa za pomocą aktów wykonawczych szczegółowe zasady działania centralnego repozytorium sprawozdawczo-statystycznego, w tym szczegółowe zabezpieczenia dotyczące przetwarzania danych osobowych, o których mowa w ust. 2 i 3, oraz zasady bezpieczeństwa obowiązujące w stosunku do repozytorium. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 64 ust. 2.

ROZDZIAŁ VII
Ochrona danych

Artykuł 40
Administrator danych

116. W stosunku do przetwarzania danych za pośrednictwem wspólnego serwisu kojarzenia danych biometrycznych organy państw członkowskich będące administratorami danych w odniesieniu do, odpowiednio, systemów VIS, EES i SIS są także uznawane za administratorów zgodnie z art. 4 ust. 7 rozporządzenia (UE) 2016/679 w stosunku do wzorców biometrycznych uzyskanych na podstawie danych, o których mowa w art. 13, które wprowadzają do odpowiednich systemów, oraz odpowiadają za przetwarzanie wzorców biometrycznych we wspólnym serwisie kojarzenia danych biometrycznych.

117. W stosunku do przetwarzania danych za pośrednictwem wspólnego repozytorium tożsamości organy państw członkowskich będące administratorami danych w odniesieniu do, odpowiednio, systemów VIS, EES i [ETIAS] są także uznawane za administratorów zgodnie z art. 4 ust. 7 rozporządzenia (UE) 2016/679 w stosunku do danych, o których mowa w art. 18, które wprowadzają do odpowiednich systemów, oraz odpowiadają za przetwarzanie danych osobowych we wspólnym repozytorium tożsamości.

118. W stosunku do przetwarzania danych za pośrednictwem modułu wykrywającego multiplikację tożsamości:

a) Europejska Agencja Straży Granicznej i Przybrzeżnej jest uznawana za administratora danych zgodnie z art. 2 lit. b) rozporządzenia nr 45/2001 w związku z przetwarzaniem danych osobowych przez jednostkę centralną ETIAS;

b) organy państw członkowskich, które dodają lub modyfikują dane w pliku potwierdzającym tożsamość, także są uznawane za administratorów danych zgodnie z art. 4 ust. 7 rozporządzenia (UE) 2016/679 i odpowiadają za przetwarzanie danych osobowych w module wykrywającym multiplikację tożsamości.

Artykuł 41
Przetwarzający dane

Za przetwarzającego dane w stosunku do przetwarzania danych osobowych we wspólnym repozytorium tożsamości należy uznać agencję eu-LISA zgodnie z art. 2 lit. e) rozporządzenia (WE) nr 45/2001.

Artykuł 42
Bezpieczeństwo przetwarzania danych

119. Zarówno eu-LISA, jak i organy państw członkowskich zapewniają bezpieczeństwo przetwarzania danych osobowych odbywającego się w ramach stosowania niniejszego rozporządzenia. Agencja eu-LISA, [jednostka centralna ETIAS] i organy państw członkowskich współpracują w zakresie realizacji zadań związanych z bezpieczeństwem.

120. Nie naruszając przepisów art. 22 rozporządzenia (WE) nr 45/2001 eu-LISA podejmuje konieczne środki, aby zapewnić bezpieczeństwo elementów interoperacyjności i związanej z nimi infrastruktury komunikacyjnej.

121. W szczególności eu-LISA przyjmuje konieczne środki, w tym plan bezpieczeństwa, plan ciągłości działania i plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, w celach:

a) fizycznej ochrony danych, w tym poprzez opracowywanie planów awaryjnych służących ochronie infrastruktury krytycznej;

b) uniemożliwienia nieuprawnionego odczytywania, kopiowania, zmieniania lub usuwania nośników danych;

c) zapobiegania nieuprawnionemu wprowadzaniu danych i nieuprawnionej inspekcji, zmianie i nieuprawnionemu usuwaniu przechowywanych danych osobowych;

d) zapobiegania nieuprawnionemu przetwarzaniu danych i nieuprawnionemu kopiowaniu, modyfikacji lub usuwaniu danych;

e) dopilnowania, aby osoby upoważnione do dostępu do elementów interoperacyjności miały dostęp jedynie do danych objętych ich upoważnieniem dostępu, wyłącznie za pomocą niepowtarzalnych identyfikatorów użytkownika oraz poufnych haseł;

f) zapewnienia możliwości sprawdzenia i ustalenia, którym organom można przesyłać dane osobowe przy użyciu sprzętu do przekazywania danych;

g) zapewnienia możliwości sprawdzenia i ustalenia, które dane zostały przetworzone w elementach interoperacyjności, kiedy, przez kogo i w jakim celu;

h) uniemożliwienia nieuprawnionego odczytu, kopiowania, modyfikowania lub usuwania danych osobowych w trakcie przekazywania danych osobowych do

lub z elementów interoperacyjności lub podczas transportu nośników danych, w szczególności za pomocą odpowiednich technik szyfrowania;

i) monitorowania skuteczności środków bezpieczeństwa, o których mowa w niniejszym ustępie, oraz podejmowania niezbędnych środków organizacyjnych w obszarze kontroli wewnętrznej, aby zapewnić zgodność z przepisami niniejszego rozporządzenia.

122. Państwa członkowskie podejmują środki równoważne tym, o których mowa w ust. 3, w zakresie bezpieczeństwa w odniesieniu do przetwarzania danych osobowych przez organy mające prawo dostępu do któregoś z elementów interoperacyjności.

Artykuł 43
Poufność danych przechowywanych w SIS

123. Każde państwo członkowskie stosuje własne przepisy dotyczące tajemnicy zawodowej lub inne równoważne wymogi poufności wobec wszystkich osób i podmiotów, które muszą operować danymi SIS, do których dostęp jest uzyskiwany za pośrednictwem któregoś z elementów interoperacyjności, zgodnie z prawem krajowym. Zobowiązanie to obowiązuje także po zakończeniu pełnienia urzędu lub ustaniu zatrudnienia oraz po zakończeniu działalności przez dane podmioty.

124. Nie naruszając przepisów art. 17 Regulaminu pracowniczego urzędników Unii Europejskiej i warunków zatrudnienia innych pracowników Unii Europejskiej eu-LISA stosuje odpowiednie zasady tajemnicy zawodowej lub inne równoważne wymogi poufności wobec wszystkich swoich pracowników, którzy muszą operować danymi SIS, na zasadach porównywalnych z zasadami, o których mowa w ust. 1. Zobowiązanie to obowiązuje również po zakończeniu pełnienia urzędu lub ustaniu zatrudnienia lub po zakończeniu ich działalności.

Art. 44
Incydenty bezpieczeństwa

125. Wszelkie zdarzenie, które ma lub może mieć wpływ na bezpieczeństwo elementów interoperacyjności oraz może spowodować uszkodzenie lub utratę przechowywanych w nich danych, uznaje się za incydent bezpieczeństwa, w szczególności gdy mogło dojść do nieuprawnionego dostępu do danych lub gdy zostały lub mogły zostać naruszone dostępność, integralność i poufność danych.

126. Incydentami bezpieczeństwa zarządza się w sposób zapewniający szybkie, skuteczne i właściwe reagowanie.

127. Bez uszczerbku dla zgłaszania i zawiadamiania w odniesieniu do naruszenia ochrony danych osobowych zgodnie z art. 33 rozporządzenia (UE) 2016/679 lub art. 30 dyrektywy (UE) 2016/680 lub obu z nich państwa członkowskie powiadamiają o incydentach bezpieczeństwa Komisję, eu-LISA i Europejskiego Inspektora Ochrony Danych. W przypadku incydentu bezpieczeństwa związanego z infrastrukturą elementów interoperacyjności eu-LISA powiadamia Komisję i Europejskiego Inspektora Ochrony Danych.

128. Informacja o incydencie bezpieczeństwa, który ma lub może mieć wpływ na funkcjonowanie elementów interoperacyjności lub na dostępność, integralność i poufność danych, zostaje przekazana państwom członkowskim i zgłoszona zgodnie

z zapewnionym przez eu-LISA planem zarządzania na wypadek incydentów bezpieczeństwa.

129. W wypadku incydentu bezpieczeństwa zainteresowane państwa członkowskie i eu-LISA współpracują ze sobą. Komisja określa specyfikację tej procedury współpracy za pomocą aktów wykonawczych. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 64 ust. 2.

Artykuł 45
Samokontrola

Państwa członkowskie i odpowiednie organy UE zapewniają, aby każdy organ uprawniony do dostępu do elementów interoperacyjności podejmował środki niezbędne do monitorowania własnego przestrzegania przepisów niniejszego rozporządzenia oraz aby w razie potrzeby współpracował z organem nadzorczym.

Administratorzy danych, o których mowa w art. 40, podejmują konieczne środki, aby monitorować zgodność przetwarzania danych z przepisami niniejszego rozporządzenia, co obejmuje częstą weryfikację zapisów w rejestrze oraz w razie potrzeby współpracę z organami nadzorczymi, o których mowa w art. 49 i 50.

Artykuł 46
Prawo do informacji

130. Organ gromadzący dane informuje osoby, których dane są przechowywane we wspólnym serwisie kojarzenia danych biometrycznych, wspólnym repozytorium tożsamości lub module wykrywającym multiplikację tożsamości, o przetwarzaniu ich danych w celach związanych z niniejszym rozporządzeniem, bez uszczerbku dla prawa do informacji, o którym mowa w art. 11 i 12 rozporządzenia (WE) nr 45/2001 oraz art. 13 i 14 rozporządzenia (UE) 2016/679. Informacji udziela się w momencie pobrania danych. Należą do nich informacje o tożsamości administratorów danych i ich dane kontaktowe oraz o procedurach związanych z korzystaniem z przysługującego im prawa do dostępu, sprostowania lub usunięcia danych, a także dane kontaktowe Europejskiego Inspektora Ochrony Danych i krajowego organu nadzorczego państwa członkowskiego odpowiedzialnego za pobieranie danych.

131. Osoby, których dane są przechowywane w systemach EES, VIS lub [ETIAS], informuje się o przetwarzaniu ich danych w celach związanych z niniejszym rozporządzeniem zgodnie z ust. 1 w następujących sytuacjach:

a) [tworzenie lub aktualizacja akt osobowych w EES zgodnie z art. 14 rozporządzenia w sprawie EES];

b) tworzenie lub aktualizacja pliku danych dotyczących wniosku w systemie VIS zgodnie z art. 8 rozporządzenia (WE) nr 767/2008;

c) [tworzenie lub aktualizacja pliku danych dotyczących wniosku w systemie ETIAS zgodnie z art. 17 rozporządzenia w sprawie ETIAS];

d) – (nie dotyczy);

e) – (nie dotyczy).

Artykuł 47

Prawo do dostępu do danych oraz żądania ich sprostowania i usunięcia

132. W celu wykonywania swoich praw na mocy art. 13, 14, 15 i 16 rozporządzenia (WE) 45/2001 oraz art. 15, 16, 17 i 18 rozporządzenia (UE) 2016/679 każda osoba ma prawo zwrócić się do państwa członkowskiego odpowiedzialnego za ręczną weryfikację różniących się tożsamości lub do dowolnego innego państwa członkowskiego, a państwo to bada jej wniosek i odpowiada na niego.

133. Państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości zgodnie z art. 29 lub państwo członkowskie, do którego skierowano wniosek, odpowiada na takie wnioski w terminie 45 dni od ich otrzymania.

134. Jeżeli wniosek o sprostowanie lub usunięcie danych osobowych skierowano do państwa członkowskiego innego niż odpowiedzialne państwo członkowskie, wówczas państwo członkowskie, do którego skierowano wniosek, kontaktuje się z właściwymi organami odpowiedzialnego państwa członkowskiego w ciągu siedmiu dni, a odpowiedzialne państwo członkowskie sprawdza poprawność danych i zgodność ich przetwarzania z prawem w ciągu 30 dni od nawiązania takiego kontaktu.

135. Jeśli w wyniku takiego badania zostanie stwierdzone, że dane przechowywane w module wykrywającym multiplikację tożsamości są w istocie niepoprawne lub zostały pobrane z naruszeniem prawa, odpowiedzialne państwo członkowskie lub, w stosownych przypadkach, państwo członkowskie, do którego skierowano wniosek, poprawia lub usuwa takie dane.

136. W przypadku, kiedy odpowiedzialne państwo członkowskie sprostuje dane przechowywane w module wykrywającym multiplikację tożsamości w okresie ich ważności państwo to ma dokonać przetwarzania określonego w art. 27 oraz, w stosownych przypadkach, w art. 29, aby ustalić, czy zmienione dane należy ze sobą powiązać. Jeśli przetwarzanie nie doprowadzi do żadnego trafienia odpowiedzialne państwo członkowskie lub, w stosownych przypadkach, państwo członkowskie, do którego skierowano wniosek, usuwa dane z pliku potwierdzającego tożsamość. Jeśli przetwarzanie automatyczne doprowadzi do wystąpienia jednego trafienia lub kilku trafień, właściwe państwo członkowskie tworzy lub aktualizuje powiązanie między danymi zgodnie z odpowiednimi przepisami niniejszego rozporządzenia.

137. Jeżeli odpowiedzialne państwo członkowskie lub, w stosownych przypadkach, państwo członkowskie, do którego skierowano wniosek, nie zgadza się z argumentem, że dane zarejestrowane w module wykrywającym multiplikację tożsamości są niezgodne ze stanem faktycznym lub że zostały zarejestrowane niezgodnie z prawem, wówczas to państwo członkowskie wydaje niezwłocznie decyzję administracyjną, w której wyjaśnia na piśmie osobie zainteresowanej, dlaczego nie jest gotowe sprostować lub usunąć dotyczących jej danych osobowych.

138. Decyzja ta zawiera też informacje dla osoby zainteresowanej wyjaśniające możliwość odwołania się od decyzji podjętej w odniesieniu do wniosku, o którym mowa w ust. 3, a w stosownych przypadkach informacje dotyczące sposobu wniesienia sprawy lub skargi do właściwych organów lub sądów oraz wszelkie informacje dotyczące pomocy, w tym ze strony właściwych krajowych organów nadzorczych.

139. Wnioski składane na podstawie ust. 3 zawierają informacje niezbędne do zidentyfikowania osoby zainteresowanej. Takie informacje wykorzystuje się wyłącznie w celu zapewnienia możliwości wykonywania praw, o których mowa w ust. 3, po czym niezwłocznie się je usuwa.

140. Odpowiedzialne państwo członkowskie lub, w stosownych przypadkach, państwo członkowskie, do którego skierowano wniosek, odnotowują w formie dokumentu pisemnego, że złożono wniosek, o którym mowa w ust. 3, oraz sposób jego rozpatrzenia, a następnie niezwłocznie udostępniają ten dokument właściwym krajowym organom nadzorczym odpowiedzialnym za ochronę danych.

Artykuł 48
Przekazywanie danych osobowych państwom trzecim, organizacjom międzynarodowym i podmiotom prywatnym

Dane osobowe przechowywane lub udostępniane za pomocą elementów interoperacyjności nie są przekazywane ani udostępniane państwom trzecim, organizacjom międzynarodowym ani podmiotom prywatnym, z wyjątkiem przekazywania danych Interpolowi w celu przeprowadzania ich automatycznego przetwarzania zgodnie z [art. 18 ust. 2 lit. b) i m) rozporządzenia w sprawie ETIAS] lub w celu realizacji przepisów art. 8 ust. 2 rozporządzenia (UE) 2016/399. Takie przekazywanie danych osobowych Interpolowi odbywa się zgodnie z art. 9 rozporządzenia (WE) nr 45/2001 i rozdziałem V rozporządzenia (UE) 2016/679.

Artykuł 49
Nadzór ze strony krajowego organu nadzorczego

141. Organ lub organy nadzorcze wyznaczone na podstawie art. 49 rozporządzenia (UE) 2016/679 zapewniają przeprowadzenie kontroli operacji przetwarzania danych przez właściwe organy krajowe zgodnie z odpowiednimi międzynarodowymi standardami kontroli przynajmniej raz na cztery lata.

142. Państwa członkowskie zapewniają, aby ich organ nadzorczy dysponował zasobami wystarczającymi do wykonania zadań powierzonych mu na podstawie niniejszego rozporządzenia.

Artykuł 50
Nadzór ze strony Europejskiego Inspektora Ochrony Danych

Europejski Inspektor Ochrony Danych zapewnia przeprowadzenie co najmniej raz na cztery lata kontroli działalności eu-LISA w zakresie przetwarzania danych osobowych, zgodnie z odpowiednimi międzynarodowymi standardami przeprowadzania kontroli. Sprawozdanie z takiej kontroli przekazuje się Parlamentowi Europejskiemu, Radzie, agencji eu-LISA, Komisji i państwom członkowskim. Agencja eu-LISA ma możliwość przedstawienia uwag dotyczących sprawozdań przed ich przyjęciem.

Artykuł 51
Współpraca między krajowymi organami nadzorczymi a Europejskim Inspektorem Ochrony Danych

143. Europejski Inspektor Ochrony Danych działa w ścisłej współpracy z krajowymi organami nadzorczymi w kwestiach wymagających zaangażowania organów krajowych, zwłaszcza jeżeli Europejski Inspektor Ochrony Danych lub krajowy organ nadzorczy stwierdzą poważne rozbieżności między praktykami państw

członkowskich lub potencjalnie niezgodne z prawem przekazywanie danych przy wykorzystaniu kanałów komunikacyjnych elementów interoperacyjności, lub w sytuacji, gdy jeden krajowy organ nadzorczy lub kilka takich organów podnosi kwestie dotyczące wdrożenia i interpretacji niniejszego rozporządzenia.

144. W przypadkach, o których mowa w ust. 1, zapewnia się skoordynowany nadzór zgodnie z art. 62 rozporządzenia (UE) nr XXXX/2018 [zmienione rozporządzenie nr 45/2001].

ROZDZIAŁ VIII
Obowiązki

Artykuł 52
Obowiązki eu-LISA w fazie projektowania i opracowywania systemu

145. Agencja eu-LISA zapewnia zgodne z niniejszym rozporządzeniem użytkowanie centralnej infrastruktury elementów interoperacyjności.

146. Elementy interoperacyjności są obsługiwane przez eu-LISA w obiektach technicznych tej agencji i zapewniają funkcje określone w niniejszym rozporządzeniu zgodnie z warunkami bezpieczeństwa, dostępności, jakości i szybkości określonymi w art. 53 ust. 1.

147. Agencja eu-LISA odpowiada za tworzenie elementów interoperacyjności, wszelkie adaptacje konieczne do ustanowienia interoperacyjności między systemami centralnymi EES, VIS, [ETIAS], SIS i Eurodac oraz [systemem ECRIS-TCN] a europejskim portalem wyszukiwania, wspólnym serwisem kojarzenia danych biometrycznych, wspólnym repozytorium tożsamości i modułem wykrywającym multiplikację tożsamości.

Agencja eu-LISA określa architekturę fizyczną elementów interoperacyjności, w tym ich infrastrukturę komunikacyjną i specyfikacje techniczne oraz ich rozwój, jeśli chodzi o infrastrukturę centralną i infrastrukturę bezpiecznej komunikacji, które zarząd przyjmuje po uzyskaniu przychylnej opinii Komisji. Agencja eu-LISA wprowadza też wszelkie konieczne adaptacje do systemów EES, [ETIAS], SIS lub VIS wynikające z ustanowienia interoperacyjności i określone w niniejszym rozporządzeniu.

Agencja eu-LISA tworzy i wdraża elementy interoperacyjności tak szybko, jak to tylko możliwe, po wejściu w życie niniejszego rozporządzenia i przyjęciu przez Komisję środków, o których mowa w art. 8 ust. 2, art. 9 ust. 7, art. 28 ust. 5 i 6, art. 37 ust. 4, art. 38 ust. 4, art. 39 ust. 5 i art. 44 ust. 5.

Opracowywanie tych elementów obejmuje stworzenie i wdrożenie specyfikacji technicznych, przeprowadzenie testów oraz ogólną koordynację projektu.

148. W fazie projektowania i opracowywania powołuje się Komisję ds. Zarządzania Programem składającą się maksymalnie z 10 członków. Komisja ds. Zarządzania Programem składa się z siedmiu członków wyznaczonych przez zarząd eu-LISA spośród jego członków lub ich zastępców, przewodniczącego grupy doradczej ds. interoperacyjności, o której mowa w art. 65, członka reprezentującego eu-LISA wyznaczonego przez jej dyrektora wykonawczego i jednego członka wyznaczonego przez Komisję. Członków wyznaczanych przez zarząd eu-LISA wybiera się jedynie

spośród tych państw członkowskich, które są w pełni związane na mocy prawa Unii aktami ustawodawczymi regulującymi opracowywanie, tworzenie, funkcjonowanie i użytkowanie wszystkich wielkoskalowych systemów informatycznych zarządzanych przez eu-LISA oraz które będą uczestniczyć w elementach interoperacyjności.

149. Komisja ds. Zarządzania Programem spotyka się regularnie, co najmniej trzy razy na kwartał. Zapewnia ona odpowiednie zarządzanie fazą projektowania i rozwoju elementów interoperacyjności.

Komisja ds. Zarządzania Programem co miesiąc przedkłada zarządowi pisemne sprawozdania z postępów w realizacji projektu. Komisji ds. Zarządzania Programem nie przysługują uprawnienia w zakresie podejmowania decyzji ani reprezentowania członków zarządu eu-LISA.

150. Zarząd eu-LISA ustanawia regulamin wewnętrzny Komisji ds. Zarządzania Programem, który obejmuje w szczególności zasady dotyczące:

a) przewodniczenia;

b) miejsca odbywania posiedzeń;

c) przygotowywania posiedzeń;

d) dopuszczenia ekspertów na posiedzenia;

e) planów w zakresie komunikacji zapewniających pełne informacje członkom zarządu, którzy nie uczestniczą w posiedzeniach.

Komisji ds. Zarządzania Programem przewodniczy państwo członkowskie, które jest w pełni związane na mocy prawa Unii aktami ustawodawczymi regulującymi opracowywanie, rozwój, funkcjonowanie i użytkowanie wszystkich wielkoskalowych systemów informatycznych zarządzanych przez eu-LISA.

Agencja zwraca wszystkie koszty podróży i utrzymania poniesione przez członków Komisji ds. Zarządzania Programem, przy czym zastosowanie ma odpowiednio art. 10 regulaminu wewnętrznego eu-LISA. eu-LISA zapewnia prowadzenie sekretariatu Komisji ds. Zarządzania Programem.

Grupa doradcza ds. interoperacyjności, o której mowa w art. 65, spotyka się regularnie do czasu rozpoczęcia funkcjonowania elementów interoperacyjności. Po każdym posiedzeniu grupa doradcza przedkłada sprawozdanie Komisji ds. Zarządzania Programem. Grupa doradcza zapewnia wiedzę techniczną w celu wsparcia Komisji ds. Zarządzania Programem w realizacji jej zadań oraz śledzi stan przygotowania państw członkowskich.

Artykuł 53
Obowiązki eu-LISA po rozpoczęciu funkcjonowania systemów

151. Po rozpoczęciu funkcjonowania każdego z elementów interoperacyjności eu-LISA odpowiada za zarządzanie techniczne infrastrukturą centralną i jednolitymi interfejsami krajowymi. We współpracy z państwami członkowskimi stale zapewnia najlepszą dostępną technologię, z uwzględnieniem analizy kosztów i korzyści. eu-LISA odpowiada też za zarządzanie techniczne całością infrastruktury komunikacyjnej, o której mowa w art. 6, 12, 17, 25 i 39.

Zarządzanie techniczne elementami interoperacyjności obejmuje wszystkie zadania niezbędne do zapewnienia funkcjonowania elementów interoperacyjności przez

24 godziny, 7 dni w tygodniu, zgodnie z niniejszym rozporządzeniem, w szczególności prace konserwacyjne i zmiany techniczne konieczne do zapewnienia zadowalającego poziomu jakości technicznej funkcjonowania systemu, zwłaszcza jeśli chodzi o czas odpowiedzi podczas wyszukiwania w infrastrukturze centralnej, zgodnie ze specyfikacją techniczną.

152. Nie naruszając przepisów art. 17 regulaminu pracowniczego urzędników Unii Europejskiej, eu-LISA stosuje właściwe przepisy dotyczące tajemnicy zawodowej lub inne równoważne obowiązki zachowania poufności do wszystkich swoich pracowników zobowiązanych do pracy z danymi przechowywanymi w elementach interoperacyjności. Zobowiązania te stosuje się także po odejściu takiego personelu z urzędu lub z pracy lub po zakończeniu przez niego działalności.

153. eu-LISA tworzy i aktualizuje mechanizm i procedury przeprowadzania kontroli jakości danych przechowywanych we wspólnym serwisie kojarzenia danych biometrycznych i wspólnym repozytorium tożsamości zgodnie z art. 37.

154. eu-LISA wypełnia też zadania związane z zapewnianiem szkoleń z zakresu technicznego użytkowania elementów interoperacyjności.

Artykuł 54
Obowiązki państw członkowskich

155. Każde państwo członkowskie odpowiada za:

a) podłączenie do infrastruktury komunikacyjnej europejskiego portalu wyszukiwania i wspólnego repozytorium tożsamości;

b) integrację istniejących krajowych systemów i infrastruktury z europejskim portalem wyszukiwania, wspólnym serwisem kojarzenia danych biometrycznych, wspólnym repozytorium tożsamości i module wykrywającym multiplikację tożsamości;

c) organizację swojej istniejącej krajowej infrastruktury, zarządzanie nią, jej funkcjonowanie i utrzymanie oraz jej podłączenie do elementów interoperacyjności;

d) zarządzanie dostępem odpowiednio upoważnionego personelu właściwych organów krajowych do EES oraz dostępem posiadającego odpowiednie pełnomocnictwo personelu właściwych organów krajowych do europejskiego portalu wyszukiwania, wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości oraz ustalenia dotyczące tego dostępu, zgodnie z niniejszym rozporządzeniem, a także sporządzenie listy takich pracowników wraz z ich profilami i jej regularną aktualizację;

e) przyjęcie środków ustawodawczych, o których mowa w art. 20 ust. 3, aby umożliwić dostęp do wspólnego repozytorium tożsamości na potrzeby identyfikacji;

f) ręczną weryfikację różniących się tożsamości, o której mowa w art. 29;

g) wdrożenie wymogów dotyczących jakości danych w systemach informacyjnych UE i elementach interoperacyjności;

h) usuwanie wszelkich niedoskonałości wykrytych w sprawozdaniu oceniającym Komisji dotyczącym jakości danych, o którym mowa w art. 37 ust. 5.

156. Każde państwo członkowskie podłącza systemy należące do swoich wyznaczonych organów określonych w art. 4 ust. 24 do wspólnego repozytorium tożsamości.

Artykuł 55
Obowiązki jednostki centralnej ETIAS

Jednostka centralna ETIAS odpowiada za:

a) ręczną weryfikację różniących się tożsamości, o której mowa w art. 29;

b) wykrywanie multiplikacji tożsamości na podstawie danych przechowywanych w systemach VIS, Eurodac i SIS, zgodnie z art. 59.

ROZDZIAŁ IX
Zmiany w innych aktach unijnych

Artykuł 55a
Zmiany w rozporządzeniu (UE) nr 2016/399

W rozporządzeniu (UE) nr 2016/399 wprowadza się następujące zmiany:

w art. 8 rozporządzenia (UE) 2016/399 dodaje się ust. 4a w brzmieniu:

„4a. Jeśli podczas wjazdu lub wyjazdu w wyniku wyszukiwania w stosownych bazach danych, w tym w module wykrywającym multiplikację tożsamości za pośrednictwem europejskiego portalu wyszukiwania, o których mowa, odpowiednio, w [art. 4 ust. 36 i 33 rozporządzenia 2018/XX w sprawie interoperacyjności] wystąpi powiązanie żółte lub czerwone, osoba poddawana kontroli zostaje skierowana do kontroli drugiej linii.

Straż graniczna w drugiej linii dokonuje wyszukiwania w module wykrywającym multiplikację tożsamości i we wspólnym repozytorium tożsamości, o których mowa w [art. 4 ust. 35 rozporządzenia 2018/XX w sprawie interoperacyjności], lub w Systemie Informacyjnym Schengen lub w obu, aby ocenić różnice w powiązanych ze sobą tożsamościach, oraz dokonuje dodatkowej weryfikacji koniecznej do podjęcia decyzji w sprawie statusu i koloru powiązania oraz decyzji w sprawie wjazdu lub odmowy wjazdu osoby, której dotyczy wyszukiwanie.

Zgodnie z [art. 59 ust. 1 rozporządzenia 2018/XX] niniejszy ustęp obowiązuje wyłącznie od momentu rozpoczęcia funkcjonowania modułu wykrywającego multiplikację tożsamości.”.

Artykuł 55b
Zmiany w rozporządzeniu (UE) nr 2017/2226

W rozporządzeniu (UE) nr 2017/2226 wprowadza się następujące zmiany:

1) w art. 1 dodaje się ustęp w brzmieniu:

„1a. Poprzez przechowywanie danych potwierdzających tożsamość, danych dokumentów podróży i danych biometrycznych we wspólnym repozytorium tożsamości ustanowionym na mocy [art. 17 rozporządzenia 2018/XX w sprawie interoperacyjności] system EES przyczynia się do ułatwienia i wspomagania poprawnej identyfikacji osób zarejestrowanych w EES na warunkach i w ostatecznych celach określonych w [art. 20] powyższego rozporządzenia.”;

2) w art. 3 ust. 1 dodaje się punkt 21a w brzmieniu:

„»wspólne repozytorium tożsamości« oznacza wspólne repozytorium tożsamości określone w [art. 4 ust. 35 rozporządzenia 2018/XX w sprawie interoperacyjności]”;

3) art. 3 ust. 1 pkt 22 otrzymuje brzmienie:

„(22) »dane EES« oznaczają wszystkie dane przechowywane w systemie centralnym EES i wspólnym repozytorium tożsamości zgodnie z art. 14 i art. 16–20.”;

4) w art. 3 dodaje się nowy pkt 22a w brzmieniu:

„(22a) »dane dotyczące tożsamości« oznaczają dane, o których mowa w art. 16 ust. 1 lit. a);”;

5) w art. 6 ust. 1 dodaje się literę w brzmieniu:

„j) zapewnienie poprawnej identyfikacji osób.”;

6) art. 7 ust. 1 lit. a) otrzymuje następujące brzmienie:

„a) wspólnego repozytorium tożsamości, o którym mowa w [art. 17 ust. 2 lit. a) rozporządzenia 2018/XX w sprawie interoperacyjności];

aa) systemu centralnego (zwanego dalej „systemem centralnym EES”);”;

7) art. 7 ust. 1 lit. f) otrzymuje następujące brzmienie:

„f) bezpiecznej infrastruktury komunikacji między systemem centralnym EES a infrastrukturą centralną europejskiego portalu wyszukiwania ustanowionego na mocy [art. 6 rozporządzenia 2018/XX w sprawie interoperacyjności], wspólnego serwisu kojarzenia danych biometrycznych ustanowionego na mocy [art. 12 rozporządzenia 2018/XX w sprawie interoperacyjności], wspólnego repozytorium tożsamości ustanowionego na mocy [art. 17 rozporządzenia 2018/XX w sprawie interoperacyjności] i modułu wykrywającego multiplikację tożsamości ustanowionego na mocy [art. 25 rozporządzenia 2018/XX w sprawie interoperacyjności].”;

8) w art. 7 dodaje się ustęp w brzmieniu:

„1a. Wspólne repozytorium tożsamości zawiera dane, o których mowa w art. 16 ust. 1 lit. a)–d) i art. 17 ust. 1 lit. a)–c), natomiast pozostałe dane są przechowywane w systemie centralnym EES.”;

9) w art. 9 dodaje się ustęp w brzmieniu:

„3. Dostęp do przeglądania danych pochodzących z EES zawartych we wspólnym repozytorium tożsamości jest zarezerwowany wyłącznie dla odpowiednio upoważnionego personelu organów krajowych każdego państwa członkowskiego i odpowiednio upoważnionego personelu organów UE, które są właściwe do celów określonych w [art. 20 i 21 rozporządzenia 2018/XX w sprawie interoperacyjności]. Dostęp taki jest ograniczony do zakresu, w jakim jest to niezbędne do wykonywania zadań tych organów krajowych i unijnych zgodnie ze wspomnianymi celami oraz proporcjonalny do wyznaczonych celów.”;

10) w art. 21 ust. 1 sformułowanie „system centralny EES”, w obu przypadkach, gdy występuje, otrzymuje brzmienie „system centralny EES lub wspólne repozytorium tożsamości”;

11) w art. 21 ust. 2 sformułowanie „do systemu centralnego EES ani do jednolitego interfejsu krajowego” otrzymuje brzmienie „do systemu centralnego EES i wspólnego repozytorium tożsamości ani do jednolitego interfejsu krajowego”;

12) w art. 21 ust. 2 sformułowanie „wprowadzane są do systemu centralnego EES” otrzymuje brzmienie „wprowadzane są do systemu centralnego EES i do wspólnego repozytorium tożsamości”;

13) w art. 32 dodaje się ust. 1a w brzmieniu:

„1a. Jeżeli wyznaczone organy dokonały zapytania we wspólnym repozytorium tożsamości zgodnie z [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności], mają one dostęp do EES w celu przeglądania danych, jeśli według uzyskanej odpowiedzi, o której mowa w [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności] ust. 3, dane te są przechowywane w EES.”;

14) art. 32 ust. 2 otrzymuje brzmienie:

„2. Dostęp do EES jako narzędzia służącego identyfikacji nieznanych osób podejrzanych, sprawców lub nieznanej domniemanej ofiary przestępstwa terrorystycznego lub innego poważnego przestępstwa jest dozwolony jedynie pod warunkiem, że zapytanie we wspólnym repozytorium tożsamości zostanie dokonane zgodnie z [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności] oraz że spełnione zostaną wszystkie warunki wymienione w ust. 1 i 1a.

Jednak ten dodatkowy warunek nie obowiązuje w nagłych przypadkach, w których istnieje potrzeba zapobieżenia bezpośredniemu zagrożeniu dla życia ludzkiego związanemu z przestępstwem terrorystycznym lub innym poważnym przestępstwem. Te uzasadnione podstawy podaje się w sporządzonym w formie elektronicznej lub pisemnej wniosku, przesyłanym przez jednostkę operacyjną wyznaczonego organu do centralnego punktu dostępu.”;

15) uchyla się art. 32 ust. 4;

16) w art. 33 dodaje się ust. 1a w brzmieniu:

„1a. Jeżeli Europol dokonał zapytania we wspólnym repozytorium tożsamości zgodnie z [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności], ma wówczas dostęp do EES w celu dokonania zapytania, jeśli z uzyskanej odpowiedzi, o której mowa w [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności] ust. 3, wynika, że dane te są przechowywane w EES.”;

17) art. 33 ust. 3 otrzymuje brzmienie:

„Stosuje się odpowiednio warunki określone w art. 32 ust. 3 i 5.”;

18) w art. 34 ust. 1 i 2 sformułowanie „w systemie centralnym EES” otrzymuje brzmienie „odpowiednio we wspólnym repozytorium tożsamości i w systemie centralnym EES”;

19) w art. 34 ust. 5 sformułowanie „z systemu centralnego EES” otrzymuje brzmienie „z systemu centralnego EES i ze wspólnego repozytorium tożsamości”;

20) art. 35 ust. 7 otrzymuje brzmienie:

„System centralny EES i wspólne repozytorium tożsamości niezwłocznie przekazują wszystkim państwom członkowskim informację o usunięciu danych z EES i ze wspólnego repozytorium tożsamości oraz, w stosownych przypadkach, usuwają je z wykazu zidentyfikowanych osób, o którym mowa w art. 12 ust. 3.”;

21) w art. 36 sformułowanie „systemu centralnego EES” otrzymuje brzmienie „systemu centralnego EES i wspólnego repozytorium tożsamości”;

22) w art. 37 ust. 1 sformułowanie „rozwój systemu centralnego EES” otrzymuje brzmienie „rozwój systemu centralnego EES i wspólnego repozytorium tożsamości”;

23) w art. 37 ust. 3 akapit pierwszy sformułowanie „system centralny EES” otrzymuje za pierwszym i za trzecim razem, gdy się pojawia, brzmienie „system centralny EES i wspólne repozytorium tożsamości”;

24) w art. 46 ust. 1 dodaje się lit. f) w brzmieniu:

„f) w razie potrzeby odniesienie do korzystania z europejskiego portalu wyszukiwania w celu przeszukania EES zgodnie z [art. 7 ust. 2 rozporządzenia 2018/XX w sprawie interoperacyjności].”;

25) art. 63 ust. 2 otrzymuje brzmienie:

„2. Do celów ust. 1 niniejszego artykułu eu-LISA przechowuje dane określone w ust. 1 w centralnym repozytorium sprawozdawczo-statystycznym, o którym mowa w [art. 39 rozporządzenia 2018/XX w sprawie interoperacyjności].”;

26) w art. 63 ust. 4 dodaje się akapit drugi w brzmieniu:

„Statystyki dzienne są przechowywane w centralnym repozytorium sprawozdawczo-statystycznym.”.

Artykuł 55c
Zmiany w decyzji Rady 2004/512/WE

W decyzji Rady 2004/512/WE w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) wprowadza się następujące zmiany:

art. 1 ust. 2 otrzymuje brzmienie:

„2. Wizowy system informacyjny jest oparty na architekturze scentralizowanej, a w jego skład wchodzą następujące elementy:

a) wspólne repozytorium tożsamości, o którym mowa w [art. 17 ust. 2 lit. a) rozporządzenia 2018/XX w sprawie interoperacyjności];

b) centralny system informacyjny zwany dalej „centralnym wizowym systemem informacyjnym” (CS-VIS);

c) interfejs krajowy w każdym państwie członkowskim, zwany dalej „interfejsem krajowym” (NI-VIS), który zapewnia połączenie z odpowiednimi centralnymi władzami krajowymi danego państwa członkowskiego;

d) infrastruktura komunikacyjna między centralnym wizowym systemem informacyjnym i interfejsami krajowymi;

e) bezpieczny kanał komunikacyjny między systemem centralnym EES i systemem centralnym VIS;

f) bezpieczna infrastruktura komunikacji między systemem centralnym VIS a infrastrukturą centralną europejskiego portalu wyszukiwania ustanowionego na mocy [art. 6 rozporządzenia 2018/XX w sprawie interoperacyjności], wspólnego serwisu kojarzenia danych biometrycznych ustanowionego na mocy [art. 12 rozporządzenia 2018/XX w sprawie interoperacyjności], wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości ustanowionego na mocy [art. 25 rozporządzenia 2018/XX w sprawie interoperacyjności].”.

Artykuł 55d
Zmiany w rozporządzeniu (WE) nr 767/2008

1) w art. 1 dodaje się ustęp w brzmieniu:

„2. Poprzez gromadzenie danych potwierdzających tożsamość, danych dokumentów podróży i danych biometrycznych we wspólnym repozytorium tożsamości ustanowionym na mocy [art. 17 rozporządzenia 2018/XX w sprawie interoperacyjności] system VIS przyczynia się do ułatwienia i wspomagania poprawnej identyfikacji osób zarejestrowanych w systemie VIS na warunkach i w ostatecznych celach określonych w ust. 1 niniejszego artykułu.”;

2) w art. 4 dodaje się punkty w brzmieniu:

„(12) »dane VIS« oznaczają wszystkie dane przechowywane w systemie centralnym VIS i wspólnym repozytorium tożsamości zgodnie z art. 9–14;

(13) »dane dotyczące tożsamości« oznaczają dane, o których mowa w art. 9 ust. 4 lit. a)–aa);

(14) »dane daktyloskopijne« oznaczają dane dotyczące odcisków pięciu palców ręki prawej: wskazującego, środkowego, serdecznego, małego i kciuka, o ile występują, oraz palców ręki lewej;

(15) »wizerunek twarzy« oznacza cyfrowe wizerunki twarzy;

(16) »dane biometryczne« oznaczają dane daktyloskopijne i wizerunek twarzy;”;

3) w art. 5 dodaje się ustęp w brzmieniu:

„1a. Wspólne repozytorium tożsamości zawiera dane, o których mowa w art. 9 ust. 4 lit. a)–cc) oraz art. 9 ust. 5 i 6, natomiast pozostałe dane zawarte w VIS są przechowywane w systemie centralnym VIS.”;

4) art. 6 ust. 2 otrzymuje brzmienie:

„2. Dostęp do VIS do celów przeglądania danych jest zarezerwowany wyłącznie dla odpowiednio upoważnionego personelu organów krajowych każdego państwa członkowskiego, które są organami właściwymi do celów określonych w art. 15–22, oraz dla odpowiednio upoważnionego personelu organów krajowych każdego państwa członkowskiego i organów UE, które są organami właściwymi do celów określonych w [art. 20 i 21 rozporządzenia 2018/XX w sprawie interoperacyjności], i ograniczony do zakresu, w jakim dane te są wymagane do realizacji ich zadań, zgodnie z tymi celami i proporcjonalnie do zamierzonych celów.”;

5) art. 9 ust. 4 lit. a)–c) otrzymują brzmienie:

„a) nazwisko; imię (imiona); data urodzenia; obywatelstwo lub obywatelstwa; płeć;

aa) nazwisko rodowe (poprzednie nazwisko lub nazwiska); miejsce i kraj urodzenia; obywatelstwo przy narodzeniu;

b) rodzaj i numer dokumentu lub dokumentów podróży i trzyliterowy kod państwa wydającego dokument lub dokumenty podróży;

c) data upływu ważności dokumentu lub dokumentów podróży;

cc) organ, który wydał dokument podróży, i data jego wydania;”;

6) art. 9 ust. 5 otrzymuje brzmienie:

„wizerunek twarzy określony w art. 4 ust. 15.”;

7) w art. 29 ust. 2 lit. a) sformułowanie „VIS” otrzymuje brzmienie „VIS lub wspólne repozytorium tożsamości” w obu miejscach, w których się pojawia.

Artykuł 55e
Zmiany w decyzji Rady 2008/633/WSiSW

1) w art. 5 dodaje się ust. 1a w brzmieniu:

„1a. Jeżeli wyznaczone organy dokonały zapytania we wspólnym repozytorium tożsamości zgodnie z [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności], mają one dostęp do systemu VIS w celu przeglądania danych, jeśli według uzyskanej odpowiedzi, o której mowa w [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności] ust. 3, dane te są przechowywane w VIS.”;

2) w art. 7 dodaje się ust. 1a w brzmieniu:

„1a. Jeżeli Europol dokonał zapytania we wspólnym repozytorium tożsamości zgodnie z [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności], ma dostęp do systemu VIS w celu przeglądania danych, jeśli z uzyskanej odpowiedzi, o której mowa w [art. 22 rozporządzenia 2018/XX w sprawie interoperacyjności] ust. 3, wynika, że dane te są przechowywane w VIS.”.

ROZDZIAŁ X
Przepisy końcowe

Artykuł 56
Sprawozdawczość i statystyki

157. Odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji i eu-LISA ma dostęp do następujących danych związanych z europejskim portalem wyszukiwania, wyłącznie do celów sporządzania sprawozdań i statystyk, bez możliwości indywidualnej identyfikacji:

   a) liczba wyszukiwań przypadających na użytkownika profilu ESP;

   b) liczba wyszukiwań w każdej bazie danych Interpolu.

158. Odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji, eu-LISA i jednostki centralnej ETIAS ma dostęp do następujących danych związanych ze wspólnym repozytorium tożsamości, wyłącznie do celów sporządzania sprawozdań i statystyk, bez możliwości indywidualnej identyfikacji:

   a) liczba wyszukiwań w celach określonych w art. 20, 21 i 22;

   b) obywatelstwo, płeć i rok urodzenia osoby, której dotyczy wyszukiwanie;

   c) rodzaj dokumentu podróży oraz trzyliterowy kod państwa wydającego;

   d) liczba wyszukiwań przeprowadzonych z użyciem danych biometrycznych i bez ich użycia.

159. Należycie upoważniony personel właściwych organów państw członkowskich, Komisji, eu-LISA i jednostki centralnej ETIAS ma dostęp do następujących danych związanych z modułem wykrywającym multiplikację tożsamości, wyłącznie do celów sporządzania sprawozdań i statystyk, bez możliwości indywidualnej identyfikacji:

   a) obywatelstwo, płeć i rok urodzenia osoby;

   a) rodzaj dokumentu podróży oraz trzyliterowy kod państwa wydającego;

b) liczba wyszukiwań przeprowadzonych z użyciem danych biometrycznych i bez ich użycia;

c) liczba powiązań każdego rodzaju.

160. Odpowiednio upoważniony personel Europejskiej Agencji Straży Granicznej i Przybrzeżnej ustanowionej rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/1624[76] ma dostęp do przeglądania danych, o których mowa w ust. 1, 2 i 3, na potrzeby przeprowadzania analiz ryzyka i ocen narażenia, o których mowa w art. 11 i 13 tego rozporządzenia.

161. Do celów ust. 1 niniejszego artykułu eu-LISA przechowuje dane, o których mowa w ust. 1 niniejszego artykułu, w centralnym repozytorium sprawozdań i statystyk, o którym mowa w rozdziale VII niniejszego rozporządzenia. Dane zawarte w tym repozytorium nie umożliwiają identyfikacji poszczególnych osób, ale pozwalają organom wymienionym w ust. 1 niniejszego artykułu na uzyskanie sprofilowanych sprawozdań i statystyk w celach zwiększenia efektywności odpraw granicznych, wsparcia organów w rozpatrywaniu wniosków wizowych oraz wsparcia kształtowania unijnej polityki w zakresie migracji i bezpieczeństwa w Unii w oparciu o dowody.

Artykuł 57

Okres przejściowy funkcjonowania europejskiego portalu wyszukiwania

W okresie dwóch lat od daty rozpoczęcia funkcjonowania europejskiego portalu wyszukiwania obowiązki, o których mowa w art. 7 ust. 2 i 4, nie obowiązują, a korzystanie z portalu pozostaje opcjonalne.

Artykuł 58

Okres przejściowy obowiązujący w stosunku do przepisów w sprawie dostępu organów ścigania do wspólnego repozytorium tożsamości

Art. 22, art. 55b pkt 13, 14, 15 i 16 oraz art. 55e obowiązują od dnia rozpoczęcia działań, o których mowa w art. 62 ust. 1.

Artykuł 59

Okres przejściowy obowiązujący w stosunku do wykrywania multiplikacji tożsamości

162. Przez okres jednego roku od wystosowania przez eu-LISA powiadomienia o zakończeniu testu, o którym mowa w art. 62 ust. 1 lit. b), w odniesieniu do modułu wykrywającego multiplikację tożsamości i przed rozpoczęciem jego funkcjonowania, jednostka centralna ETIAS, o której mowa w [art. 33 lit. a) rozporządzenia (UE) 2016/1624], odpowiada za wykrywanie multiplikacji tożsamości między danymi przechowywanymi w systemach VIS, Eurodac i SIS. Operacje wykrywania multiplikacji tożsamości są przeprowadzane przy użyciu wyłącznie danych biometrycznych zgodnie z art. 27 ust. 2 niniejszego rozporządzenia.

[76] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej, zmieniające rozporządzenie Parlamentu Europejskiego (UE) 2016/399 oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 863/2007, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE (Dz.U. L 251 z 16.9.2016, s. 1).

163. Jeśli zapytanie wykaże jedno lub kilka trafień, a dane dotyczące tożsamości zawarte w powiązanych ze sobą aktach osobowych są identyczne lub podobne, ustanawia się powiązanie białe zgodnie z art. 33.

Jeśli zapytanie wykaże jedno lub kilka trafień, a danych dotyczących tożsamości zawartych w powiązanych ze sobą aktach osobowych nie można uznać za podobne, ustanawia się powiązanie żółte zgodnie z art. 30; obowiązuje wówczas procedura, o której mowa w art. 29.

W wypadku wystąpienia kilku trafień tworzone jest powiązanie między wszystkimi elementami danych, które doprowadziły do ich wystąpienia.

164. W razie utworzenia powiązania żółtego moduł wykrywający multiplikację tożsamości udostępnia jednostce centralnej ETIAS dane dotyczące tożsamości obecne w różnych systemach informacyjnych.

165. W razie utworzenia powiązania do wpisu w SIS innego niż wpis dotyczący odmowy wjazdu lub wpis dotyczący zgłoszenia zaginięcia, kradzieży lub unieważnienia dokumentu podróży, zgodnie z, odpowiednio, art. 24 rozporządzenia w sprawie SIS w odniesieniu do odpraw granicznych i art. 38 rozporządzenia w sprawie SIS w odniesieniu do ścigania przestępstw, moduł wykrywający multiplikację tożsamości udostępnia dostęp do danych dotyczących tożsamości obecnych w różnych systemach informacyjnych biuru Sirene państwa członkowskiego, które dokonało wpisu.

166. Jednostka centralna ETIAS lub biuro Sirene państwa członkowskiego, które dokonało wpisu, mają dostęp do danych zawartych w pliku potwierdzającym tożsamość i analizują różne tożsamości, a także aktualizują łącze zgodnie z art. 31, 32 i 33 oraz dodają je do pliku potwierdzającego tożsamość.

167. eu-LISA w razie potrzeby pomaga jednostce centralnej ETIAS w wykrywaniu multiplikacji tożsamości, o którym mowa w niniejszym artykule.

Artykuł 60
Koszty

1. Koszty poniesione w związku z ustanowieniem i funkcjonowaniem europejskiego portalu wyszukiwania, wspólnego serwisu kojarzenia danych biometrycznych, wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości są pokrywane z budżetu ogólnego Unii.

2. Koszty poniesione w związku z integracją istniejącej krajowej infrastruktury oraz jej połączeniem z jednolitymi interfejsami krajowymi, a także w związku z obsługą jednolitych interfejsów krajowych są pokrywane z budżetu ogólnego Unii.

Wyłącza się następujące koszty:

a) funkcjonowania biura zarządzania projektami państw członkowskich (posiedzenia, podróże służbowe, biura);

b) obsługi krajowych systemów informatycznych (pomieszczenia, wdrażanie, energia elektryczna, chłodzenie);

c) funkcjonowania krajowych systemów informatycznych (umowy z operatorami i umowy w zakresie wsparcia);

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

3. Koszty poniesione przez wyznaczone organy, o których mowa w art. 4 ust. 24, są pokrywane, odpowiednio, przez poszczególne państwa członkowskie i Europol. Koszty podłączenia systemów należących do wyznaczonych organów do wspólnego repozytorium tożsamości ponoszą, odpowiednio, poszczególne państwa członkowskie i Europol.

Artykuł 61
Powiadomienia

168. Państwa członkowskie powiadamiają eu-LISA o organach, o których mowa w art. 7, 20, 21 i 26, które mogą korzystać z europejskiego portalu wyszukiwania, wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości oraz uzyskiwać do nich dostęp.

Skonsolidowany wykaz tych organów jest publikowany w *Dzienniku Urzędowym Unii Europejskiej* w terminie trzech miesięcy od daty uruchomienia poszczególnych elementów interoperacyjności zgodnie z art. 62. W przypadku zmian w wykazie eu-LISA raz w roku publikuje zaktualizowany skonsolidowany wykaz.

169. eu-LISA informuje Komisję o pomyślnym zakończeniu testu, o którym mowa w art. 62 ust. 1 lit. b).

170. Jednostka centralna ETIAS powiadamia Komisję o zakończeniu z powodzeniem stosowania środka przejściowego, o którym mowa w art. 59.

171. Komisja udostępnia informacje zgłoszone zgodnie z ust. 1 państwom członkowskim i podaje je do ogólnej wiadomości za pośrednictwem stale aktualizowanej ogólnodostępnej strony internetowej.

Artykuł 62
Uruchomienie systemu

172. Komisja decyduje o dacie planowanego uruchomienia poszczególnych elementów interoperacyjności po tym, jak spełnione zostaną następujące warunki:

a) przyjęto środki, o których mowa w art. 8 ust. 2, art. 9 ust. 7, art. 28 ust. 5 i 6, art. 37 ust. 4, art. 38 ust. 4, art. 39 ust. 5 i art. 44 ust. 5;

b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test odpowiednich elementów interoperacyjności, który eu-LISA przeprowadza we współpracy z państwami członkowskimi;

c) eu-LISA zatwierdziła uzgodnienia techniczne i prawne dotyczące zbierania i przekazywania danych, o których mowa w art. 8 ust. 1, art. 13, art. 19, art. 34 i art. 39 oraz powiadomiła o nich Komisję;

d) państwa członkowskie przekazały Komisji powiadomienia, o których mowa w art. 61 ust. 1;

e) w odniesieniu do modułu wykrywającego multiplikację tożsamości jednostka centralna ETIAS powiadomiła Komisję w sposób określony w art. 61 ust. 3.

173. Komisja informuje Parlament Europejski i Radę o wynikach testu przeprowadzonego zgodnie z ust. 1 lit. b).

174. Decyzja Komisji, o której mowa w ust. 1, jest publikowana w *Dzienniku Urzędowym Unii Europejskiej*.

175. Państwa członkowskie i Europol rozpoczynają korzystanie z elementów interoperacyjności od daty określonej przez Komisję zgodnie z ust. 1.

Artykuł 63
Wykonywanie przekazanych uprawnień

176. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

177. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 8 ust. 2 i art. 9 ust. 7, powierza się Komisji na czas nieokreślony od [*dnia wejścia w życie niniejszego rozporządzenia*].

178. Przekazanie uprawnień, o których mowa w art. 8 ust. 2 i art. 9 ust. 7, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

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

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

181. Akt delegowany przyjęty zgodnie z art. 8 ust. 2 i art. 9 ust. 7 wchodzi w życie tylko wtedy, jeśli ani Parlament Europejski, ani Rada nie wyrażą sprzeciwu w terminie [dwóch miesięcy] od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub jeśli przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformują Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o [dwa miesiące] z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 64
Procedura komitetowa

182. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

183. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 65
Grupa doradcza

eu-LISA ustanawia grupę doradczą w celu uzyskania dostępu do wiedzy fachowej związanej z interoperacyjnością, w szczególności w kontekście sporządzania swojego rocznego programu prac oraz rocznego sprawozdania z działalności. W fazie projektowania i rozwoju instrumentów interoperacyjności obowiązują przepisy art. 52 ust. 4–6.

Artykuł 66
Szkolenia

eu-LISA wykonuje zadania związane z zapewnianiem szkoleń z zakresu technicznego użytkowania elementów interoperacyjności zgodnie z rozporządzeniem (UE) nr 1077/2011.

Artykuł 67
Praktyczny podręcznik

Komisja, w ścisłej współpracy z państwami członkowskimi, eu-LISA i innymi odpowiednimi agencjami, udostępnia praktyczny podręcznik wdrażania elementów interoperacyjności i zarządzania nimi. Ten praktyczny podręcznik zawiera wytyczne o charakterze technicznym i operacyjnym, zalecenia i najlepsze praktyki. Komisja przyjmuje praktyczny podręcznik w formie zalecenia.

Artykuł 68
Monitorowanie i ocena

184. eu-LISA zapewnia wdrożenie procedur w zakresie monitorowania rozwoju elementów interoperacyjności pod kątem celów dotyczących planowania i kosztów oraz procedur w zakresie monitorowania funkcjonowania elementów interoperacyjności pod kątem celów w zakresie rezultatów technicznych, efektywności kosztowej, bezpieczeństwa i jakości działania.

185. Do dnia [*sześć miesięcy od daty wejścia w życie niniejszego rozporządzenia* — do Urzędu Publikacji: proszę zastąpić rzeczywistą datą] i co sześć miesięcy od tego dnia w trakcie fazy rozwojowej elementów interoperacyjności eu-LISA przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie z aktualnej sytuacji w zakresie rozwoju elementów interoperacyjności. Po zakończeniu tworzenia systemu przekazuje się Parlamentowi Europejskiemu i Radzie sprawozdanie zawierające szczegółowe wyjaśnienia dotyczące sposobu osiągnięcia celów, w szczególności w zakresie planowania i kosztów, a także zawierające uzasadnienie wszelkich rozbieżności.

186. Na potrzeby obsługi technicznej eu-LISA ma dostęp do niezbędnych informacji związanych z operacjami przetwarzania danych przeprowadzonymi w ramach elementów interoperacyjności.

187. Cztery lata po rozpoczęciu funkcjonowania poszczególnych elementów interoperacyjności, a następnie co cztery lata, eu-LISA przedkłada Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie dotyczące technicznego funkcjonowania elementów interoperacyjności, w tym ich bezpieczeństwa.

188. Dodatkowo jeden rok po złożeniu każdego ze sprawozdań przez eu-LISA Komisja sporządza ocenę ogólną tych elementów, obejmującą:

a) ocenę stosowania niniejszego rozporządzenia;

b) analizę osiągniętych wyników w stosunku do wyznaczonych celów i ocenę wpływu na prawa podstawowe;

c) ocenę aktualności przesłanek do stworzenia elementów interoperacyjności;

d) ocenę bezpieczeństwa elementów interoperacyjności;

e) ocenę wszelkich konsekwencji, w tym wszelkich nieproporcjonalnych skutków dla płynności ruchu na przejściach granicznych, a także konsekwencji mających wpływ na budżet Unii.

Oceny te obejmują wszelkie konieczne zalecenia. Komisja przekazuje powyższe sprawozdanie oceniające Parlamentowi Europejskiemu, Radzie, Europejskiemu Inspektorowi Danych Osobowych i Agencji Praw Podstawowych Unii Europejskiej ustanowionej na mocy rozporządzenia Rady (WE) nr 168/2007[77].

189. Państwa członkowskie i Europol dostarczają eu-LISA i Komisji informacji niezbędnych do sporządzania sprawozdań, o których mowa w ust. 4 i 5. Informacje te nie mogą stwarzać zagrożenia dla metod pracy ani ujawniać informacji o źródłach, członkach personelu lub dochodzeniach prowadzonych przez wyznaczone organy.

190. eu-LISA przekazuje Komisji informacje niezbędne do sporządzenia ocen, o których mowa w ust. 5.

191. Z poszanowaniem przepisów prawa krajowego dotyczących publikacji danych szczególnie chronionych każde państwo członkowskie i Europol przygotowują coroczne sprawozdania na temat skuteczności dostępu do danych przechowywanych we wspólnym repozytorium tożsamości na potrzeby ścigania przestępstw, zawierające informacje i dane statystyczne dotyczące:

a) dokładnego celu dokonania zapytania, w tym rodzaju przestępstw terrorystycznych lub poważnych przestępstw;

b) przedstawionych uzasadnionych podstaw zasadnego podejrzenia, że osoba podejrzana, sprawca lub ofiara są objęci zakresem [rozporządzenia w sprawie EES], rozporządzenia w sprawie VIS lub [rozporządzenia w sprawie ETIAS];

c) liczby wniosków o uzyskanie dostępu do wspólnego repozytorium tożsamości w celach ścigania przestępstw;

d) liczby i rodzaju spraw, które zakończyły się udaną identyfikacją;

e) potrzeby i zastosowania trybu obowiązującego w szczególnie naglących przypadkach, w tym przypadków, w których w wyniku weryfikacji *ex post* przez centralny punkt dostępu tryb taki nie został zaakceptowany.

Roczne sprawozdania państw członkowskich i Europolu są przekazywane Komisji do dnia 30 czerwca następnego roku.

Artykuł 69
Wejście w życie i stosowanie

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

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

[77] Rozporządzenie Rady (WE) nr 168/2007 z dnia 15 lutego 2007 r. ustanawiające Agencję Praw Podstawowych Unii Europejskiej (Dz.U. L 53 z 22.2.2007, s. 1).

Sporządzono w Strasburgu dnia r.

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

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

1.3. Charakter wniosku/inicjatywy

1.4. Cele

1.5. Uzasadnienie wniosku/inicjatywy

1.6. Okres trwania działania i jego wpływ finansowy

1.7. Planowane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

3.2.2. Szacunkowy wpływ na środki operacyjne

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia interoperacyjności między systemami informacyjnymi Unii Europejskiej służącymi bezpieczeństwu oraz zarządzaniu granicami i migracją.

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

Sprawy wewnętrzne (Tytuł 18)

1.3. Charakter wniosku/inicjatywy

X Wniosek/inicjatywa dotyczy **nowego działania**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego / działania przygotowawczego**[78]

☐ Wniosek/inicjatywa wiąże się z **przedłużeniem bieżącego działania**

☐ Wniosek/inicjatywa dotyczy **działania, które zostało przekształcone pod kątem nowego działania**

1.4. Cele

1.4.1. Wieloletnie cele strategiczne Komisji wskazane we wniosku/inicjatywie

Zarządzanie granicami – ratowanie życia i zabezpieczanie granic zewnętrznych

Elementy interoperacyjności stwarzają szansę na lepsze wykorzystanie informacji zgromadzonych w istniejących systemach UE służących bezpieczeństwu oraz zarządzaniu granicami i migracją. Środki te mają przede wszystkim na celu uniknięcie rejestracji tej samej osoby w różnych systemach pod różnymi tożsamościami. Obecnie identyfikacja jednostkowa osoby fizycznej jest możliwa w ramach danego systemu, lecz nie w sposób międzysystemowy. Może to prowadzić do podejmowania przez władze błędnych decyzji lub być wykorzystywane przez osoby podróżujące w złej wierze w celu ukrycia swojej prawdziwej tożsamości.

Lepsza wymiana informacji

Proponowane środki zapewniają też usprawniony dostęp organów ścigania do tych danych, nadal jednak respektujący wyznaczone granice. Jednak w przeciwieństwie do aktualnej sytuacji, wprowadza się tylko jeden zestaw warunków zamiast różnych takich zestawów dla każdego zbioru danych.

1.4.2. Cel(e) szczegółowy(e) i cel szczegółowy nr [ ]

Ustanowienie elementów interoperacyjności służy następującym celom ogólnym:

a) usprawnieniu zarządzania granicami zewnętrznymi;

b) przyczynieniu się do zapobiegania nielegalnej migracji i jej zwalczania; oraz

[78] Zgodnie z art. 54 ust. 2 lit. a) lub b) rozporządzenia finansowego.

c) przyczynianiu się do podwyższenia poziomu bezpieczeństwa w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej, w tym do utrzymania bezpieczeństwa publicznego i polityki publicznej oraz zagwarantowania bezpieczeństwa na terytoriach państw członkowskich.

Cele zapewnienia interoperacyjności są osiągane poprzez:

a) zapewnienie poprawnej identyfikacji osób;

b) wspieranie walki z oszustwami dotyczącymi tożsamości;

c) poprawę i harmonizację wymogów dotyczących jakości danych w poszczególnych systemach informacyjnych UE;

d) ułatwienie technicznego i operacyjnego wdrożenia przez państwa członkowskie istniejących i przyszłych systemów informacyjnych UE;

e) wzmocnienie i uproszczenie oraz ujednolicenie warunków bezpieczeństwa danych i ochrony danych regulujących odpowiednie systemy informacyjne UE;

f) uproszczenie i ujednolicenie warunków dostępu organów ścigania do systemów EES, VIS, [ETIAS] i Eurodac;

h) wspieranie realizacji celów systemów EES, VIS, ETIAS, Eurodac, SIS i ECRIS-TCN.

Działania ABM/ABB, których dotyczy wniosek/inicjatywa

Rozdział: Bezpieczeństwo i ochrona swobód: Bezpieczeństwo wewnętrzne

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Ogólne zadania niniejszej inicjatywy wynikają z dwóch celów określonych w Traktatach, którymi są:

1. poprawa zarządzania granicami zewnętrznymi strefy Schengen, na podstawie Europejskiego programu w dziedzinie migracji i wydanych w jego następstwie komunikatów, w tym komunikatu dotyczącego utrzymania i wzmocnienia strefy Schengen;

2. przyczynienie się do poprawy bezpieczeństwa wewnętrznego Unii Europejskiej, na podstawie Europejskiej agendy bezpieczeństwa i prac Komisji na rzecz skutecznej i rzeczywistej unii bezpieczeństwa.

Szczegółowe cele polityczne niniejszej inicjatywy na rzecz interoperacyjności są następujące:

Szczegółowe cele niniejszego wniosku są następujące:

1. zapewnienie, aby użytkownicy końcowi — a zwłaszcza funkcjonariusze straży granicznej i organów ścigania, urzędnicy imigracyjni i organy wymiaru sprawiedliwości — dysponowali szybkim, sprawnym, systematycznym i kontrolowanym dostępem do informacji, których potrzebują, aby wykonywać swoje zadania;

2. dostarczenie rozwiązania pozwalającego wykrywać różne tożsamości powiązane z tymi samymi danymi biometrycznymi, co służyłoby podwójnemu celowi poprawnej identyfikacji osób podróżujących w dobrej wierze i zwalczania oszustw dotyczących tożsamości;

3. ułatwienie kontroli tożsamości obywateli państw trzecich na terytorium państw członkowskich przez organy policji; oraz

4. ułatwienie i usprawnienie dostępu organów ścigania do systemów informacyjnych niezwiązanych ze ściganiem przestępstw na szczeblu UE, w razie potrzeby w celach zapobiegania poważnym przestępstwom i terroryzmowi, prowadzenia w ich sprawie dochodzeń, ich wykrywania lub ścigania.

Aby osiągnąć cel szczegółowy nr 1, opracowany zostanie europejski portal wyszukiwania.

Aby osiągnąć cel szczegółowy nr 2, wprowadzony zostanie moduł wykrywający multiplikację tożsamości, wspierany przez wspólne repozytorium tożsamości i wspólny serwis kojarzenia danych biometrycznych.

Aby osiągnąć cel szczegółowy nr 3, upoważnieni urzędnicy otrzymają dostęp do wspólnego repozytorium tożsamości w celu dokonywania identyfikacji.

Aby osiągnąć cel szczegółowy nr 4, wspólne repozytorium tożsamości będzie zawierać funkcję „wynik/brak wyniku”, która umożliwi wprowadzenie dwuetapowego podejścia do dostępu organów ścigania do systemów zarządzania granicami.

W ramach uzupełnienia tych czterech elementów interoperacyjności osiąganie celów opisanych w punkcie 1.4.2 będzie ponadto wspierane przez ustanowienie uniwersalnego formatu wiadomości (UMF) jako standardu UE w zakresie rozwijania systemów informacyjnych w dziedzinach sprawiedliwości i spraw wewnętrznych

oraz poprzez zarządzanie tym formatem, a także poprzez ustanowienie wspólnego repozytorium sprawozdawczo-statystycznego.

1.4.4. *Wskaźniki wyników i wpływu*

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

Każdy z zaproponowanych środków wymaga opracowania, a następnie utrzymania i funkcjonowania tego elementu.

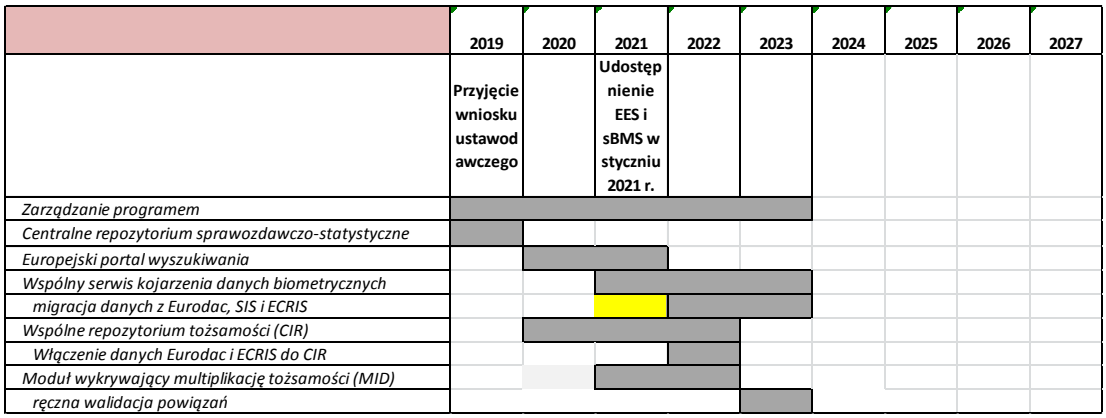
W fazie rozwoju

Każdy element jest rozwijany po spełnieniu warunków wstępnych, tzn. przyjęciu przez współustawodawców odpowiedniego wniosku dotyczącego aktu prawnego oraz spełnienia technicznych warunków wstępnych, ponieważ niektóre elementy mogą zostać skonstruowane dopiero wówczas, gdy pozostałe będą już dostępne.

Cel szczegółowy: gotowość do działania do dnia będącego terminem docelowym

Do końca 2017 r. wniosek zostanie przekazany współustawodawcom w celu przyjęcia. Zakłada się, że proces jego przyjęcia zakończy się w ciągu 2018 r., analogicznie do czasu przyjmowania pozostałych wniosków.

Przy tym założeniu początek fazy rozwojowej usta się na początku 2019 r. (= T0), aby dysponować punktem odniesienia, od którego naliczane będą pozostałe terminy, nie zaś datami absolutnymi. Jeśli przyjęcie aktu przez współustawodawców nastąpi później, cały harmonogram ulegnie odpowiednim zmianom. Z drugiej strony wspólny serwis kojarzenia danych biometrycznych musi być dostępny przed ukończeniem opracowywania wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości. Poniższa tabela przedstawia czas trwania prac rozwojowych:



(Żółte pasmo oznacza konkretne zadanie związane z systemem Eurodac.)

- Wspólne repozytorium sprawozdawczo-statystyczne: termin: T0 + 12 miesięcy (2019–2020)

- Europejski portal wyszukiwania: termin: T0+ 36 miesięcy (2019–2021)

- W pierwszej kolejności zostanie opracowany wspólny serwis kojarzenia danych biometrycznych, aby umożliwić stworzenie systemu wjazdu/wyjazdu (EES). Po realizacji tego kroku aplikacje korzystające ze wspólnego serwisu kojarzenia danych biometrycznych będą wymagały aktualizacji, przeprowadzona też zostanie migracja danych ze zautomatyzowanego systemu identyfikacji daktyloskopijnej SIS (AFIS), zautomatyzowanego systemu identyfikacji daktyloskopijnej Eurodac i danych

z systemu ECRIS-TCN do wspólnego serwisu kojarzenia danych biometrycznych. Termin ukończenia to koniec 2023 r.

- Wspólne repozytorium tożsamości zostanie najpierw utworzone podczas wdrażania systemu wjazdu/wyjazdu (EES). Po zakończeniu opracowywania EES dane z systemów Eurodac i ECRIS zostaną włączone do wspólnego repozytorium tożsamości. Termin ukończenia to koniec 2022 r. (data rozpoczęcia dostępności wspólnego serwisu kojarzenia danych biometrycznych + 12 miesięcy).

- moduł wykrywający multiplikację tożsamości zostanie utworzony po uruchomieniu wspólnego repozytorium tożsamości. Termin ukończenia przewidziany jest na koniec 2022 r. (data dostępności wspólnego serwisu kojarzenia danych biometrycznych + 24 miesiące), należy jednak wziąć pod uwagę wymagający wielu zasobów okres walidacji powiązań między tożsamościami, które sugeruje moduł wykrywający multiplikację. Każde z domniemanych powiązań wymaga walidacji ręcznej. Prace te będą trwały do końca 2023 r.

Okres operacyjny rozpocznie się po zakończeniu powyższej fazy rozwojowej.

Operacje

Wskaźniki związane z każdym celem szczegółowym wymienionym w punkcie 1.4.3 są następujące:

1. Cel szczegółowy: szybki, sprawny i systematyczny dostęp do autoryzowanych źródeł danych

- Liczba wykonanych przypadków użycia (= liczba wyszukiwań, jakie może obsłużyć ESP) w danym okresie.

- Liczba wyszukiwań obsługiwanych przez ESP w porównaniu z całkowitą liczbą wyszukiwań (wykonanych zarówno za pośrednictwem ESP, jak i poszczególnych systemów stosowanych bezpośrednio) w danym okresie.

2. Cel szczegółowy: wykrywanie multiplikacji tożsamości

- Liczba tożsamości powiązanych z tym samym zestawem danych biometrycznych w porównaniu z liczbą tożsamości, dla których dostępne są dane biograficzne w danym okresie.

- Liczba wykrytych przypadków oszustw dotyczących tożsamości w porównaniu z liczbą powiązanych tożsamości i całkowitą liczbą tożsamości w danym okresie.

3. Cel szczegółowy: ułatwienie identyfikacji obywateli państw trzecich

- Liczba wykonanych kontroli identyfikacyjnych w porównaniu z całkowitą liczbą transakcji w danym okresie.

4. Cel szczegółowy: uproszczenie dostępu organów ścigania do autoryzowanych źródeł danych

- Liczba przypadków dostępu w celach związanych ze ściganiem przestępstw w ramach „etapu 1” (= kontrola obecności danych) w danym okresie.

- Liczba przypadków dostępu w celach związanych ze ściganiem przestępstw w ramach „etapu 2” (= rzeczywistego przeglądania danych z systemów UE w określonym zakresie) w danym okresie.

5. Dodatkowy cel przekrojowy: Poprawa jakości danych i ich wykorzystywania do lepszego kształtowaniu polityki

- Regularne sprawozdania z monitorowania jakości danych.

- Liczba wniosków *ad hoc* o informacje statystyczne w danym okresie.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej

Jak wykazała ocena skutków towarzysząca niniejszemu wnioskowi ustawodawczemu, odpowiednie proponowane elementy są konieczne do osiągnięcia interoperacyjności:

• aby osiągnąć cel, jakim jest zapewnienie uprawnionym użytkownikom szybkiego, sprawnego, systematycznego i kontrolowanego dostępu do odpowiednich systemów informacyjnych, należy utworzyć europejski portal wyszukiwania, oparty na wspólnym serwisie kojarzenia danych biometrycznych, uwzględniający wszystkie bazy danych;

• aby osiągnąć cel, jakim jest ułatwienie kontroli tożsamości obywateli państw trzecich na terytorium państw członkowskich przez właściwie uprawnionych urzędników, należy utworzyć wspólne repozytorium tożsamości, zawierające minimalny zestaw danych umożliwiających identyfikację i opierający się na tym samym wspólnym serwisie kojarzenia danych biometrycznych;

• aby osiągnąć cel, jakim jest wykrywanie multiplikacji tożsamości powiązanych z tym samym zestawem danych biometrycznych, co służy zarówno ułatwieniu kontroli tożsamości osób podróżujących w dobrej wierze, jak i zwalczaniu oszustw dotyczących tożsamości, należy utworzyć moduł wykrywający multiplikację tożsamości zawierający powiązania między różnymi tożsamościami zarejestrowanymi w różnych systemach;

• aby osiągnąć cel ułatwienia i usprawnienia dostępu organów ścigania do systemów informacyjnych niezwiązanych ze ściganiem przestępstw, a także aby zapobiegać poważnym przestępstwom i terroryzmowi, prowadzić w ich sprawie dochodzenia, wykrywać je i ścigać, do wspólnego repozytorium tożsamości należy wprowadzić funkcję „wynik/brak wyniku”.

Ponieważ wszystkie cele muszą zostać spełnione, pełnym rozwiązaniem jest łączne stosowanie europejskiego portalu wyszukiwania, wspólnego repozytorium tożsamości (z oznaczeniem „wynik/brak wyniku”) i modułu wykrywającego multiplikację tożsamości, gdzie wszystkie opierałyby się na wspólnym serwisie kojarzenia danych biometrycznych.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii” należy rozumieć jako wartość wynikającą z unijnej interwencji wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Działania są konieczne na szczeblu unijnym, ponieważ systemy, które mają stać się interoperacyjne, będą używane przez wiele państw członkowskich: albo przez wszystkie państwa członkowskie (w przypadku Eurodac), albo przez wszystkie państwa członkowskie będące członkami strefy Schengen (EES, VIS, ETIAS i SIS). Z definicji więc działania te nie mogą zostać podjęte na innym szczeblu.

Główna spodziewana wartość dodana polega na eliminacji przypadków oszustw dotyczących tożsamości, lepszej identyfikacji przypadków, w których jakaś osoba posługuje się różnymi tożsamościami przy wjeździe do UE, oraz unikaniu mylenia osób podróżujących w dobrej wierze z osobami podróżującymi w złej wierze o takim samym nazwisku. Dodatkową wartością dodaną jest to, że proponowana tu interoperacyjność umożliwia łatwiejsze wdrożenie i obsługę techniczną wielkoskalowych systemów informatycznych UE. Dla organów ścigania środki będące przedmiotem niniejszego wniosku powinny prowadzić do częstszego i skuteczniejszego dostępu do konkretnych danych zawartych w wielkoskalowych systemach informatycznych UE. Na poziomie operacyjnym jakość danych można utrzymać i udoskonalać jedynie pod warunkiem jej monitorowania. Ponadto w celach kształtowania i podejmowania decyzji politycznych konieczne jest umożliwienie dokonywania wyszukiwań *ad hoc* w anonimowych danych.

Analiza kosztów i korzyści stanowi część tej oceny skutków i – uwzględniając jedynie korzyści wymierne – spodziewane korzyści można w uzasadniony sposób oszacować na poziomie 77,5 mln EUR rocznie, głównie na rzecz państw członkowskich. Korzyści te wynikają głównie z:

- ograniczonych kosztów zmian w aplikacjach krajowych po uruchomieniu systemu centralnego (według szacunków oszczędności wyniosą 6 mln EUR rocznie dla departamentów informatycznych państw członkowskich);

- oszczędności kosztów wynikających z dysponowania jednym wspólnym serwisem kojarzenia danych biometrycznych zamiast posiadania odrębnego serwisu dla każdego systemu centralnego zawierającego dane biometryczne (szacowane oszczędności wyniosą 1,5 mln EUR rocznie oraz jednorazowo 8 mln EUR dla eu-LISA).

- oszczędności kosztów identyfikacji multiplikacji tożsamości w porównaniu z sytuacją, w której te same rezultaty zostałyby osiągnięte bez zaproponowanych tu środków. Będzie to odpowiadało oszczędnościom wynoszącym co najmniej 50 mln EUR rocznie dla administracji państw członkowskich w wydatkach na zarządzanie granicami i migracją oraz ściganie przestępstw.

- oszczędności w kosztach szkoleń dla licznej grupy użytkowników końcowych w porównaniu z sytuacją, w której konieczne byłyby powtarzające się szkolenia, wynoszące ok. 20 mln EUR rocznie dla administracji państw członkowskich w wydatkach na zarządzanie granicami i migracją oraz ściganie przestępstw.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Doświadczenia związane z rozwojem Systemu Informacyjnego Schengen drugiej generacji (SIS II) i wizowego systemu informacyjnego (VIS) umożliwiły wyciągnięcie następujących wniosków:

1. Każdy nowy system informacyjny w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, zwłaszcza oparty na wielkoskalowym systemie informatycznym, powinien zostać utworzony i rozwijany dopiero po ostatecznym przyjęciu podstawowych instrumentów prawnych określających cel, zakres, funkcje i szczegóły techniczne tego systemu. Podejście takie ma stanowić ewentualne zabezpieczenie przed przekroczeniem kosztów i opóźnieniami wynikającymi ze zmieniających się wymagań.

2. W przypadku SIS II i VIS rozwiązania krajowe w państwach członkowskich mogły być współfinansowane z Funduszu Granic Zewnętrznych (EBF), ale nie było to obowiązkowe. Nie było zatem możliwe uzyskanie ogólnego obrazu stopnia zaawansowania prac w państwach członkowskich, które w swoich programach wieloletnich nie przewidziały odpowiednich działań lub których programy nie były dostatecznie precyzyjne. W związku z tym proponuje się, aby Komisja dokonywała zwrotu wszystkich kosztów integracji ponoszonych przez państwa członkowskie, tak by móc monitorować rozwój sytuacji.

3. Aby ułatwić ogólną koordynację wdrożenia wszystkie proponowane wymiany komunikatów między systemami krajowymi a centralnymi będą wykorzystywać już istniejące sieci i jednolity interfejs krajowy.

1.5.4. Spójność z innymi właściwymi instrumentami oraz możliwa synergia

Zgodność z obecnymi WRF

Rozporządzenie w sprawie Funduszu Bezpieczeństwa Wewnętrznego i wsparcia w zakresie granic jest instrumentem finansowym, w którym uwzględniono budżet przeznaczony na realizację inicjatywy w sprawie interoperacyjności.

Jego art. 5 lit. b) stanowi, że kwota 791 mln EUR ma zostać przeznaczona na program, którego celem jest opracowanie systemów informatycznych, na podstawie istniejących lub nowych systemów informatycznych, wspierających zarządzanie przepływami migracyjnymi przez granice zewnętrzne, z zastrzeżeniem przyjęcia odpowiednich aktów ustawodawczych Unii i na warunkach określonych w art. 15. Z kwoty 791 mln EUR, 480,2 mln EUR jest zarezerwowane na opracowywanie systemu EES, 210 mln EUR — na system ETIAS, a 67,9 mln EUR — na przegląd SIS II. Pozostała kwota (32,9 mln EUR) będzie poddana realokacji za pomocą mechanizmów Funduszu Bezpieczeństwa Wewnętrznego ds. Granic i Wiz. Niniejszy wniosek wymaga kwoty 32,1 mln EUR w obecnym okresie wieloletnich ram finansowych, mieści się zatem w granicach dostępnego budżetu.

Niniejszy wniosek wymaga ogółem budżetu wynoszącego 424,7 mln EUR (z uwzględnieniem działu 5) w okresie od 2019 do 2027 r. Obecne WRF obejmują jedynie dwuletni okres od 2019 do 2020 r. Sporządzono jednak szacunki kosztów do 2027 r. włącznie, aby przekazać dokładny obraz konsekwencji finansowych niniejszego wniosku, nie przesądzając jednak o kształcie kolejnych wieloletnich ram finansowych.

Wnioskowany dziewięcioletni budżet wynosi 424,7 mln EUR i obejmuje także następujące pozycje:

1) 136,3 mln EUR przeznaczone dla państw członkowskich na pokrycie kosztów zmian w ich systemach krajowych, aby mogły korzystać z elementów interoperacyjności i jednolitego interfejsu krajowego dostarczanego przez eu-LISA oraz na szkolenia licznej społeczności użytkowników końcowych. Nie wpływa to na obecne WRF, ponieważ finansowanie będzie przekazywane dopiero od 2021 r.

2) 4,8 mln EUR przeznaczone dla Europejskiej Straży Granicznej i Przybrzeżnej na zatrudnienie zespołu specjalistów, którzy w ciągu jednego roku (2023) będą zatwierdzać powiązania między poszczególnymi tożsamościami po uruchomieniu modułu wykrywającego multiplikację tożsamości. Działania tego zespołu będą związane z ujednoznacznianiem tożsamości zgodnie z zadaniami Europejskiej Straży

Granicznej i Przybrzeżnej na mocy wniosku w sprawie ETIAS. Nie wpływa to na obecne WRF, ponieważ finansowanie będzie przekazywane dopiero od 2021 r.

3) 48,9 mln EUR przeznaczone dla Europolu na aktualizację systemów informatycznych tej agencji, aby przygotować je na ilość komunikatów, które mają otrzymywać, oraz aby zwiększyć ich wydajność. Elementy interoperacyjności będą wykorzystywane przez system ETIAS w celu przeglądania danych Europolu. Aktualne zdolności Europolu do przetwarzania informacji nie odpowiadają jednak znacznym ilościom (średnio 100 000 zapytań dziennie) i skróconemu czasowi udzielenia odpowiedzi. Wydatki z obecnych WRF wyniosą 9,1 mln EUR.

4) 2,0 mln EUR przeznaczone dla CEPOL-u na pokrycie kosztów przygotowania i przeprowadzenia szkoleń dla personelu operacyjnego. Zaplanowano wydatki wysokości 0,1 mln EUR na 2020 r.

5) Kwota 225,0 mln EUR dla eu-LISA, która obejmuje całkowite koszty opracowania programu służącego dostarczeniu pięciu elementów interoperacyjności (68,3 mln EUR), koszty obsługi technicznej od czasu dostarczenia elementów do 2027 r. (56,1 mln EUR), specjalne środki wynoszące 25,0 mln EUR przeznaczone na migrację danych z istniejących systemów do wspólnego serwisu kojarzenia danych biometrycznych oraz dodatkowe koszty aktualizacji jednolitego interfejsu krajowego, sieci, szkoleń i posiedzeń. Specjalne środki w wysokości 18,7 mln EUR obejmują koszty aktualizacji i działania systemu ECRIS-TCN w trybie wysokiej dostępności od 2022 r. Z kwoty całkowitej w czasie trwania bieżących WRF wydana zostanie kwota 23,0 mln EUR.

6) Kwota 7,7 mln EUR dla Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych będzie przeznaczona na pokrycie nieznacznego wzrostu kosztów personelu i kosztów powiązanych w okresie opracowywania poszczególnych elementów, gdyż Komisja będzie też odpowiadać za prace komitetu opracowującego uniwersalny format wiadomości (UMF). Środki ujęte w dziale 5 nie są pokrywane z Funduszu Bezpieczeństwa Wewnętrznego. W celach orientacyjnych należy podać, że w latach 2019–2020 należna będzie kwota 2,0 mln EUR.

Zgodność z wcześniejszymi inicjatywami

Niniejsza inicjatywa jest zgodna z następującymi wcześniejszymi inicjatywami:

W **komunikacie** Komisji z kwietnia 2016 r. ***pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”*** wskazano kilka strukturalnych niedociągnięć związanych z systemami informacyjnymi. W związku z tym zaproponowano następujące trzy działania:

Po pierwsze, Komisja podjęła **działania na rzecz wzmocnienia i maksymalizacji korzyści czerpanych z istniejących systemów informacyjnych**. W grudniu 2016 r. Komisja przyjęła wnioski w sprawie dalszego wzmocnienia istniejącego systemu informacyjnego Schengen (SIS). W międzyczasie, w następstwie wniosku Komisji z maja 2016 r., przyspieszono negocjacje w sprawie zmiany podstawy prawnej systemu Eurodac — unijnej bazy danych zawierającej odciski palców osób ubiegających się o azyl. Wniosek w sprawie nowej podstawy prawnej wizowego systemu informacyjnego (VIS) także jest w przygotowaniu i zostanie przedłożony w drugim kwartale 2018 r.

Po drugie, Komisja wniosła o utworzenie **dodatkowych systemów informacyjnych, aby wyeliminować zidentyfikowane luki** w unijnej strukturze zarządzania danymi.

Negocjacje w sprawie wniosku Komisji z kwietnia 2016 r. na rzecz ustanowienia systemu wjazdu/wyjazdu (EES)[79] — w celu udoskonalenia procedur odprawy granicznej w stosunku do obywateli państw spoza UE podróżujących do UE — zakończono w lipcu 2017 r., gdy współustawodawcy osiągnęli porozumienie polityczne, potwierdzone przez Parlament Europejski w październiku 2017 r. i przyjęte formalnie przez Radę w listopadzie 2017 r. W listopadzie 2016 r. Komisja przedstawiła także wniosek w sprawie ustanowienia europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)[80]. Wniosek ten ma na celu wzmocnienie kontroli bezpieczeństwa w stosunku do podróżnych zwolnionych z obowiązku wizowego, tak aby móc przeprowadzać z wyprzedzeniem kontrole pod kątem nielegalnej migracji i kontrole bezpieczeństwa. Jest on obecnie przedmiotem negocjacji przez współustawodawców. W czerwcu 2017 r. przedstawiono także wniosek w sprawie europejskiego systemu przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (system ECRIS-TCN)[81], aby wyeliminować zidentyfikowaną lukę związaną z wymianą informacji między państwami członkowskimi o obywatelach państw trzecich skazanych za przestępstwa.

Po trzecie, Komisja pracowała **nad interoperacyjnością systemów informacyjnych**, skupiając się na czterech opcjach przedstawionych w komunikacie z kwietnia 2016 r.[82], mających na celu osiągnięcie interoperacyjności. Trzema z tych czterech opcji są właśnie europejski portal wyszukiwania, wspólne repozytorium tożsamości i wspólny serwis kojarzenia danych biometrycznych. Następnie stało się jasne, że należy wprowadzić rozróżnienie między wspólnym repozytorium tożsamości jako bazą danych dotyczących tożsamości a nowym elementem służącym identyfikacji multiplikacji tożsamości powiązanych z tym samym identyfikatorem biometrycznym (moduł wykrywający multiplikację tożsamości). Tymi czterema elementami są zatem obecnie: europejski portal wyszukiwania, wspólne repozytorium tożsamości, moduł wykrywający multiplikację tożsamości i wspólny serwis kojarzenia danych biometrycznych.

Synergia

Synergię należy tu rozumieć jako korzyść wynikającą z wykorzystywania już istniejących rozwiązań i unikania stale nowych inwestycji.

Między omawianymi inicjatywami a opracowaniem systemów EES i ETIAS istnieje znaczna synergia.

Na potrzeby funkcjonowania EES tworzone są akta osobowe dla każdego obywatela państwa trzeciego przekraczającego granicę strefy Schengen w celu krótkiego pobytu. Dlatego aktualny system kojarzenia danych biometrycznych wykorzystywany przez VIS, który zawiera wzorce daktyloskopijne dla wszystkich podróżnych objętych obowiązkiem wizowym, zostanie rozszerzony, tak aby objąć także dane biometryczne podróżnych zwolnionych z obowiązku wizowego. Koncepcja wspólnego serwisu kojarzenia danych biometrycznych stanowi zatem dalszą generalizację serwisu kojarzenia danych biometrycznych, który zostanie skonstruowany w ramach EES. Następnie przeprowadzona zostanie migracja (jest to techniczny termin oznaczający przenoszenie danych z jednego systemu do drugiego) wzorców biometrycznych zawartych w serwisach kojarzenia danych biometrycznych

[79] COM(2016) 194 z dnia 6 kwietnia 2016 r.
[80] COM(2016) 731 z dnia 16 listopada 2016 r.
[81] COM(2017) 344 z dnia 29 czerwca 2017 r.
[82] COM(2016) 205 z dnia 6 kwietnia 2016 r.

systemów SIS i Eurodac do wspólnego serwisu kojarzenia danych biometrycznych. Według danych dostawców przechowywanie w odrębnych bazach danych kosztuje średnio 1 EUR dla każdego zestawu danych biometrycznych (całkowita liczba takich zestawów może wynosić 200 mln), ten średni koszt spada jednak do 0,35 EUR za każdy zestaw po stworzeniu wspólnego rozwiązania w zakresie danych biometrycznych. Wyższe koszty sprzętu komputerowego wymaganego do obsługi dużej ilości danych częściowo równoważą te korzyści, ale ostateczne koszty wspólnego serwisu kojarzenia danych biometrycznych szacuje się jako o 30 % niższe niż w sytuacji, w której te same dane byłyby przechowywane w licznych mniejszych systemach kojarzenia danych biometrycznych.

Aby system ETIAS mógł funkcjonować, konieczny jest element służący do przeszukiwania zestawu systemów unijnych. W tym celu wykorzystywany będzie albo europejski portal wyszukiwania, albo inny element specjalnie skonstruowany w ramach wniosku w sprawie tego portalu. Wniosek w sprawie interoperacyjności umożliwia stworzenie jednego takiego elementu zamiast dwóch.

Osiągnięta zostanie też synergia poprzez ponowne wykorzystanie tego samego jednolitego interfejsu krajowego, który jest używany w przypadku systemów EES i ETIAS. Jednolity interfejs krajowy będzie wymagał aktualizacji, nadal jednak będzie mógł być wykorzystywany.

1.6. Okres trwania działania i wpływ finansowy

☐ Wniosek/inicjatywa o **ograniczonym okresie trwania**

– ☐ Okres trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r.

☒ Wniosek/inicjatywa o **nieograniczonym okresie trwania**

– Faza rozwojowa obejmuje lata 2019–2023 włącznie, po czym nastąpi etap pełnego funkcjonowania.

– Okres trwania wpływu finansowego obejmuje zatem lata 2019–2027.

1.7. Planowane tryby zarządzania[83]

☒ **Bezpośrednie zarządzanie** przez Komisję

– X w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

– ☐ przez agencje wykonawcze

☒ **Zarządzanie dzielone** z państwami członkowskimi

☒ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym;

– ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

– ☐EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

– ☒ organom, o których mowa w art. 208 i 209 rozporządzenia finansowego;

– ☐ organom prawa publicznego;

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

– ☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

– *W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi”.*

Uwagi

Bloki	Etap prac rozwojowych	Faza operacyjna	Tryb zarządzania	Podmiot
Opracowanie i aktualizacja (elementów	X	X	Pośredni	eu-LISA Europol

[83] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Bloki	Etap prac rozwojowych	Faza operacyjna	Tryb zarządzania	Podmiot
interoperacyjności dla systemów centralnych, szkolenia z systemów)				CEPOL
Migracja danych (migracja wzorców biometrycznych do wspólnego serwisu kojarzenia danych biometrycznych), koszty sieci, aktualizacja jednolitych interfejsów krajowych, spotkania i szkolenia	X	X	Pośredni	eu-LISA
Walidacja powiązań podczas tworzenia modułu wykrywającego multiplikację tożsamości	X	-	Pośredni	Europejska Straż Graniczna i Przybrzeżna
Dostosowanie jednolitego interfejsu krajowego, integracja systemów krajowych i szkolenia dla użytkowników końcowych	X	X	Dzielone (lub bezpośrednie) (1)	Komisja Europejska + państwa członkowskie

(1) Niniejszy instrument nie obejmuje żadnych kwot związanych z fazą operacyjną.

Faza rozwojowa rozpocznie się w 2019 r. i będzie trwać do czasu dostarczenia poszczególnych elementów, w okresie od 2019 r. do 2023 r. (zob. pkt 1.4.4.).

1. Zarządzanie bezpośrednie przez Dyrekcję Generalną ds. Migracji i Spraw Wewnętrznych (DG HOME): W fazie rozwojowej Komisja może także w razie konieczności prowadzić działania bezpośrednio. Może to w szczególności obejmować unijne wsparcie finansowe dla działań w postaci dotacji (w tym dla organów krajowych państw członkowskich), zamówienia publiczne lub zwrot kosztów poniesionych przez ekspertów zewnętrznych.

2. Zarządzanie dzielone: w fazie rozwojowej państwa członkowskie będą miały obowiązek dostosowania swoich systemów krajowych, aby uzyskać dostęp do europejskiego portalu wyszukiwania zamiast do poszczególnych systemów (dotyczy to wiadomości wychodzących pochodzących od państw członkowskich), oraz w związku ze zmianami w odpowiedziach na ich wnioski wyszukiwania (wiadomości przychodzące do państw członkowskich). Przeprowadzona zostanie też aktualizacja istniejącego jednolitego interfejsu krajowego używanego przez systemy EES i ETIAS.

3. Zarządzanie pośrednie: eu-LISA odpowiada za fazę rozwojową wszystkich pasm informatycznych projektu, czyli za elementy interoperacyjności, aktualizację jednolitego interfejsu krajowego w każdym państwie członkowskim, aktualizację infrastruktury komunikacyjnej między systemami centralnymi a jednolitymi interfejsami krajowymi, migrację wzorców biometrycznych z istniejących systemów kojarzenia danych

biometrycznych SIS i Eurodac do wspólnego serwisu kojarzenia danych biometrycznych oraz związane z tym czyszczenie danych.

W fazie operacyjnej eu-LISA wykonuje wszystkie działania techniczne związane z obsługą techniczną elementów.

W skład Europejskiej Agencji Straży Granicznej i Przybrzeżnej wejdzie dodatkowy zespół odpowiedzialny za walidację powiązań po uruchomieniu modułu wykrywającego multiplikację tożsamości. Zadanie to jest ograniczone czasowo.

Europol będzie odpowiadać za opracowanie i obsługę techniczną swoich systemów, aby zapewnić interoperacyjność z europejskim portalem wyszukiwania i ETIAS.

CEPOL przygotowuje i przeprowadza szkolenia dla służb operacyjnych na zasadzie szkolenia przyszłych instruktorów.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Zasady nadzoru i sprawozdawczości w odniesieniu do opracowywania i obsługi technicznej pozostałych systemów:

1. eu-LISA zapewnia wdrożenie procedur w zakresie monitorowania rozwoju elementów interoperacyjności pod kątem celów dotyczących planowania i kosztów oraz procedur w zakresie monitorowania funkcjonowania elementów pod kątem celów dotyczących rezultatów technicznych, efektywności kosztowej, bezpieczeństwa i jakości działania.

2. W ciągu sześciu miesięcy od daty wejścia w życie niniejszego rozporządzenia i co sześć miesięcy od tego dnia w trakcie fazy rozwojowej elementów eu-LISA przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie z aktualnej sytuacji w zakresie opracowywania każdego z elementów. Po zakończeniu tworzenia systemu, Parlament Europejski i Rada otrzymają sprawozdanie zawierające szczegółowe wyjaśnienia dotyczące sposobu osiągnięcia określonych celów, w szczególności w zakresie planowania i kosztów, zawierające też uzasadnienie wszelkich rozbieżności.

3. Na potrzeby obsługi technicznej eu-LISA ma dostęp do niezbędnych informacji o operacjach przetwarzania danych przeprowadzonych za pomocą elementów.

4. Cztery lata po rozpoczęciu funkcjonowania ostatniego wdrożonego elementu, a następnie co cztery lata, eu-LISA przedkłada Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie dotyczące technicznego funkcjonowania elementów.

5. Po upływie pięciu lat od uruchomienia ostatniego wdrożonego elementu, a następnie co cztery lata, Komisja przeprowadza ogólną ocenę i przedstawia konieczne zalecenia. Ta całościowa ocena obejmuje: wyniki osiągnięte dzięki tym elementom, z uwzględnieniem ich celów związanych z interoperacyjnością, łatwością utrzymania, wydajnością i konsekwencjami finansowymi oraz oddziaływaniem na prawa podstawowe.

Komisja przekazuje sprawozdania z oceny Parlamentowi Europejskiemu i Radzie.

6. Państwa członkowskie i Europol przekazują eu-LISA i Komisji informacje niezbędne do sporządzania sprawozdań, o których mowa w ust. 4 i 5, zgodnie ze wskaźnikami ilościowymi określonymi odpowiednio przez Komisję lub eu-LISA. Informacje te nie mogą stwarzać zagrożenia dla metod pracy ani ujawniać informacji o źródłach, tożsamości członków personelu lub dochodzeniach prowadzonych przez wyznaczone organy.

7. eu-LISA przekazuje Komisji informacje niezbędne do opracowania całościowych ocen, o których mowa w ust. 5.

8. Z poszanowaniem przepisów prawa krajowego dotyczących publikacji informacji szczególnie chronionych, poszczególne państwa członkowskie i Europol przygotowują sprawozdania roczne ze skuteczności dostępu do danych przechowywanych w systemach UE na potrzeby ochrony porządku publicznego, zawierające informacje i statystyki na temat:

- dokładnego celu przeglądania danych, w tym rodzaju przestępstwa terrorystycznego lub poważnego przestępstwa;

- przedstawionych uzasadnionych podstaw zasadnego podejrzenia, że osoba podejrzana, sprawca lub ofiara są objęci zakresem niniejszego rozporządzenia;

- liczby wniosków o uzyskanie dostępu do elementów na potrzeby ochrony porządku publicznego;

- liczby i rodzaju spraw, które zakończyły się udaną identyfikacją;

- potrzeby i zastosowania trybu obowiązującego w szczególnie naglących przypadkach, w tym przypadków, w których w wyniku weryfikacji *ex post* przez centralny punkt dostępu tryb taki nie został zaakceptowany.

Roczne sprawozdania państw członkowskich i Europolu są przekazywane Komisji do dnia 30 czerwca następnego roku.

2.2. System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko (ryzyka)

Ryzyka wiążą się z opracowaniem informatycznym pięciu elementów przez zewnętrznego wykonawcę działającego na zlecenie eu-LISA. Typowe ryzyko związane z projektami polega na:

1. nieukończeniu projektu w terminie;

2. nieukończeniu projektu w granicach ustalonego budżetu;

3. niewykonaniu projektu w pełnym zakresie.

To pierwsze ryzyko jest najpoważniejsze, ponieważ opóźnienie prowadzi do wyższych kosztów, z których większość wiąże się z czasem trwania: koszty związane z pracownikami, opłacane corocznie koszty licencji itp.

Ryzyko to można załagodzić poprzez stosowanie technik zarządzania projektami, w tym planów awaryjnych w projektach rozwojowych i zapewnienia wystarczającej liczby personelu, aby zapewnić obsługę w momentach najintensywniejszej pracy. Oszacowania wysiłku zwykle dokonuje się przy założeniu obciążenia pracą równomiernie rozłożonego w czasie, podczas gdy w rzeczywistości jest ono nierówne, co wymusza większe przydziały zasobów.

Istnieje kilka rodzajów ryzyka związanych ze zleceniem prac rozwojowych zewnętrznemu wykonawcy:

1. w szczególności ryzyko, że wykonawca nie przeznaczy wystarczających środków na projekt lub opracuje i będzie rozwijać system, który nie będzie odzwierciedlać najnowszej wiedzy naukowej i technicznej;

2. ryzyko, że wykonawca nie będzie w pełni przestrzegał technik administracyjnych i metod prowadzenia wielkoskalowych projektów informatycznych, dążąc do obniżenia kosztów;

3. ponadto nie można całkowicie wykluczyć ryzyka, że wykonawca stanie w obliczu trudności finansowych ze względów niezwiązanych z projektem.

Powyższe rodzaje ryzyka można łagodzić poprzez udzielanie zamówień na podstawie surowych kryteriów jakościowych, sprawdzanie referencji wykonawców i utrzymywanie z nimi bliskich relacji. Jako ostateczność, można wreszcie także

ustanowić rygorystyczne zapisy umowne dotyczące kar i wypowiedzenia umowy oraz stosować je w razie potrzeby.

2.2.2. Informacje dotyczące struktury wewnętrznego systemu kontroli

Agencja eu-LISA ma za zadanie funkcjonować jako centrum doskonałości w dziedzinie rozwoju wielkoskalowych systemów informatycznych i zarządzania nimi. Sporządza ona harmonogram działań związanych z opracowaniem i funkcjonowaniem poszczególnych elementów interoperacyjności obejmujący obsługę techniczną jednolitego interfejsu krajowego w państwach członkowskich.

W fazie rozwojowej wszystkie działania związane z rozwojem będą wykonywane przez eu-LISA. Obejmuje to opracowanie wszystkich pasm projektu. Kosztami związanymi z integracją systemów w państwach członkowskich w fazie rozwojowej zarządza Komisja w drodze zarządzania dzielonego lub za pomocą dotacji.

eu-LISA odpowiada w fazie operacyjnej za zarządzanie techniczne i finansowe centralnie użytkowanymi elementami, a zwłaszcza za udzielanie zamówień i zarządzanie nimi. Komisja będzie zarządzać środkami dla państw członkowskich przeznaczonymi na wydatki na jednostki krajowe za pośrednictwem Funduszu Bezpieczeństwa Wewnętrznego — granice i wizy (programy krajowe).

Aby uniknąć opóźnień na poziomie krajowym, planuje się wprowadzenie skutecznej struktury zarządzania obejmującej wszystkie zainteresowane strony jeszcze przed rozpoczęciem fazy rozwojowej. Komisja zakłada określenie interoperacyjnej architektury na początku projektu, aby mogła być ona zastosowana w projektach EES i ETIAS, ponieważ projekty te budują wspólny serwis kojarzenia danych biometrycznych, wspólne repozytorium tożsamości i europejski portal wyszukiwania oraz z nich korzystają. Członek zespołu zarządzającego projektem interoperacyjności powinien też uczestniczyć w strukturach zarządzania projektami EES i ETIAS.

2.2.3. Oszacowanie kosztów i korzyści wynikających z kontroli i ocena prawdopodobnego ryzyka błędu

Nie podaje się oszacowania, ponieważ kontrola i łagodzenie ryzyka są zadaniami nieodłącznie związanymi ze strukturą zarządzania projektami.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony.

Środki przewidziane na zwalczanie nadużyć finansowych określono w art. 35 rozporządzenia (UE) nr 1077/2011, który stanowi następująco:

1. W celu zwalczania nadużyć finansowych, korupcji i innych bezprawnych działań zastosowanie ma rozporządzenie (WE) nr 1073/1999.

2. Agencja przystępuje do porozumienia międzyinstytucjonalnego dotyczącego wewnętrznych dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) i niezwłocznie wydaje odpowiednie przepisy, które mają zastosowanie do wszystkich pracowników agencji.

3. Decyzje dotyczące finansowania oraz umowy i akty wykonawcze do nich powinny wyraźnie zastrzegać, że Trybunał Obrachunkowy i OLAF mogą, w razie konieczności, przeprowadzać kontrole na miejscu wśród odbiorców funduszy agencji oraz urzędników odpowiedzialnych za ich przyznawanie.

Zgodnie z tym przepisem, w dniu 28 czerwca 2012 r. przyjęto decyzję Zarządu Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości dotyczącą zasad i warunków wewnętrznych dochodzeń w związku z zapobieganiem nadużyciom finansowym, korupcji i wszelkiej innej nielegalnej działalności przynoszącej szkody interesom finansowym Unii.

Zastosowanie będzie miała strategia Dyrekcji Generalnej do Spraw Wewnętrznych dotycząca zapobiegania nadużyciom finansowym i ich wykrywania.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

SZACUNKOWY WPŁYW NA WYDATKI I PERSONEL W 2021 R. I KOLEJNYCH LATACH ZOSTAŁ UMIESZCZONO DO CELÓW DEMONSTRACYJNYCH I NIE PRZESĄDZA O KSZTAŁCIE KOLEJNYCH WIELOLETNICH RAM FINANSOWYCH

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj wydatków	Wkład			
	Numer [Dział……]	Zróżn./niezróżn.[84].	państw EFTA[85]	krajów kandydujących[86]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
3	18.02.01.03 — Inteligentne Granice	Zróżn.	Nie	Nie	Tak	Nie
3	18.02.03 — Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex)	Zróżn.	Nie	Nie	Tak	Nie
3	18.02.04 — Europol	Zróżn.	Nie	Nie	Nie	Nie
3	18.02.05 — CEPOL	Niezróżn.	Nie	Nie	Nie	Nie
3	18.02.07 — Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA)	Zróżn.	Nie	Nie	Tak	Nie

[84] Środki zróżnicowane / środki niezróżnicowane.
[85] EFTA: Europejskie Stowarzyszenie Wolnego Handlu.
[86] Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ na wydatki

[Niniejszą część należy uzupełnić przy użyciu **arkusza kalkulacyjnego dotyczącego danych budżetowych o charakterze administracyjnym** (drugi dokument w załączniku do niniejszej oceny skutków finansowych) i przesłać do CISNET w celu konsultacji między służbami.]

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	3	Bezpieczeństwo i obywatelstwo

DG HOME			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**Rok 2028**	**OGÓŁEM**
•Środki operacyjne													
18.02.01.03 — Inteligentne Granice	Środki na zobowiązania	(1)	0	0	43 150	48 150	45 000	0	**0**	**0**	**0**	**0**	**136 300**
	Środki na płatności	(2.	0	0	34 520	47 150	45 630	9 000	**0**	**0**	**0**	**0**	136 300
Środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne[87]													
Numer linii budżetowej		(3)											
Środki OGÓŁEM dla DG HOME	Środki na zobowiązania	=1+1a +3)	0	0	43 150	48 150	45 000	0	**0**	**0**	**0**	**0**	**136 300**
	Środki na płatności	=2+2a +3	0	0	34 520	47 150	45 630	9 000	**0**	**0**	**0**	**0**	136 300

Wydatki te obejmą następujące koszty:

[87] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

– koszty adaptacji jednolitego interfejsu krajowego, którego rozwój jest finansowany w ramach wniosku w sprawie EES, kwotę budżetu na zmiany w systemach państw członkowskich w celu uwzględnienia zmian w systemach centralnych i kwotę budżetu na szkolenia użytkowników końcowych.

18.02.03 — Europejska Straż Graniczna i Przybrzeżna			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Tytuł 1: Wydatki na personel	Środki na zobowiązania	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Środki na płatności	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Tytuł 2: Wydatki na infrastrukturę i wydatki operacyjne	Środki na zobowiązania	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Środki na płatności	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Tytuł 3: Wydatki operacyjne	Środki na zobowiązania	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Środki na płatności	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
Środki OGÓŁEM dla Europolu	(Środki na zobowiązania ogółem = środki na płatności ogółem)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– Budżet Europejskiej Straży Granicznej i Przybrzeżnej pokrywa wydatki zespołu odpowiedzialnego za walidację powiązań wygenerowanych przez moduł wykrywający multiplikację tożsamości na podstawie dotychczasowych danych (ok. 14 mln rekordów). Liczba powiązań wymagających ręcznej walidacji wynosi ok. 550 000. Specjalny powołany w tym celu zespół zostanie dołączony do zespołu ds. ETIAS Europejskiej Straży Granicznej i Przybrzeżnej, ponieważ ich funkcje są zbliżone i pozwoli to na uniknięcie kosztów powołania zupełnie nowego zespołu. Prace mają się rozpocząć w 2023 r. Pracownicy kontraktowi zostaną zatem zatrudnieni z co najmniej 3-miesięcznym wyprzedzeniem, natomiast ich umowy wygasną do 2 miesięcy po zakończeniu migracji. Zakłada się, że pozostałej części niezbędnych zasobów ludzkich nie będą stanowili pracownicy kontraktowi, lecz zatrudnieni konsultanci. Wyjaśnia to koszty podane w tytule 3 na 2023 r.

Przyjmuje się, że zostaną oni zatrudnieni z miesięcznym wyprzedzeniem. Szczegółowe informacje dotyczące liczebności personelu zostaną podane w późniejszym terminie.

– Tytuł 1 obejmuje zatem koszty 20 pracowników wewnętrznych oraz rezerwy na zwiększenie liczby pracowników odpowiedzialnych za zarządzanie i wsparcie.

– Tytuł 2 obejmuje dodatkowe koszty przyjęcia 10 dodatkowych pracowników wykonawcy.

– Tytuł 3 obejmuje opłaty za 10 dodatkowych pracowników wykonawcy. Nie uwzględniono żadnych innych rodzajów kosztów.

18.02.04 — Europol			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Tytuł 1: Wydatki na personel	Środki na zobowiązania	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Środki na płatności	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Tytuł 2: Wydatki na infrastrukturę i wydatki operacyjne	Środki na zobowiązania	(1a)	0	0	0	0	0	0	0	0	0	0
	Środki na płatności	(2a)	0	0	0	0	0	0	0	0	0	0
Tytuł 3: Wydatki operacyjne	Środki na zobowiązania	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Środki na płatności	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
Środki OGÓŁEM dla Europolu	(Środki na zobowiązania ogółem = środki na płatności ogółem)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Wydatki Europolu obejmą modernizację zdolności systemów informatyczno-komunikacyjnych Europolu do przetwarzania zwiększonej ilości komunikatów oraz podniesienie wymaganych poziomów wydajności (czas odpowiedzi).

Tytuł 1 „Wydatki na personel” obejmuje koszty związane z zatrudnieniem dodatkowych pracowników branży ICT w celu wzmocnienia systemów informacyjnych Europolu ze względów opisanych powyżej. Dalsze szczegóły podziału stanowisk między pracownikami zatrudnionymi na czas określony a pracownikami kontraktowymi oraz wymaganej od nich wiedzy podano niżej.

Tytuł 3 obejmuje koszty sprzętu komputerowego i oprogramowania konieczne do wzmocnienia systemów informacyjnych Europolu. Aktualnie systemy informatyczne Europolu służą ograniczonej, wyznaczonej grupie, do której należy Europol, oficerowie łącznikowi Europolu i śledczy z państw członkowskich, którzy korzystają z nich w celach analitycznych i śledczych. Wraz z wdrożeniem QUEST (interfejsu systemowego, który umożliwi europejskiemu portalowi wyszukiwania przeszukiwanie danych Europolu) przy podstawowym poziomie ochrony (obecnie systemy informacyjne Europolu mogą być sklasyfikowane nawet jako *EU restricted* i *EU confidential*) systemy informacyjne Europolu zostaną udostępnione znacznie większej grupie uprawnionych organów ścigania. Z europejskiego portalu wyszukiwania korzystać będzie ponadto system ETIAS do automatycznego przeglądania danych Europolu w celu rozpatrywania zezwoleń na podróż. Zwiększy to liczbę zapytań dotyczących danych Europolu z obecnego poziomu ok. 107 000 miesięcznie do ponad 100 000 zapytań dziennie oraz będzie wymagało całodobowej dostępności systemów informacyjnych Europolu i bardzo skróconego czasu odpowiedzi, aby spełnić wymogi nałożone przez rozporządzenie w sprawie ETIAS. Większość tych kosztów ogranicza się do okresu przed uruchomieniem elementów interoperacyjności, jednak pewne zobowiązania bieżące będą konieczne, aby zapewnić wysoką i stałą dostępność systemów informacyjnych Europolu. Konieczne będą także pewne prace rozwojowe, aby Europol mógł wdrożyć elementy interoperacyjności, których będzie użytkownikiem.

18.02.05 — CEPOL			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Tytuł 1: Wydatki na personel	Środki na zobowiązania	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Środki na płatności	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Tytuł 2: Wydatki na infrastrukturę i wydatki operacyjne	Środki na zobowiązania	(1a)	0	0	0	0	0	0	0	0	0	0
	Środki na płatności	(2a)	0	0	0	0	0	0	0	0	0	0
Tytuł 3: Wydatki operacyjne	Środki na zobowiązania	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Środki na płatności	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Środki OGÓŁEM dla CEPOL-u	(Środki na zobowiązania ogółem =	=1+1a +3a	0	0,144	0.384,	0,482	0,208	0,208	0,208	0,208	0,208	2,050

	środki na płatności ogółem)											

Centralna koordynacja szkoleń na szczeblu UE ułatwia spójne prowadzenie szkoleń na szczeblu krajowym i w rezultacie zapewnia poprawne i udane wdrożenie i użytkowanie elementów interoperacyjności. CEPOL, jako Agencja UE ds. Szkolenia w Dziedzinie Ścigania, jest odpowiednim organem do przeprowadzania szkoleń na centralnym szczeblu unijnym. Wydatki te obejmują przygotowanie szkoleń dla instruktorów z państw członkowskich, koniecznych do rozpoczęcia użytkowania systemów centralnych po ich uruchomieniu. Koszty te obejmują koszty niewielkiego zwiększenia liczebności personelu CEPOL-u odpowiedzialnego za koordynację, organizację i aktualizację kursów oraz koszty przeprowadzenia każdego roku szeregu sesji szkoleniowych i przygotowania kursu internetowego. Szczegóły tych kosztów wyjaśniono poniżej. Aktywność szkoleniowa będzie miała miejsce przede wszystkim w okresach bezpośrednio poprzedzających uruchomienie. Po uruchomieniu konieczne będą stałe dalsze działania w związku z obsługą techniczną oraz tym, że instruktorami nie zawsze będą te same osoby, zgodnie z doświadczeniami zdobytymi przy okazji prowadzenia istniejących szkoleń z Systemu Informacyjnego Schengen.

18.02.07 — eu-LISA			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Tytuł 1: Wydatki na personel	Środki na zobowiązania	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Środki na płatności	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Tytuł 2: Wydatki na infrastrukturę i wydatki operacyjne	Środki na zobowiązania	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Środki na płatności	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Tytuł 3: Wydatki operacyjne	Środki na zobowiązania	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Środki na płatności	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Środki OGÓŁEM dla eu-LISA	(Środki na zobowiązania ogółem = środki na płatności ogółem)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Wydatki te obejmą:

– opracowanie i obsługę techniczną czterech elementów interoperacyjności (europejski portal wyszukiwania, wspólny serwis kojarzenia danych biometrycznych, wspólne repozytorium tożsamości i moduł wykrywający multiplikację tożsamości), ujętych we wniosku dotyczącym rozporządzenia, oraz wspólnego repozytorium sprawozdawczo-statystycznego. eu-LISA będzie działać w charakterze przedstawiciela właściciela projektu i korzystać z własnego personelu, aby sporządzać specyfikacje, wybierać wykonawców, kierować swoimi pracami, poddawać rezultaty szeregowi testów i dokonywać odbioru wykonanych prac;

– koszty związane z migracją danych z dotychczasowych systemów do nowych elementów. eu-LISA nie odgrywa jednak bezpośredniej roli w początkowym przekazywaniu danych do modułu wykrywającego multiplikację tożsamości (walidacja powiązań), ponieważ działanie to dotyczy samej treści danych. Migracja danych biometrycznych z dotychczasowych systemów wiąże się z formatem i oznakowaniem danych, nie zaś z ich treścią;

– koszty aktualizacji systemu ECRIS-TCN, aby stał się systemem o wysokiej dostępności od 2022 r., i jego funkcjonowania. ECRIS-TCN to system centralny zawierający informacje z rejestrów karnych dotyczące obywateli państw trzecich. System ten ma zostać udostępniony od 2020 r. Zgodnie z oczekiwaniami elementy interoperacyjności mają także uzyskiwać dostęp do tego systemu, który musi przez to stać się systemem o wysokiej dostępności. Wydatki operacyjne obejmują dodatkowe koszty osiągnięcia takiej wysokiej dostępności. W 2021 r. występują znaczne koszty opracowania, a następnie stałe koszty związane z obsługą techniczną i funkcjonowaniem. Koszty te nie zostały ujęte w ocenie skutków finansowych regulacji dotyczącej przeglądu rozporządzenia ustanawiającego eu-LISA[88], która uwzględnia tylko budżety od 2018 do 2020 r., zatem nie pokrywa się z niniejszym wnioskiem budżetowym;

– struktura wydatków jest wynikiem sekwencyjnego charakteru projektów. Ponieważ poszczególne elementy są od siebie wzajemnie uzależnione, faza rozwojowa będzie trwała od 2019 r. do 2023 r. Jednak już od 2020 r. rozpoczną się prace związane z obsługą techniczną i funkcjonowaniem pierwszych dostępnych elementów. Wyjaśnia to, dlaczego wydatki są na początku niewielkie, następnie zwiększają się, a potem maleją do stałej wartości;

– wydatki ujęte w tytule 1 (wydatki na personel) będą zgodne z kolejnością projektów: konieczne będzie zwiększenie liczby pracowników, aby zrealizować projekt z udziałem wykonawcy (związane z tym wydatki podano w tytule 3). Po realizacji projektu część zespołu projektowego przejmie odpowiedzialność za jego rozwój i obsługę techniczną. Jednocześnie liczba pracowników odpowiedzialnych za użytkowanie nowo dostarczonych systemów zwiększy się;

[88] COM 2017/0145 (COD) Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości oraz zmieniającego rozporządzenie (WE) nr 1987/2006 i decyzję Rady 2007/533/WSiSW i uchylającego rozporządzenie (UE) nr 1077/2011

– wydatki ujęte w tytule 2 (wydatki na infrastrukturę i wydatki operacyjne) obejmują dodatkową przestrzeń biurową przeznaczoną na tymczasowe pomieszczenie zespołów wykonawcy odpowiedzialnych za opracowanie, obsługę techniczną i zadania operacyjne. Harmonogram wydatków uwzględnia zatem także zmiany w wymaganej liczbie pracowników. Koszty dodatkowego wyposażenia już zostały ujęte w budżecie eu-LISA. Z pracownikami eu-LISA nie wiążą się żadne dodatkowe koszty, ponieważ koszty ich pracy już zostały ujęte w standardowych kosztach personelu;

– Wydatki ujęte w tytule 3 (wydatki operacyjne) obejmują koszy wykonawcy związane z opracowaniem i obsługą techniczną systemu oraz nabyciem odpowiedniego sprzętu komputerowego i oprogramowania.
Koszty wykonawcy pierwotnie rozpoczynają się od badań w celu ustalenia specyfikacji elementów oraz rozpoczęcia prac rozwojowych nad wyłącznie jednym elementem (centralne repozytorium sprawozdawczo-statystyczne). W okresie 2020–2022 koszty wzrastają w miarę, jak większa liczba elementów jest opracowywana równolegle. Po osiągnięciu punktu szczytowego koszty nie przestają rosnąć, ponieważ w niniejszym portfelu projektów zadania związane z migracją danych pochłaniają szczególnie dużo nakładów. Koszty wykonawcy następnie maleją w miarę dostarczania poszczególnych elementów i wkraczania w tryb operacyjny, który wymaga stałej struktury zasobów.
Jednocześnie z wydatkami ujętymi w tytule 3 wydatki w 2020 r. znacznie się zwiększają w porównaniu poprzednim rokiem ze względu na początkową inwestycję w sprzęt i oprogramowanie konieczne podczas opracowywania systemów; Wydatki ujęte w tytule 3 (wydatki operacyjne) rosną w 2021 i 2022 r., ponieważ koszty inwestycji w sprzęt komputerowy i oprogramowanie związane z informatycznymi środowiskami operacyjnymi (faza produkcyjna i przedprodukcyjna zarówno jednostki centralnej, jak i zapasowej jednostki centralnej) są ponoszone w roku poprzedzającym uruchomienie, odpowiednio, elementów interoperacyjności o znacznych wymaganiach związanych z oprogramowaniem i sprzętem (wspólne repozytorium tożsamość i moduł wykrywający multiplikację tożsamości). Po uruchomieniu koszty sprzętu komputerowego i oprogramowania to głównie koszty obsługi technicznej.

– Więcej szczegółów podano poniżej.

Dział wieloletnich ram finansowych	**5**	„Wydatki administracyjne”

w mln EUR (do trzech miejsc po przecinku)

		Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
DG HOME											
• Zasoby ludzkie Numer linii budżetowej 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Pozostałe koszty administracyjne (spotkania itp.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
OGÓŁEM DG HOME	Środki	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Środki OGÓŁEM na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

w mln EUR (do trzech miejsc po przecinku)

		Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	Rok 2028	**OGÓŁEM**
Środki OGÓŁEM w ramach DZIAŁÓW 1 do 5 wieloletnich ram finansowych	Środki na zobowiązania	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Środki na płatności	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Szacunkowy wpływ na środki operacyjne

3.2.2.1. Szacunkowy wpływ na środki Europejskiej Agencji Straży Granicznej i Przybrzeżnej

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty **Europejska Straż Graniczna i Przybrzeżna** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[89]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 1[90] Walidacja powiązań																						
Liczba pracowników zatrudnionych jako eksperci odpowiedzialni za walidację powiązań	Koszty wykonawcy		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Cel szczegółowy nr 1 — suma cząstkowa			**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

[89] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[90] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

Wydatki te obejmą:

- zatrudnienie wystarczającej liczby dodatkowych pracowników (ok. 10 ekspertów), którzy dołączą do obecnych pracowników wewnętrznych (ok. 20 osób), których przyjmie Europejska Straż Graniczna i Przybrzeżna w celu walidacji powiązań. Na rekrutację pracowników, aby osiągnąć wymagany poziom personelu, przed planowaną datą rozpoczęcia przeznaczono tylko jeden miesiąc;

- nie sporządzono szacunków dotyczących jakichkolwiek innych kosztów wykonawcy. Wymagane oprogramowanie stanowi część kosztów licencyjnych wspólnego serwisu kojarzenia danych biometrycznych. Nie określono możliwości przetwarzania oferowanych przez sprzęt. Zakłada się, że pracowników wykonawcy przyjmie Europejska Straż Graniczna i Przybrzeżna. Dlatego w ramach wydatków ujętych w tytule 2 dodano roczne koszty powierzchni wynoszącej ok. 12 metrów kwadratowych na osobę.

3.2.2.2. Szacunkowy wpływ na środki Europolu

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty Europol ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[91]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 1[92] Rozwój i utrzymanie systemów (Europolu)																						
Środowisko informatyczne	Infrastruktura					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
Środowisko informatyczne	Sprzęt komputerowy					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
Środowisko informatyczne	Oprogramowanie					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948

[91] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[92] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

Prace rozwojowe	Wykonawca				0,360		0,360												0,720
Suma cząstkowa			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Wskazane wydatki będą przeznaczone na pokrycie potrzeb związanych ze wzmocnieniem systemów informacyjnych i infrastruktury Europolu, aby obsłużyć zwiększoną liczbę zapytań. Koszty te obejmują:

- modernizację infrastruktury bezpieczeństwa i sieci, sprzęt komputerowy (serwery, pamięć) i oprogramowanie (licencje). Ulepszenia te muszą zostać ukończone przed uruchomieniem europejskiego portalu wyszukiwania i ETIAS w 2021 r. Koszty zostały równomiernie rozłożone na lata 2020 i 2021. Od 2022 r. jako podstawę do obliczania kosztów obsługi technicznej przyjęto roczny współczynnik kosztów obsługi technicznej wynoszący 20 %. Dodatkowo uwzględniono standardowy pięcioletni cykl wymiany nieaktualnego sprzętu i nieaktualnej infrastruktury.
- Koszty wykonawcy w związku z pracami rozwojowymi w celu wdrożenia interfejsu QUEST o podstawowym poziomie ochrony.

3.2.2.3. Szacunkowy wpływ na środki operacyjne CEPOL-u

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty CEPOL ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[93]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 1[94] Opracowanie i prowadzenie szkoleń																						
Liczba kursów stacjonarnych	0,34 na kurs		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Szkolenia online	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Suma cząstkowa				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

[93] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[94] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

Aby zapewnić jednolitość wdrożenia i użytkowania rozwiązań w zakresie interoperacyjności, szkolenia będą organizowane zarówno centralnie na szczeblu UE przez CEPOL, jak i przez państwa członkowskie. Wydatki na szkolenia na szczeblu UE obejmują:

- opracowanie wspólnego programu szkoleń wykorzystywanego przez państwa członkowskie podczas szkoleń krajowych;

- szkolenia stacjonarne dla instruktorów. W ciągu dwóch lat bezpośrednio po uruchomieniu elementów interoperacyjności szkolenia mają zostać wdrożone na szerszą skalę, a następnie przyjąć formę dwóch kursów rocznie.

- kurs online uzupełniający szkolenia stacjonarne na szczeblu UE i w państwach członkowskich.

3.2.2.4. Szacunkowy wpływ na środki eu-LISA

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[95]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 1[96] Rozwój elementów interoperacyjności																						
Budowa systemów	Wykonawca			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Oprogramowanie	Oprogramowanie			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Sprzęt komputerowy	Sprzęt komputero			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
Szkolenie informatyczne	Szkolenia i inne			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340

[95] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[96] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

Cel szczegółowy nr 1 — suma cząstkowa		**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Cel ten obejmuje jedynie koszty dostarczenia czterech elementów interoperacyjności i centralnego repozytorium sprawozdawczo-statystycznego.

– Koszty wspólnego serwisu kojarzenia danych biometrycznych oszacowano przy założeniu, że mający zostać wkrótce opracowany EES posłuży jako system podstawowy do jego opracowania. Planowane jest zatem ponowne użycie licencji na oprogramowanie do przetwarzania danych biometrycznych (36 mln EUR) przewidzianych dla EES.

– W ramach tego budżetu wspólny serwis kojarzenia danych biometrycznych traktuje się jako dalsze rozszerzenie serwisu kojarzenia danych biometrycznych stworzonego na potrzeby EES. Dlatego obecny arkusz finansowy obejmuje koszt krańcowy licencji na oprogramowanie (6,8 mln EUR) na dodanie ok. 20 mln zestawów danych biometrycznych zawartych w AFIS Systemu Informacyjnego Schengen (AFIS to zautomatyzowany system identyfikacji daktyloskopijnej = „serwis kojarzenia danych biometrycznych” SIS), zautomatyzowanym systemie identyfikacji daktyloskopijnej Eurodac i przyszłym ECRIS-TCN (europejskim systemie przekazywania informacji z rejestrów karnych o obywatelach państw trzecich) do serwisu kojarzenia danych biometrycznych sporządzonego z myślą o EES. W niniejszym arkuszu finansowym zawarto koszty integracji różnych systemów (SIS, Eurodac, ECRIS-TCN) ze wspólnym serwisem kojarzenia danych biometrycznych.

– W ramach prac prowadzonych w latach 2019 i 2020 eu-LISA będzie odpowiadać za opracowanie szczegółowego rozwiązania technicznego, w momencie przedłożenia niniejszego wniosku ustawodawczego nie można jednak jeszcze określić tego rozwiązania ani oszacować konsekwencji finansowych wdrożenia takiego preferowanego rozwiązania technicznego. Może ono wymagać zmian w przedstawionych tu szacowanych kosztach.

– Wszystkie elementy zostaną dostarczone do 2023 r., co wyjaśnia, dlaczego koszty wykonawcy spadają wówczas do niemal zera. Pozostaje jedynie kwota przeznaczona na cykliczne aktualizacje centralnego repozytorium sprawozdawczo-statystycznego.

– W okresie od 2019 do 2021 r. wydatki na oprogramowanie znacznie się zwiększają, ponieważ należy wówczas ponieść koszty licencji na oprogramowanie związane z różnymi środowiskami wymaganymi na etapach produkcyjnym, przedprodukcyjnym i testowym, zarówno w odniesieniu do witryny centralnej, jak i zapasowej. Dodatkowo pewne szczegółowe i niezbędne elementy oprogramowania są wyceniane według liczby „obiektów, do których występują odniesienia” (tzn. ilości danych). Ponieważ w ostateczności baza danych będzie zawierać ok. 220 mln tożsamości, cena oprogramowania będzie proporcjonalne do tej wartości.

Określić cele i produkty eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[97]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 2 Obsługa techniczna i funkcjonowanie elementów interoperacyjności																						
Utrzymanie funkcjonowania systemów	Wykonawca			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Oprogramowanie	Oprogramowanie			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Sprzęt komputerowy	Sprzęt komputerowy			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
Szkolenie	Szkolenia			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Cel szczegółowy nr 2 — suma cząstkowa				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– Obsługa techniczna rozpocznie się tuż po dostarczeniu niektórych elementów interoperacyjności. Budżet przeznaczony dla wykonawcy odpowiedzialnego za utrzymanie został przedstawiony zatem od momentu dostarczenia europejskiego portalu wyszukiwania (w 2021 r.).

[97] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

Budżet przeznaczony na utrzymanie zwiększa się w miarę, jak dostarczane są nowe elementy, a następnie osiąga w przybliżeniu stałą wartość stanowiącą odsetek (między 15 % a 22 %) inwestycji początkowej.

– Utrzymanie sprzętu komputerowego i oprogramowania rozpoczyna się od roku uruchomienia: ewolucja kosztów jest podobna do tej przewidzianej w przypadku kosztów wykonawcy.

Określić cele i produkty eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[98]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 3[99] Migracja danych																						
Migracja danych z dotychczasowych systemów kojarzenia danych biometrycznych	do wspólnego serwisu kojarzenia danych biometrycznych			0		0		0		7,000		3,000		0		0		0		0		10,000
Umożliwienie migracji dotychczasowych danych EDAC	Dostosowanie i przebudowa EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Cel szczegółowy nr 3 — suma cząstkowa				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

[98] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[99] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

– W przypadku projektu wspólnego serwisu kojarzenia danych biometrycznych konieczna jest migracja danych z pozostałych wyszukiwarek danych biometrycznych do tego serwisu, ponieważ ten wspólny system cechuje się większą skutecznością operacyjną i jest korzystniejszy finansowo w porównaniu z sytuacją, w której utrzymana zostałaby większa liczba mniejszych serwisów kojarzenia danych biometrycznych.

– Aktualna logika działania systemu Eurodac nie jest jasno oddzielona od mechanizmu kojarzenia danych biometrycznych tak jak ma to miejsce w przypadku systemu kojarzenia danych biometrycznych działającego w ramach VIS. Funkcjonowanie wewnętrzne Eurodac i mechanizmu, za którego pomocą służby operacyjne uruchamiają podstawowe usługi kojarzenia danych biometrycznych, stanowi dla zewnętrznego świadka czarną skrzynkę i opiera się na zastrzeżonej technologii. Zwyczajna migracja danych do wspólnego systemu kojarzenia danych biometrycznych przy jednoczesnym utrzymaniu obecnej warstwy biznesowej nie będzie możliwa. Migracji danych towarzyszą zatem znaczne koszty związane ze zmianą mechanizmów wymiany z aplikacją centralną Eurodac.

Określić cele i produkty eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[100]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 4[101] Sieć																						
Połączenia sieciowe	Konfiguracja sieci			0		0		0		0,505										0		0,505
Obsługa ruchu sieciowego	Operacje sieciowe			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Cel szczegółowy nr 4 — suma				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

[100] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).
[101] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

cząstkowa																						

– Elementy interoperacyjności mają jedynie minimalny wpływ na ruch sieciowy. Jeśli chodzi o dane, tworzone są jedynie powiązania między istniejącymi danymi, co stanowi pozycję niskonakładową. Ujęte tu koszty prowadzą jedynie do niewielkiego zwiększenia budżetu wymaganego jako dodatku do budżetów EES i ETIAS na konfigurację sieci i ruch sieciowy.

Określić cele i produkty eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[102]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 5[103] Aktualizacja jednolitego interfejsu krajowego																						
Aktualizacja jednolitego interfejsu krajowego	Wykonawca			0		0		0		0,505		0,505								0		1,010
Cel szczegółowy nr 5 — suma cząstkowa				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– We wniosku w sprawie EES wprowadzono pojęcie jednolitego interfejsu krajowego, za którego opracowanie i obsługę techniczną odpowiada eu-LISA. Powyższa tabela przedstawia budżet przeznaczony na aktualizację jednolitego interfejsu krajowego, aby dostosować go do nowego

[102] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).
[103] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

rodzaju wymiany informacji. Nie występują żadne dodatkowe koszty związane z działaniem jednolitego interfejsu krajowego, ponieważ te zostały już ujęte we wniosku w sprawie EES.

Określić cele i produkty eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj [104]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 6: Spotkania i szkolenia																						
Miesięczne spotkania dotyczące postępów (rozwój)	0,021 na spotkanie x 10 rocznie		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Spotkania kwartalne (operacje)	0,021 x 4 rocznie		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Grupy doradcze	0,021 x 4 rocznie		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Szkolenia w państwach członkowskic	0,025 za szkolenie		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150

[104] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

Cel szczegółowy nr 6 — suma cząstkowa	20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

– Suma cząstkowa dla celu nr 6 obejmuje koszty organizacji spotkań przez organ zarządzający (w tym przypadku eu-LISA) na potrzeby zarządzania projektem. Są to koszty dodatkowych spotkań poświęconych dostarczaniu elementów interoperacyjności.

– Suma cząstkowa dla celu nr 6 obejmuje koszty spotkań eu-LISA z personelem z państw członkowskich odpowiedzialnym za opracowywanie, utrzymanie i funkcjonowanie elementów interoperacyjności oraz za organizację i prowadzenie szkoleń dla pracowników informatycznych w państwach członkowskich.

– W fazie rozwojowej budżet obejmuje 10 spotkań projektowych rocznie. Od czasu rozpoczęcia przygotowań do uruchomienia (w tym przypadku od 2019 r.) organizowane będą cztery spotkania rocznie. Od początku ustanowiona zostaje grupa doradcza wyższego szczebla, aby wdrażać decyzje wykonawcze Komisji. Planowane są cztery spotkania rocznie, jak ma to miejsce w przypadku istniejących grup doradczych. Ponadto eu-LISA przygotowuje i przeprowadza szkolenia dla personelu informatycznego z państw członkowskich. Przedmiotem tych szkoleń są aspekty techniczne elementów interoperacyjności.

Określić cele i produkty eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[105]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 7[106] Wysoka dostępność ECRIS-TCN																						
System o wysokiej dostępności	Konfiguracja systemu			0		0		8,067												0		8,067
Operacje o wysokiej dostępności	Obsługa techniczna i funkcjonowanie systemu			0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Cel szczegółowy nr 4 — suma cząstkowa				**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– Cel nr 7 polega na przekształceniu systemu ECRIS-TCN z systemu o „standardowej” dostępności w system o wysokiej dostępności. Usprawnienie ECRIS-TCN, które przede wszystkim będzie wymagało zakupu dodatkowego sprzętu komputerowego, nastąpi w 2021 r. Ponieważ ECRIS-TCN ma zostać ukończony w 2020 r., uzasadnione wydawałoby się zbudowanie tego systemu od początku jako systemu o wysokiej dostępności, zintegrowanego z elementami interoperacyjności. Jednak ponieważ liczne projekty są wzajemnie od siebie uzależnione, ostrożność nakazuje nieprzyjmowanie takiego założenia i sporządzenie budżetu dla odrębnych działań. Budżet ten stanowi budżet dodatkowy w stosunku do kosztów opracowania, obsługi technicznej i funkcjonowania ECRIS-TCN w latach 2019 i 2020.

[105] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).
[106] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

3.2.2.5. Szacunkowy wpływ na środki DG HOME

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty **DG HOME** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**OGÓŁEM**	
	Rodzaj[107]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt ogółem
CEL SZCZEGÓŁOWY NR 1: Integracja systemów krajowych (państw członkowskich)																						
Gotowość do użytkowania jednolitego interfejsu krajowego	Dostosowanie jednolitego interfejsu krajowego — prace rozwojowe						30	3,150	30	3,150											30	6,300

[107] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

Dostosowanie systemów państw członkowskich do interoperacyjności	Koszty integrowania					30	40,000	30	40,000	30	40,000									30	120,000
Szkolenia dla użytkowników końcowych	W sumie 10 000 sesji szkoleniowych dla							5000	5,000	5000	5,000									10 000	10,000
Cel szczegółowy nr 1 — suma cząstkowa							**43 150**		**48 150**		**45 000**										**136 300**

– Cel szczegółowy nr 1 dotyczy środków udostępnianych państwom członkowskim, aby mogły korzystać z interoperacyjnych systemów centralnych. Jednolity interfejs krajowy wymaga dostosowania zarówno w momencie wdrożenia europejskiego portalu wyszukiwania, jak i po uruchomieniu modułu wykrywającego multiplikację tożsamości. Każde państwo członkowskie będzie musiało wówczas wprowadzić stosunkowo niewielką zmianę (ok. 150 osobodni), aby się odpowiednio dostosować do zaktualizowanej wymiany komunikatów z systemami centralnymi. Bardziej istotna jest zmiana w treści danych, która zostanie wprowadzona wraz z interoperacyjnością, ujęta w „kosztach integrowania”. Środki te są przeznaczone na zmiany w rodzaju komunikatów przesyłanych do systemu centralnego i przetwarzanie udzielanych odpowiedzi. Do celów oszacowania kosztów tych zmian, każdemu państwu członkowskiemu przydzielono budżet w wysokości 4 mln EUR. Kwota ta jest taka sama jak w przypadku EES, ponieważ wymagana będzie porównywalna ilość pracy w związku z dostosowaniem integracji systemów krajowych z jednolitym interfejsem krajowym.

– Użytkownicy końcowi będą musieli zostać przeszkoleni z tych systemów. Szkolenia te — przeznaczone dla bardzo licznej grupy użytkowników końcowych — będą finansowane zgodnie z podstawą wynoszącą 1 000 EUR za sesję szkoleniową dla 10–20 użytkowników końcowych, przy ok. 10 000 sesjach, które mają zostać zorganizowane przez wszystkie państwa członkowskie w ich własnych lokalach.

3.2.3. Szacowany wpływ na zasoby ludzkie

3.2.3.1. Streszczenie dla Europejskiej Staży Granicznej i Przybrzeżnej

☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Urzędnicy (grupa zaszeregowania AD)										
Urzędnicy (grupa zaszeregowania AST)	0									
Personel kontraktowy	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Personel zatrudniony na czas określony	0	0	0	0	0	0	0	0	0	0
Oddelegowani eksperci krajowi										
OGÓŁEM	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

Spodziewane prace wykonywane przez tych dodatkowych pracowników Europejskiej Straży Granicznej i Przybrzeżnej są ograniczone czasowo (do 2023 r.), a dokładniej rzecz biorąc, rozpoczynają się 24 miesiące pod dacie udostępnienia wyszukiwarki danych biometrycznych dla EES. Pracowników należy jednak zatrudnić z wyprzedzeniem (zgodnie z obliczeniami ok. trzymiesięcznym), co wyjaśnia wartość podaną dla 2022 r. Po zakończeniu prac należy wykonywać zadania podsumowujące i zakańczające przez okres dwóch miesięcy, co wyjaśnia poziom personelu w 2024 r.

Podstawowy poziom personelu to 20 osób koniecznych do wykonania prac (plus 10 pracowników zapewnionych przez wykonawcę, czemu dano wyraz w tytule 3). Zakłada się także, że zadania te będą wykonywane w wydłużonych godzinach pracy, wykraczających poza zwykły czas pracy. Zakłada się zapewnienie usług pracowników odpowiedzialnych za wsparcie i zarządzanie, korzystając z zasobów Agencji.

Liczebność personelu opiera się na założeniu, że konieczna będzie analiza ok. 550 000 odcisków palców, przy czym obsługa jednego przypadku wynosi średnio 5–10 minut (17 000 odcisków palców sprawdzanych rocznie)[108].

Liczba pracowników	2019	2020	2021	2022	2023	2024	2025	2026	2027	Ogółem
Personel odpowiedzialny za ręczne rozpatrywanie łączy i decyzji	0.0	0.0	0.0	5.0	20.0	3.3	0.0	0.0	0.0	28.3
Ogółem Tytuł 1 — pracownicy kontraktowi	0.0	0.0	0.0	5.0	20.0	3.3	0.0	0.0	0.0	28.3
Ogółem Tytuł 1 — pracownicy zatrudnieni na czas określony	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Ogółem Tytuł 1	0.0	0.0	0.0	5.0	20.0	3.3	0.0	0.0	0.0	28.3

.

3.2.3.2. Streszczenie dla Europolu

☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Urzędnicy (grupa zaszeregowania AD)										
Urzędnicy (grupa zaszeregowania AST)	0									
Personel kontraktowy	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Personel zatrudniony na czas określony	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Oddelegowani eksperci krajowi										
OGÓŁEM	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Koszty oszacowano na podstawie następujących poziomów zatrudnienia:

Liczba EPC	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogóle**

[108] Personel w 2020 r. i w latach kolejnych — dane szacunkowe, które trzeba będzie ocenić w stosunku do prognoz dotyczących personelu Europejskiej Straży Granicznej i Przybrzeżnej przedstawionych w COM(2015) 671 — czy je przekraczają czy nie

w dziedzinie ICT										**m**
Personel kontraktowy	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Personel zatrudniony na czas określony	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Personel ogółem (EPC)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Rozważa się zatrudnienie przez Europol dodatkowych pracowników w dziedzinie ICT, aby wzmocnić systemy informacyjne Europolu i przez to umożliwić obsługę zwiększonej liczby zapytań pochodzących z europejskiego portalu wyszukiwania i ETIAS, a następnie utrzymywać całodobową pracę systemów.

– W fazie wdrażania europejskiego portalu wyszukiwania (w latach 2020 i 2021) konieczni będą dodatkowi eksperci techniczni (architekci, inżynierowie, twórcy oprogramowania, testerzy). Mniejsza liczba ekspertów technicznych będzie wymagana od 2022 r., aby wdrażać pozostałe elementy interoperacyjności i utrzymywać pracę systemów.

– Od drugiej połowy 2021 r. konieczne będzie wprowadzenie całodobowego monitorowania systemów informacyjno-komunikacyjnych, aby zapewnić gwarantowany poziom usług dla europejskiego portalu wyszukiwania i ETIAS. Za zadanie to będą odpowiadać 2 pracownicy kontraktowi pracujący na 4 zmianach 24 godziny na dobę.

– W miarę możliwości profile zostały podzielone między pracowników zatrudnionych na czas określony i pracowników kontraktowych. Należy jednak zauważyć, że ze względu na wysokie wymagania dotyczące bezpieczeństwa na kilku stanowiskach możliwe jest zatrudnienie wyłącznie pracowników kontraktowych. Wniosek o zatrudnienie pracowników na czas określony będzie uwzględniał wyniki postępowania pojednawczego w związku z procedurą budżetową na 2018 r.

3.2.3.3. Streszczenie dla CEPOL-u

☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Urzędnicy (grupa zaszeregowania AD)										

Urzędnicy (grupa zaszeregowania AST)										
Personel kontraktowy			0,070	0,070						**0,140**
Personel zatrudniony na czas określony		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Oddelegowani eksperci krajowi										

OGÓŁEM		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Konieczny jest dodatkowy personel, ponieważ szkolenia dla instruktorów z państw członkowskich muszą zostać opracowane specjalnie z myślą o użytkowaniu elementów interoperacyjności w sytuacjach operacyjnych.

- Opracowywanie programu i modułów szkoleniowych powinno rozpocząć się co najmniej na 8 miesięcy przed uruchomieniem systemu. Szkolenia odbywają się najintensywniej w ciągu pierwszych dwóch lat po uruchomieniu. Muszą być jednak utrzymywane przez dłuższy okres, aby zapewnić spójne wdrożenie, jak wynika z doświadczeń z Systemem Informacyjnym Schengen.

- Dodatkowi pracownicy będą mieć za zadanie przygotowanie, koordynację i realizację programu szkoleń, kursów stacjonarnych i internetowych. Kursy te można przeprowadzać jedynie w dodatku do istniejącego katalogu szkoleniowego CEPOL-u, potrzebni są zatem dodatkowi pracownicy.

- Planowane jest powołanie jednego kierownika szkoleń jako pracownika zatrudnionego na czas określony w fazie rozwojowej i w fazie utrzymania, którego w najintensywniejszym okresie organizacji szkoleń wspierałby pracownik kontraktowy.

3.2.3.4. Streszczenie dla eu-LISA

☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
Urzędnicy (grupa zaszeregowania AD)										

Urzędnicy (grupa zaszeregowania AST)										
Personel kontraktowy	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Personel zatrudniony na czas określony	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Oddelegowani eksperci krajowi										

OGÓŁEM	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

- Wymagania co do liczby pracowników uwzględniają to, że cztery elementy i centralne repozytorium sprawozdawczo-statystyczne stanowią portfolio wzajemnie uzależnionych od siebie projektów (tj. program). Aby zarządzać współzależnościami między projektami, utworzony zostanie zespół ds. zarządzania projektami, w którego skład wejdą kierownicy programu i projektów oraz pracownicy o profilach odpowiedzialnych za określenie elementów wspólnych między nimi (zwani często architektami). Realizacja programu/projektów wymaga też profili związanych ze wsparciem programu i projektów.
- Wymogi dotyczące personelu dla każdego projektu wstępnie określono w sposób analogiczny do wcześniejszych projektów (wizowy system informacyjny), z rozróżnieniem na fazę ukończenia projektu i fazę operacyjną.
- Pracownicy, których profile muszą pozostać aktualne w trakcie fazy operacyjnej, zostaną zatrudnieni na czas określony. Pracownicy o profilach wymaganych w trakcie realizacji programu/projektów zostaną zatrudnieni jako pracownicy kontraktowi. Aby zapewnić spodziewaną ciągłość zadań i utrzymać wiedzę w ramach Agencji, stanowiska zostały niemal równo podzielone między pracowników zatrudnionych na czas określony a pracowników kontraktowych.
- Przyjmuje się założenie, że do realizacji projektu związanego z zapewnieniem wysokiej dostępności systemu ECRIS-TCN nie będą konieczni dodatkowi pracownicy oraz że personel eu-LISA będą stanowić dotychczasowi pracownicy zatrudnieni wcześniej przy projektach, które do tego czasu zostaną ukończone.

Szacunki opierają się na następujących poziomach zatrudnienia:

Dla personelu kontraktowego:

3.2.1. produkty EU-LISA (tak samo jak w T1) pod kątem liczby osób	2019	2020	2021	2022	2023	2024	2025	2026	2027	Ogółem (wzór)
Personel kontraktowy										-
Zarządzanie programem/projektami	4.0	5.0	5.5	5.5	4.5	3.0	3.0	3.0	3.0	36.5
Zarządzanie projektem CRRS	*1.0*	*0.5*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*1.5*
Moduł wykrywający multiplikację tożsamości	*0.0*	*0.5*	*0.5*	*0.5*	*0.5*	*0.0*	*0.0*	*0.0*	*0.0*	*2.0*
Biuro programów/projektów	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*1.0*	*1.0*	*1.0*	*1.0*	*14.0*
Zapewnienie jakości	*1.0*	*2.0*	*3.0*	*3.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*19.0*
Finanse i zamówienia	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Zarządzanie finansowe										*0.0*
Planowanie budżetowe i kontrola										*0.0*
Zarządzanie zamówieniami/umowami	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Eksperci techniczni	7.0	7.0	7.0	7.0	6.0	5.0	5.0	5.0	5.0	54.0
Centralne repozytorium sprawozdawczo-statystyczne	*3.0*	*3.0*	*3.0*	*3.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*22.0*
Europejski portal wyszukiwania	*4.0*	*4.0*	*4.0*	*4.0*	*4.0*	*3.0*	*3.0*	*3.0*	*3.0*	*32.0*
Wspólny serwis kojarzenia danych biometrycznych	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Wspólne repozytorium tożsamości	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Wspólne repozytorium tożsamości	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Testowanie	1.5	3.0	4.0	4.0	4.0	3.0	2.0	2.0	2.0	25.5
Centralne repozytorium sprawozdawczo-statystyczne	*1.0*	*1.0*	*1.0*	*0.5*	*0.5*	*0.5*	*0.5*	*0.5*	*0.5*	*6.0*
Europejski portal wyszukiwania	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Wspólny serwis kojarzenia danych biometrycznych	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Wspólne repozytorium tożsamości	*0.5*	*1.0*	*2.0*	*2.5*	*2.5*	*1.5*	*1.0*	*1.0*	*1.0*	*13.0*
Moduł wykrywający multiplikację tożsamości	*0.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*0.5*	*0.5*	*0.5*	*6.5*
Monitorowanie systemów	0.0	5.0	10.0	20.0	20.0	20.0	20.0	20.0	20.0	135.0
Wspólne (całodobowo)	0.0	*5.0*	*10.0*	*20.0*	*20.0*	*20.0*	*20.0*	*20.0*	*20.0*	*135.0*
Koordynacja ogólna	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Zasoby ludzkie	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
HR	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	*0.0*
Suma cząstkowa dla personelu kontraktowego	**12.5**	**20.0**	**26.5**	**36.5**	**34.5**	**31.0**	**30.0**	**30.0**	**30.0**	**251.0**

Dla pracowników zatrudnionych na czas określony:

Personel zatrudniony na czas określony										
Zarządzanie programem/projektami	3.0	4.0	5.5	5.5	5.5	4.5	4.0	4.0	4.0	40.0
Programme mgr	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*9.0*
Project mgt	*0.0*	*0.0*	*1.0*	*1.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*12.0*
Programme/project office	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*9.0*
ESP	*0.5*	*1.0*	*1.0*	*0.5*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*3.0*
Shared BMS	*0.5*	*0.5*	*0.5*	*1.0*	*1.0*	*0.5*	*0.0*	*0.0*	*0.0*	*4.0*
CIR	*0.0*	*0.5*	*1.0*	*1.0*	*0.5*	*0.0*	*0.0*	*0.0*	*0.0*	*3.0*
MID	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Finanse i zamówienia	3.0	3.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	34.0
Financial mgt	*0.0*	*0.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*7.0*
Budgetary planning and control	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*9.0*
Procurement/contract mgt	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*18.0*
Eksperci techniczni	6.0	14.0	17.0	17.0	15.0	11.0	10.0	10.0	10.0	110.0
CRRS	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
ESP	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Shared BMS	*2.0*	*3.0*	*5.0*	*5.0*	*5.0*	*3.0*	*3.0*	*3.0*	*3.0*	*32.0*
CIR	*2.0*	*5.0*	*5.0*	*5.0*	*3.0*	*3.0*	*3.0*	*3.0*	*3.0*	*32.0*
Security	*1.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*2.0*	*17.0*
MID	*0.0*	*2.0*	*2.0*	*2.0*	*2.0*	*1.0*	*1.0*	*1.0*	*1.0*	*12.0*
Architects	*1.0*	*2.0*	*3.0*	*3.0*	*3.0*	*2.0*	*1.0*	*1.0*	*1.0*	*17.0*
Testowanie	2.5	3.0	4.0	4.0	4.0	2.5	2.0	2.0	2.0	26.0
CRRS	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
ESP	*0.5*	*1.0*	*1.0*	*1.0*	*1.0*	*0.5*	*0.5*	*0.5*	*0.5*	*6.5*
Shared BMS	*2.0*	*2.0*	*3.0*	*3.0*	*3.0*	*2.0*	*1.5*	*1.5*	*1.5*	*19.5*
CIR	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
MID	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Monitorowanie systemów	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
CRRS	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
ESP	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Shared BMS	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
CIR	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
MID	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Szkolenia	0.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	8.0
Training	*0.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*1.0*	*8.0*
Zasoby ludzkie	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
HR	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	*0.0*
Inne	0.0	0.0	0.0	0.0	1.0	1.0	1.0	1.0	1.0	5.0
Data protection specialist	0.0	0.0	0.0	0.0	1.0	1.0	1.0	1.0	1.0	*5.0*
Suma cząstkowa dla personelu zatrudnionego na czas określony	**14.5**	**25.0**	**31.5**	**31.5**	**30.5**	**24.0**	**22.0**	**22.0**	**22.0**	**223.0**
Ogółem	**27.0**	**45.0**	**58.0**	**68.0**	**65.0**	**55.0**	**52.0**	**52.0**	**52.0**	**474.0**

3.2.4. Szacunkowy wpływ na środki administracyjne

3.2.4.1. DG HOME: Streszczenie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
DZIAŁ 5 wieloletnich ram finansowych										
Zasoby ludzkie DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Pozostałe wydatki administracyjne	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
DZIAŁ 5 — suma cząstkowa wieloletnich ram finansowych	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Poza DZIAŁEM 5[109] wieloletnich ram finansowych	(nieuży wane)									
Zasoby ludzkie										
Inne wydatki administracyjne										
Suma cząstkowa Poza DZIAŁEM 5 wieloletnich ram finansowych										

OGÓŁEM	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

[109] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

3.2.4.2. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i personelu zatrudnionego na czas określony)										
18 01 01 01 (w centrali i w biurach przedstawicielstw Komisji) DG HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (w delegaturach)										
XX 01 05 01 (pośrednie badania naukowe)										
10 01 05 01 (bezpośrednie badania naukowe)										
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)[110]										
XX 01 02 02 (CA, LA, SNE, INT i JED w delegaturach)										
XX 01 04 **yy** 111 - w centrali										
XX 01 04 **yy** 111 - w delegaturach										
XX 01 05 02 (AC, END, INT — pośrednie badania naukowe)										
10 01 05 02 (CA, SNE, INT — bezpośrednie badania naukowe)										
Inne linie budżetowe (określić)										
OGÓŁEM	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 oznacza odpowiednią dziedzinę polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Kontrole i monitorowanie projektów. Trzej urzędnicy odpowiedzialni za monitorowanie. Pracownicy zajmują się realizacją obowiązków Komisji związanych z realizacją programu: sprawdzają zgodność z wnioskiem ustawodawczym, rozwiązują problemy związane z niezgodnością z przepisami, przygotowują sprawozdania dla Parlamentu Europejskiego i Rady oraz oceniają postępy państwa członkowskiego. Ponieważ program stanowi dodatkowe działanie w stosunku do istniejącego obciążenia pracą, konieczne będzie zatrudnienie nowych pracowników. To zwiększenie liczebności personelu jest ograniczone czasowo i obejmuje tylko fazę rozwojową.

Zarządzanie uniwersalnym formatem wiadomości (UMF)

[110] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JED = młodszy oddelegowany ekspert.

[111] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA”).

Komisja będzie na bieżąco zarządzać standardem UMF. W tym celu koniecznych jest dwóch urzędników: jedna osoba będąca ekspertem w zakresie ścigania przestępstw i druga o solidnej wiedzy na temat modelowania biznesowego i ICT.

Uniwersalny format wiadomości (UMF) ustanawia standard dla uporządkowanej, transgranicznej wymiany informacji między systemami informacyjnymi, organami lub organizacjami działającymi w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych. UMF określa wspólny język i struktury logiczne wzajemnie wymienianych informacji, aby ułatwić interoperacyjność poprzez umożliwienie tworzenia i odczytywania treści wymiany w sposób spójny i semantycznie równoważny.

W celu zapewnienia jednolitych warunków wdrażania uniwersalnego formatu wiadomości proponuje się powierzenie Komisji uprawnień wykonawczych. Zgodnie z wnioskiem uprawnienia te byłyby wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję.

3.2.5. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

– ☐ Wniosek/inicjatywa jest zgodny(-a) z obowiązującymi wieloletnimi ramami finansowymi.

– ☒ Wniosek/inicjatywa wymaga przeprogramowania odpowiedniego działu w wieloletnich ramach finansowych.

Należy wyjaśnić, na czym ma polegać przeprogramowanie, określając linie budżetowe, których ma ono dotyczyć, oraz podając odpowiednie kwoty.

Instrumentem finansowym, w którym ujęto budżet przeznaczony na realizację inicjatywy dotyczącej interoperacyjności, jest rozporządzenie w sprawie Funduszu Bezpieczeństwa Wewnętrznego i wsparcia w zakresie granic.

Jego art. 5 lit. b) stanowi, że kwota 791 mln EUR ma zostać przeznaczona na program, którego celem jest opracowanie systemów informatycznych, na podstawie istniejących lub nowych systemów informatycznych, wspierających zarządzanie przepływami migracyjnymi przez granice zewnętrzne, z zastrzeżeniem przyjęcia odpowiednich aktów ustawodawczych Unii i na warunkach określonych w art. 15. Z tej kwoty wynoszącej 791 mln EUR kwota 480,2 mln EUR jest zarezerwowana na opracowanie systemu EES, 210 mln EUR — na system ETIAS, a 67,9 mln EUR — na przegląd SIS II. Pozostała kwota (32,9 mln EUR) będzie poddana realokacji za pomocą mechanizmów Funduszu Bezpieczeństwa Wewnętrznego ds. Granic i Wiz. **Niniejszy wniosek wymaga kwoty 32,1 mln EUR w obecnym okresie WRF, mieści się zatem w granicach dostępnego budżetu**.

Podsumowanie zawarte w polu powyżej dotyczące wymaganej kwoty w wysokości 32,1 mln EUR wynika z zastosowania następującego arkusza obliczeń:

ZOBOWIĄZANIA										
3.2. Szacunkowy wpływ na wydatkiDG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem (poziomo)**
18 02 01 03 — Inteligentne granice (obejmuje wsparcie dla państw członkowskich)	0	0	43.150	48.150	45.000	0	0	0	0	136.300
Ogółem (1)	**0**	**0**	**43.150**	**48.150**	**45.000**	**0**	**0**	**0**	**0**	**136.300**
18.0207-3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem (wzór)**
T1: Wydatki na personel	2.876	4.850	6.202	6.902	6.624	5.482	5.136	5.136	5.136	48.344
T2: Wydatki na infrastrukturę i wydatki operacyjne	0.136	0.227	0.292	0.343	0.328	0.277	0.262	0.262	0.262	2.389
T3: Wydatki operacyjne	2.818	11.954	45.249	37.504	22.701	14.611	13.211	13.131	13.131	174.309
Ogółem (2)	**5.830**	**17.031**	**51.743**	**44.749**	**29.653**	**20.370**	**18.609**	**18.529**	**18.529**	**225.041**
		22.861							**202.181**	**225.041**
18.02.04-3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem (wzór)**
T1: Wydatki na personel	0.690	2.002	2.002	1.181	1.181	0.974	0.974	0.974	0.974	10.952
T2: Wydatki na infrastrukturę i wydatki operacyjne	0	0	0	0	0	0	0	0	0	0
T3: Wydatki operacyjne	0	6.380	6.380	2.408	2.408	2.408	7.758	7.758	2.408	37.908
Ogółem (3)	**0.690**	**8.382**	**8.382**	**3.589**	**3.589**	**3.382**	**8.732**	**8.732**	**3.382**	**48.860**
		9.072							39.788	48.860
18.02.05-3.2. Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL)										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem (wzór)**
T1: Wydatki na personel	0	0.104	0.208	0.208	0.138	0.138	0.138	0.138	0.138	1.210
T2: Wydatki na infrastrukturę i wydatki operacyjne	0	0	0	0	0	0	0	0	0	0
T3: Wydatki operacyjne	0	0.040	0.176	0.274	0.070	0.070	0.070	0.070	0.070	0.840
Ogółem (4)	**0**	**0.144**	**0.384**	**0.482**	**0.208**	**0.208**	**0.208**	**0.208**	**0.208**	**2.050**
		0.144							**1.906**	**2.050**
18.02.0-3.2. Frontex — Europejska Straż Graniczna i Przybrzeżna										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem (wzór)**
T1: Wydatki na personel	0	0	0	0.350	1.400	0.233	0	0	0	1.983
T2: Wydatki na infrastrukturę i wydatki operacyjne	0	0	0	0.075	0.300	0.050	0	0	0	0.425
T3: Wydatki operacyjne	0	0	0	0.183	2.200	0	0	0	0	2.383
Ogółem (5)	**0**	**0**	**0**	**0.608**	**3.900**	**0.283**	**0**	**0**	**0**	**4.792**
		0							**4.792**	**4.792**
Ogółem (1)+(2)+(3) +(4) +(5)	6.520	25.556	103.659	97.578	82.350	24.243	27.549	27.469	22.119	417.043
		32.076							384.966	
3.2. Dział 5 DG HOME „Wydatki administracyjne"										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem**
Ogółem (6)	1.013	1.013	1.013	1.013	1.013	1.013	0.539	0.539	0.539	7.695
OGÓŁEM (1)+(2)+(3)+(4)+(5)+(6)	7.533	26.569	104.672	98.591	83.363	25.256	28.088	28.008	22.658	424.738

– ☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych.

3.2.6. *Udział osób trzecich w finansowaniu*

– Wniosek/inicjatywa **nie** przewiduje współfinansowania ze strony osób trzecich.

3.3. Szacunkowy wpływ na dochody

– ☐ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☒ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

  – ☐ wpływ na zasoby własne

  – ☒ wpływ na dochody różne

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[112]								
		Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**
Artykuł 6313 - Wkład państw stowarzyszonych w ramach Schengen (CH, NO, LI, IS)…… …….		pm	pm	pm	pm	pm	pm	pm	pm	pm

W przypadku wpływu na dochody różne „przeznaczone na określony cel” należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

18.0207

Należy określić metodę obliczania wpływu na dochody.

Budżet zawiera wkład państw uczestniczących we wdrażaniu, stosowaniu i rozwijaniu dorobku Schengen oraz środków dotyczących systemu Eurodac zgodnie z ustaleniami zawartymi w odnośnych umowach.

[112] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 25 % na poczet kosztów poboru.