



Ministerstwo Spraw
Wewnętrznych i Administracji

Plan Dostosowania Organów Polskiej Administracji do Współpracy z Wielkoskalowymi Systemami Informacyjnymi UE *MasterPlan 2.0*

Warszawa, listopad 2024 r.

1 Metryka dokumentu

Tytuł:	Plan Dostosowania Organów Polskiej Administracji do Współpracy z Wielkoskalowymi Systemami Informacyjnymi UE – MasterPlan 2.0
Wersja:	2.0
Status:	Projekt przyjęty Uchwałą nr 23 Zespołu ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE oraz zatwierdzony przez Pełnomocnika Rządu do Spraw Wielkoskalowych Systemów Informacyjnych Unii Europejskiej.
Liczba stron:	78
Liczba załączników:	1
Opracowanie	Departament Teleinformatyki Ministerstwo Spraw Wewnętrznych i Administracji

Zatwierdzenie projektu dokumentu:

Data	Imię i Nazwisko	Stanowisko
21.11.2024 r.	Dariusz Nowak-Nova	Pełnomocnik Ministra Spraw Wewnętrznych i Administracji do Spraw Informatyzacji, Dyrektor Departamentu Teleinformatyki MSWiA

Przyjęcie projektu dokumentu:

Data	Organ
22.11.2024 r.	Rada Programu Zespołu ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE

Zatwierdzenie projektu dokumentu:

Data	Imię i Nazwisko	Stanowisko
26.11.2024 r.	Tomasz Szymański	Pełnomocnik Rządu do Spraw Wielkoskalowych Systemów Informacyjnych Unii Europejskiej, Sekretarz Stanu MSWiA

Przyjęcie dokumentu:

Data	Organ
	Komitet Rady Ministrów do spraw Cyfryzacji
	Komitet do spraw Europejskich
	Stały Komitet Rady Ministrów
	Rada Ministrów

Spis treści

1	Metryka dokumentu	2
2	Wykaz używanych skrótów.....	6
3	Powiązane dokumenty	9
3.1	Prawo Unii Europejskiej:	9
3.2	Prawo krajowe	9
4	Wielkoskalowe Systemy Informacyjne UE.....	11
4.1	System Informacyjny Schengen (SIS).....	11
4.2	Wizowy System Informacyjny (VIS).....	12
4.3	System Eurodac	12
4.4	System wjazdu/wyjazdu (EES)	13
4.5	Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)	14
4.6	Europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN)	15
4.7	Interoperacyjność Wielkoskalowych Systemów Informacyjnych UE (IO)	15
4.8	Infrastruktura transportowa (TESTA-ng).....	21
5	Współpraca polskich instytucji z Wielkoskalowymi Systemami Informacyjnymi UE.....	22
5.1	Ramy prawne.....	22
5.2	Ochrona danych osobowych	22
5.3	Cyberbezpieczeństwo	23
5.4	Ramy organizacyjne	25
5.4.1	Zarządzanie Programem	25
5.4.2	Interesariusze.....	27
5.4.3	Centralny Organ Techniczny KSI – Komendant Główny Policji.....	28
5.4.4	Centralny Organ Techniczny IO/EES/ETIAS – Komendant Główny Straży Granicznej	28
5.4.5	Biuro SIRENE	29
5.4.6	Krajowy Punkt Dostępu do systemu Eurodac – Komendant Główny Policji	30
5.4.7	Krajowa Jednostka ds. EES – Komendant Główny Straży Granicznej	30
5.4.8	Jednostka Krajowa ETIAS – Komendant Główny Straży Granicznej	31
5.4.9	Organ centralny ECRIS-TCN – Biuro Informacyjne Krajowego Rejestru Karnego w Ministerstwie Sprawiedliwości	31
6	Koncepcja dostosowania polskiej administracji do zmian.....	33
6.1	Cele przedsięwzięcia.....	33

6.2	Potwierdzenie osiągnięcia celów	33
6.3	Projekty do realizacji.....	35
6.4	Zakres zmian prawnych.....	35
7	Szczegółowy opis projektów.....	36
7.1	PROJEKT 1: Modernizacja systemu SIS II (SIS Recast)	36
7.2	PROJEKT 2: Modernizacja systemu VIS (VIS Revised)	37
7.3	PROJEKT 3: Modernizacja systemu Eurodac (Eurodac Recast).....	41
7.4	PROJEKT 4: Wdrożenie systemu EES.....	45
7.5	PROJEKT 5: Wdrożenie systemu ETIAS.....	50
7.6	PROJEKT 6: Wdrożenie systemu ECRIS-TCN.....	56
7.7	PROJEKT 7: Wdrożenie narzędzi Interoperacyjności Systemów (IO)	61
7.8	PROJEKT 8: Dostosowanie przepisów prawnych systemu EES.....	65
7.9	PROJEKT 9: Dostosowanie przepisów prawnych systemu ETIAS.....	67
7.10	PROJEKT 10: Dostosowanie przepisów prawnych systemu VIS	71
7.11	PROJEKT 11: Dostosowanie przepisów prawnych systemu Eurodac	73
7.12	PROJEKT 12: Modernizacja infrastruktury TESTA-ng.....	74
8	Plan realizacji	76
8.1	Harmonogram realizacji	76
8.2	Prognoza finansowa.....	77
8.3	Główne ryzyka	77

2 Wykaz używanych skrótów

Akronim	Rozwinięcie
ABW	Agencja Bezpieczeństwa Wewnętrznego
API	Advance Passenger Information (Wyprzedzające Informacje o Pasażerze)
AFIS	Automated Fingerprint Identification System (Automatyczny System Identyfikacji Daktyloskopijnej)
AW	Agencja Wywiadu
BI KRK	Biuro Informacyjne Krajowego Rejestru Karnego
CBA	Centralne Biuro Antykorupcyjne
CIR	Common Identity Repository (Wspólne Repozytorium Danych Umożliwiających Identyfikację)
CLKP	Centralne Laboratorium Kryminalistyczne Policji
COT KSI	Centralny Organ Techniczny Krajowego Systemu Informatycznego
COT IO/EES/ETIAS	Centralny Organ Techniczny Interoperacyjności/EES/ETIAS
CEPOL	Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania
COW	Centralny Organ Wizowy
CRRS	Central Repository for Reporting and Statistics (Centralne Repozytorium Sprawozdawczo-Statystyczne)
EES	Entry/Exit System (System wjazdu/wyjazdu)
ECRIS-TCN	European Criminal Records Information System – Third Country Nationals (Europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich)
ESP	European Search Portal (Europejski Portal Wyszukiwania)
ETIAS	European Travel Information and Authorisation System (Europejski system informacji o podróży oraz zezwoleń na podróż)
ETIAS NU	European Travel Information and Authorisation System National Unit (Krajowa Jednostka w Europejskim Systemie Informacji o Podróży oraz Zezwoleń na Podróż)
Eurodac	European Asylum Dactyloscopy Database (Europejski Zautomatyzowany System Rozpoznawania Odcisków Palców)
EUROPOL	European Union Agency for Law Enforcement Cooperation (Agencja Unii Europejskiej ds. Współpracy Organów Ścigania)
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems (Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi)
FRONTEX	European Border and Coast Guard Agency (Europejska Agencja Straży Granicznej i Przybrzeżnej)
ICD	Interface Control Document (Specyfikacja techniczna)
JKE	Jednostka Krajowa Europolu
KAS	Krajowa Administracja Skarbowa
KE	Komisja Europejska
KIG EES	Krajowa Infrastruktura Graniczna EES

Akronim	Rozwinięcie
KGP	Komenda Główna Policji
KGSG	Komenda Główna Straży Granicznej
KPD Eurodac	Krajowy Punkt Dostępu Eurodac
KSK	Krajowy System Konsultacyjny
KSI	Krajowy System Informatyczny
KSI EES/ETIAS	Krajowy System Informatyczny EES i ETIAS
KSIP	Krajowy System Informacyjny Policji
MF	Ministerstwo Finansów
MID	Multiple-Identity Detector (Detektor Wielokrotnych Tożsamości)
MS	Ministerstwo Sprawiedliwości
MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji
MSZ	Ministerstwo Spraw Zagranicznych
PCz	Państwa/o członkowskie
PNR	Passenger Name Record (Dane o Przelocie Pasażera)
Rada JHA	Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych
RDO-SRP	Rejestr Dowodów Osobistych/System Rejestrów Państwowych
SIS	Schengen Information System (System Informacyjny Schengen)
SIS II	Schengen Information System II (System Informacyjny Schengen drugiej generacji)
SKW	Służba Kontrwywiadu Wojskowego
SPP	System Poszukiwawczy Policji
sBMS	Shared Biometric Matching Service (Wspólny System Porównywania Danych Biometrycznych)
SIENA	Secure Information Exchange Network Application (Aplikacja Sieci Bezpiecznej Wymiany Informacji)
SLTD	Stolen and Lost Travel Documents (Baza Skradzionych i Utraconych Dokumentów Podróży)
STBS	System Teleinformatyczny Biura SIRENE
ST KRK	System Teleinformatyczny Krajowego Rejestru Karnego
SUD	System Udostępniania Danych
TESTA-ng	Trans-European Services for Telematics between Administrations – new generation
TDawn	Travel Documents Associated with Notices database (Baza Danych Dokumentów Podróży Powiązanych z Notami)
UDSC	Urząd ds. Cudzoziemców
UE	Unia Europejska
UI	Użytkownik Instytucjonalny
UIn	Użytkownik Indywidualny
UMF	Universal Message Format (Uniwersalny Format Wiadomości)
WE	Wspólnota Europejska

Akronim	Rozwinięcie
WSiSW	Wymiar Sprawiedliwości i Spraw Wewnętrznych
WSIUE	Wielkoskalowe Systemy Informacyjne Unii Europejskiej
VIS	Visa Information System (Wizowy System Informacyjny)
ZSE6	System teleinformatyczny SG

3 Powiązane dokumenty

3.1 Prawo Unii Europejskiej:

System Informacyjny Schengen (SIS)

- Rozporządzenie (WE) nr 1986/2006 (Dz. Urz. UE L 381 z 28.12.2006 r., s. 1–3, z późn. zm.);
- Rozporządzenie (WE) nr 1987/2006 (Dz. Urz. UE L 381 z 28.12.2006, s. 4, z późn. zm.);
- Decyzja Rady 2007/533/WSiSW (Dz. Urz. UE L 205 z 07.08.2007, s. 63–84, z późn. zm.);
- Rozporządzenie (UE) 2018/1860 (Dz. Urz. UE L 312 z 07.12.2018, s. 1, z późn. zm.);
- Rozporządzenie (UE) 2018/1861 (Dz. Urz. UE L 312 z 07.12.2018, s. 14, z późn. zm.);
- Rozporządzenie (UE) 2018/1862 (Dz. Urz. UE L 312 z 07.12.2018, s. 56, z późn. zm.).

Wizowy System Informacyjny (VIS)

- Decyzja Rady 2004/512/WE (Dz. Urz. UE L 213 z 15.06.2004, s. 5–7, z późn. zm.);
- Decyzja Rady 2008/633/WSiSW (Dz. Urz. UE L 218 z 13.08.2008, s. 129, z późn. zm.);
- Rozporządzenie (WE) 767/2008 (Dz. Urz. UE L 218 z 13.08.2008, s. 60, z późn. zm.);
- Rozporządzenie (UE) 2021/1133 (Dz. Urz. UE L 248 z 13.07.2021, s. 1, z późn. zm.);
- Rozporządzenie (UE) 2021/1134 (Dz. Urz. UE L 248 z 13.07.2021, s. 11, z późn. zm.).

System Eurodac

- Rozporządzenie (UE) 603/2013 (Dz. Urz. UE L 180 z 29.06.2013, s. 1–30, z późn. zm.);
- Rozporządzenie (UE) 604/2013 (Dz. Urz. UE L 180 z 29.06.2013, s. 31–59, z późn. zm.);
- Rozporządzenie (UE) 2024/1358 (Dz. Urz. UE L 1358 z 22.05.2024).

System wjazdu/wyjazdu (EES)

- Rozporządzenie (UE) 2017/2225 (Dz. Urz. UE L 327 z 09.12.2017, s. 1–19, z późn. zm.);
- Rozporządzenie (UE) 2017/2226 (Dz. Urz. UE L 327 z 09.12.2017, s. 20, z późn. zm.).

Europejski system informacji o podróżach oraz zezwoleń na podróż (ETIAS)

- Rozporządzenie (UE) 2018/1240 (Dz. Urz. UE L 236 z 19.09.2018, s. 1, z późn. zm.).

Europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN)

- Rozporządzenie (UE) 2019/816 (Dz. Urz. UE L 135 z 22.05.2019, s. 1, z późn. zm.);
- Dyrektywa (UE) 2019/884 (Dz. Urz. UE L 151 z 07.06.2019, s. 143, z późn. zm.).

Interoperacyjność (IO)

- Rozporządzenie (UE) 2019/817 (Dz. Urz. UE L 135 z 22.05.2019, s. 27, z późn. zm.);
- Rozporządzenie (UE) 2019/818 (Dz. Urz. UE L 135 z 22.05.2019, s. 85, z późn. zm.).

3.2 Prawo krajowe

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2023 r. poz. 171, z późn. zm.), zwana w dokumencie ustawą o Policji;

Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, (Dz. U. z 2021 r. poz. 1041, z późn. zm.), zwana w dokumencie ustawą o SIS i VIS;

Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz. U. z 2024 r. poz. 769);

Ustawa z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2023 r. poz. 1504 z późn. zm.);

Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2024 r. poz. 276), zwana w dokumencie ustawą o KRK;

Rozporządzenie Rady Ministrów z dnia 10 listopada 2020 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw Wielkoskalowych Systemów Informacyjnych Unii Europejskiej (Dz. U. z 2020 r. poz. 2049);

Zarządzenie nr 2 Prezesa Rady Ministrów z dnia 13 stycznia 2021 r. w sprawie Zespołu do spraw Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi Unii Europejskiej (M.P. poz. 46 oraz z 2023 r. poz. 1274), zwane w dokumencie zarządzeniem ws. Zespołu;

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703), zwana w dokumencie UKSC.

4 Wielkoskalowe Systemy Informacyjne UE

4.1 System Informacyjny Schengen (SIS)

28 listopada 2018 r., przyjęto pakiet reform SIS II zwany *SIS Recast* (*rozporządzenie 2018/1860, rozporządzenie 2018/1861, rozporządzenie 2018/1862*). Wprowadziły one bardzo istotne zmiany w funkcjonowaniu SIS. W szczególności wprowadziły nowe kategorie wpisów:

- wpisy na potrzeby rozpytania kontrolnego, pozwalające na zebranie od danej osoby dodatkowych informacji, wprowadzonych przez państwo poszukujące;
- wpisy o nieznanach osobach podejrzanych lub poszukiwanych, czyli wprowadzanie do SIS odbitek linii papilarnych palców lub odbitek linii papilarnych dłoni znalezionych na miejscu poważnego przestępstwa lub incydentu terrorystycznego i uznanych za należące do sprawy;
- wpisy prewencyjne dotyczące dzieci zagrożonych uprowadzeniem przez rodzica, członka rodziny lub opiekuna, którym należy uniemożliwić podróżowanie;
- wpisy prewencyjne dotyczące dzieci, którym należy uniemożliwić podróżowanie ze względu na konkretne i realne zagrożenie, że zostaną wywiezione z terytorium państwa członkowskiego lub opuszczą to terytorium oraz że staną się ofiarami handlu ludźmi lub ofiarami przymusowego małżeństwa, okaleczenia żeńskich narządów płciowych lub innych form przemocy warunkowanej płcią; lub staną się ofiarami przestępstw terrorystycznych lub wezmą udział w popełnianiu takich przestępstw; lub zostaną zwerbowane lub zaciągnięte do ugrupowań zbrojnych lub zmuszone do aktywnego udziału w działaniach wojennych;
- osoby narażone na niebezpieczeństwo, które są pełnoletnie i którym dla ich własnej ochrony należy uniemożliwić podróżowanie, ze względu na konkretne i realne zagrożenie, że zostaną wywiezione z terytorium państwa członkowskiego lub opuszczą to terytorium i że staną się ofiarami handlu ludźmi lub przemocy warunkowanej płcią;
- wpisy do celów powrotu, czyli odnotowywanie decyzji nakazującej powrót obywatelom państw trzecich, którzy nielegalnie przebywają w UE;
- obowiązkowe jest niezwłoczne zamieszczanie w SIS wpisów dotyczących odmowy wjazdu i pobytu dla obywateli państw trzecich;
- liczne, nowe kategorie przedmiotów, których dotyczyć mogą wpisy, m.in. pojazdy – niezależnie od układu napędowego (w tym np. rowery), części samochodowe i części urządzeń przemysłowych, sprzęt informatyczny, fałszywe dokumenty i blankiety oraz możliwe do zidentyfikowania przedmioty o dużej wartości.

Przepisy UE wprowadziły również zasadę, że jeżeli kontrole szczególne nie są dopuszczalne w świetle prawa krajowego państwa wykonującego, są one zastępowane w danym państwie członkowskim rozpytaniami kontrolnymi. Jeżeli rozpytania kontrolne nie są dopuszczalne w świetle prawa krajowego państwa wykonującego, są one zastępowane w danym państwie członkowskim kontrolami niejawnymi.

Ponadto 28 grudnia 2020 r. zmieniły się przepisy dotyczące centralnego AFIS (Automatyczny System Identyfikacji Daktyloskopijnej) w SIS II nakładające jednocześnie na państwa członkowskie obowiązek dostosowania się do nowych przepisów szczegółowych dotyczących wprowadzania wpisów, weryfikacji lub wyszukiwania przy użyciu fotografii i odbitek linii papilarnych palców. Dodatkowo *rozporządzenie 2018/1861* przyznało prawo do dostępu do danych w SIS oraz prawo do bezpośredniego wyszukiwania tych danych właściwym organom krajowym odpowiedzialnym za naturalizację, określonym w prawie krajowym, do celów rozpatrywania wniosków o naturalizację. Doprecyzowano zakres uprawnień do systemu dla organów rejestrujących broń oraz dla służb rejestrujących jednostki pływające i statki powietrzne. Obok nowych uprawnień dla użytkowników przepisy wymogły wprowadzenia nowych ram dla procedur krajowych i współpracy organów krajowych w celu realizacji wymagających szybkiego działania terminów wykonania niektórych zadań (kilkugodzinne terminy pozyskania danych uzupełniających do wpisów przez Biura SIRENE, krótkie terminy konsultacji oraz określone, poddane ewidencjonowaniu i monitorowaniu organów nadzorczych terminy usuwania danych z systemu).

Rozporządzenia SIS Recast regulują ponadto dostęp do danych SIS dla Europolu i Frontexu.

Wdrożenie nowej wersji systemu SIS nastąpiło w dniu **7 marca 2023 r.**

4.2 Wizowy System Informacyjny (VIS)

16 maja 2018 r. KE przyjęła wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniającego *rozporządzenie (WE) 767/2008* i inne z nim związane, w sprawie zmian w systemie VIS (tzw. *VIS Revised*). Po miesiącach dyskusji i prac, 27 maja 2021 r. projekt rozporządzenia został przyjęty przez Radę, a następnie uzyskał akceptację w głosowaniu na forum Parlamentu Europejskiego. 13 lipca 2021 r. *rozporządzenie (UE) 2021/1134* zostało opublikowane w dzienniku Urzędowym UE¹. Główne proponowane zmiany to:

- wzmocnienie roli VIS w procedurze wizowej (m.in. weryfikacja automatyczna wszystkich właściwych systemów);
- rozszerzenie kategorii danych przechowywanych w VIS – likwidacja luk informacyjnych, np. dotyczących posiadaczy długoterminowych/zezwoleń na pobyt, wprowadzenie skanu strony personalizacyjnej z paszportu;
- użycie odbitek linii papilarnych palców do uruchomienia alertów SIS w sprawie zaginionych osób (np. ofiar handlu ludźmi),
- rozszerzenie dostępu do danych wizowych na organy azylowe;
- dostosowanie do nowych wyzwań – trwają dyskusje dotyczące obniżenia i wprowadzenia górnej granicy wieku pobierania odbitek linii papilarnych palców (Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz. Urz. UE L 243 z 15.09.2009, s. 1) obecnie przewiduje pobieranie odbitek od 12 r.ż.);
- umożliwienie krajowym organom ścigania oraz Europolowi dostępu do danych VIS na ściśle określonych warunkach na potrzeby ścigania przestępstw.

Komisja przyjmie w drodze aktu wykonawczego decyzję określającą datę uruchomienia VIS zgodnie z *rozporządzeniem 2021/1134*. Na dzień powstania niniejszego dokumentu zakłada się, że nastąpi to po pełnej implementacji komponentów interoperacyjności, czyli najwcześniej **w drugiej połowie 2026 r.**

4.3 System Eurodac

23 września 2020 r. KE opublikowała *Pakt w sprawie Migracji i Azylu* oraz pięć nowych propozycji legislacyjnych. Wśród nich znalazło się *rozporządzenie Eurodac*². Dokument opierając się na wstępnym porozumieniu politycznym zawartym w 2016 r., uzupełnia wypracowane zmiany. Istotą projektu jest przekształcenie Eurodac we wspólną europejską bazę danych, która będzie wspierać politykę UE w obszarze azylu, przesiedleń i migracji nieuregulowanej. Ponadto, umożliwi gromadzenie bardziej dokładnych i kompletnych danych będących źródłem informacji na etapie kształtowania polityki, a tym samym skuteczniejsze wspieranie kontroli migracji nieuregulowanej i wykrywania niedozwolonego przemieszczania się, poprzez umożliwienie liczenia osób ubiegających się o ochronę międzynarodową, a nie tylko wniosków o ochronę międzynarodową. Projekt zakłada także wprowadzenie rozwiązań umożliwiających wdrożenie ram interoperacyjności zgodnie z *rozporządzeniem (UE) 2019/818*.

¹ Jednocześnie zostało opublikowane Rozporządzenie 2021/1133 z dnia 7 lipca 2021 r. w sprawie zmiany rozporządzeń (UE) nr 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 i (UE) 2019/818 w odniesieniu do ustanowienia warunków dostępu do innych systemów informacyjnych UE do celów Wizowego Systemu Informacyjnego (Dz. Urz. UE L 248 z 13.07.2021, s.1).

² https://ec.europa.eu/info/publications/migration-and-asylum-package_en

W dniu 14 maja 2024 r. przyjęto rozporządzenia (UE) 2024/1358 w sprawie ustanowienia systemu Eurodac do porównywania danych biometrycznych w celu skutecznego stosowania rozporządzeń Parlamentu Europejskiego i Rady (UE) 2024/1351 i (UE) 2024/1350 i dyrektywy Rady 2001/55/WE oraz w celu identyfikowania nielegalnie przebywających obywateli państw trzecich oraz bezpaństwowców, w sprawie występowania z wnioskami o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, w sprawie zmiany rozporządzeń Parlamentu Europejskiego i Rady (UE) 2018/1240 i (UE) 2019/818 oraz w sprawie uchylenia rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 603/2013.

Główne zmiany dotyczą:

- nowych kategorii osób podlegających rejestracji w Eurodac;
- beneficjentów tymczasowej ochrony;
- rejestracji osób w procedurze przyjmowania na podstawie rozporządzenia w sprawie przesiedleń;
- nowych kategorii informacji, w tym: wizerunek twarzy, dane biograficzne (imię, nazwisko, obywatelstwo, data urodzenia, miejsce urodzenia), rodzaj i numer oraz data ważności dokumentu tożsamości lub dokumentu podróży, zeskanowana kolorowa kopia wspomnianego dokumentu, data pobrania danych biometrycznych, numer referencyjny wniosku, informacje o państwie członkowskim odpowiedzialnym za rozpatrzenie wniosku, państwie członkowskim relokacji, data przybycia danej osoby po jej udanym przekazaniu, data opuszczenia przez daną osobę terytorium państw członkowskich, data wydalenia, fakt o wydanej wizie, fakt że dana osoba może stanowić zagrożenie dla bezpieczeństwa wewnętrznego, fakt odrzucenia wniosku, fakt wyrażenia zgody na zastosowanie wspomaganego dobrowolnego powrotu i środków reintegracyjnych, data udzielenia ochrony międzynarodowej lub przyznania statusu humanitarnego na mocy prawa krajowego;
- przepisów dotyczących małoletnich i ich ochrony - wiek osoby, od której dane daktyloskopijne będą mogły być pobrane obniżony z 14 do 6 lat (ukończone 6 lat);
- osadzenia Eurodac w ramach interoperacyjności (IO) – system powiązany z CIR, MID, ESP, sBMS, CRRS.

Na dzień powstania niniejszego dokumentu zakłada się, że wdrożenie zmodernizowanego Eurodac nastąpi wieloetapowo w czerwcu oraz grudniu 2026 r.

4.4 System wjazdu/wyjazdu (EES)

Komisja Europejska w komunikacie z 13 lutego 2008 r. „Przygotowanie kolejnych etapów rozwoju zarządzania granicami w Unii Europejskiej” zarysowała potrzebę utworzenia – w ramach strategii UE zintegrowanego zarządzania granicami – **systemu wjazdu/wyjazdu** rejestrującego drogą elektroniczną czas i miejsce wjazdu i wyjazdu obywateli państw trzecich (objętych obowiązkiem wizowym i zwolnionych z tego obowiązku) dopuszczonych do pobytu krótkoterminowego na terytorium PCz oraz służącego do obliczania dozwolonego czasu pobytu tej kategorii obywateli. Rezultatem tych prac było przyjęcie przez gremia UE *rozporządzenia (UE) 2017/2226* oraz *rozporządzenia (UE) 2017/2225*.

Rozporządzenie 2017/2226 ustanawia nowy **system wjazdu/wyjazdu (EES)**, w celu:

- rejestrowania i przechowywania danych osobowych, w tym danych biometrycznych (wizerunek twarzy i 4 odciski linii papilarnych palców prawej lub lewej dłoni), daty, godziny i miejsca wjazdu i wyjazdu obywateli państw trzecich w ramach pobytów krótkoterminowych przekraczających granice państw członkowskich, na których działa EES;
- zastąpienia obowiązku systematycznego stemplowania dokumentów podróży obywateli państw trzecich;

- obliczania okresu dozwolonego czasu pobytu obywateli państw trzecich na terytorium UE i generowania wpisów informujących PCz o upływie okresu dozwolonego pobytu;
- rejestrowania i przechowywania daty, godziny i miejsca odmowy wjazdu udzielonej obywatelom państw trzecich, którym odmówiono wjazdu na pobyt krótkoterminowy, oraz do rejestrowania organu PCz, który odmówił wjazdu, i przyczyn odmowy.

Rozporządzenie (UE) 2017/2226 określa również warunki, zgodnie z którymi wyznaczone organy państw członkowskich i Europol mogą uzyskać dostęp do przeglądania danych EES. Ma to pomóc w zapobieganiu przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywaniu i prowadzeniu w ich sprawie postępowań przygotowawczych.

Wdrożenie EES wprowadzi także zmiany w VIS dotyczące wymiany ograniczonej liczby danych pomiędzy ww. systemami wielkoskalowymi UE oraz dostępu do niektórych informacji zawartych w ww. systemach za pośrednictwem operacji wykonywanych w drugim z tychże systemów.

Na dzień powstania niniejszego dokumentu termin uruchomienia systemu EES to **listopad 2024 r.** Ze względu na brak gotowości niektórych państw członkowskich istnieje prawdopodobieństwo przesunięcia tego terminu. Na dzień powstania dokumentu Komisja Europejska nie przekazała wiążącej propozycji w tym zakresie.

4.5 Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)

W dniu 6 kwietnia 2016 r. Komisja Europejska w komunikacie „*Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa*” przedstawiła potrzebę wzmocnienia i ulepszenia przez UE swoich systemów informatycznych, architektury danych i wymiany informacji w dziedzinie zarządzania granicami, ścigania przestępstw i zwalczania terroryzmu. W kolejnym komunikacie (wrzesień 2016 r.) „*Zwiększanie bezpieczeństwa w mobilnym świecie: ulepszona wymiana informacji na rzecz walki z terroryzmem i wzmocnionych granic zewnętrznych*” KE potwierdziła, że ochrona granic zewnętrznych jest priorytetem, i przedstawiła konkretne inicjatywy mające na celu poszerzenie zakresu i przyspieszenie działań UE służących dalszej poprawie zarządzania granicami zewnętrznymi. Rezultatem tych prac było przyjęcie przez gremia UE *rozporządzenia (UE) 2018/1240*, które:

- ustanawia **Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)** dla obywateli państw trzecich zwolnionych z obowiązku posiadania wizy przy przekraczaniu granic zewnętrznych, umożliwiając rozważenie tego, czy obecność tych obywateli państw trzecich na terytorium państw członkowskich stworzyłaby ryzyko dla bezpieczeństwa, ryzyko nielegalnej imigracji lub wysokie ryzyko epidemiologiczne;
- określa warunki, na jakich wyznaczone organy państw członkowskich oraz Europol mają zasilać danymi ETIAS oraz mogą przeglądać dane przechowywane w systemie centralnym ETIAS do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom objętym zakresem ich kompetencji, wykrywania tych przestępstw i prowadzenia postępowań przygotowawczych w ich sprawie.

System ETIAS będzie systemem komplementarnym dla obecnie istniejącego Wizowego Systemu Informacyjnego (VIS) oraz nowotworzonego systemu wjazdu/wyjazdu (EES). ETIAS wypełni poważną lukę w systemie zapewnienia bezpieczeństwa obywatelom UE w zakresie przepływu obywateli państw trzecich korzystających z ruchu bezwizowego, w związku z czym będzie w sposób efektywny wspólnie z systemem VIS uzupełniał i wspierał system EES.

Uruchomienie ETIAS spowoduje także wdrożenie jednego z komponentów interoperacyjności o nazwie ESP wraz z modułem CIR, który w przyszłości będzie odpowiadał m.in. za kojarzenie danych alfanumerycznych w ramach odpytania wszystkich systemów wielkoskalowych UE. Ponadto służbom

imigracyjnych w trakcie realizacji czynności weryfikacyjnych na terytorium UE, uruchomienie systemu ETIAS umożliwi jego weryfikację w formie kaskadowej poprzez zainicjowanie odpytania w systemie EES.

Na dzień powstania niniejszego dokumentu termin uruchomienia systemu ETIAS to **II połowa 2025 r.** (data rozpoczęcia eksploatacji systemu zależna jest od pełnego wdrożenia i uruchomienia systemu EES w zakładanym w dokumencie terminie, tj. IV kwartał 2024 r.).

4.6 Europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN)

W dniu 19 stycznia 2016 r. Komisja Europejska przyjęła wniosek w sprawie dyrektywy zmieniającej decyzję ramową Rady 2009/315/WSiSW dotyczącą ECRIS oraz – w dniu 29 czerwca 2017 r. – uzupełniający wniosek w sprawie rozporządzenia w celu ustanowienia scentralizowanego systemu ECRIS-TCN obejmującego obywateli państw trzecich i bezpieczeństwa umożliwiającego skuteczne określanie PCz, które wydały wyrok skazujący wobec danego obywatela państwa trzeciego lub bezpieczeństwa. Wynikiem tych prac było przyjęcie przez gremia UE *rozporządzenia (UE) 2019/816* oraz *dyrektywy (UE) 2019/884*.

Rozporządzenie (UE) 2019/816 ustanawia przepisy dotyczące utworzenia scentralizowanego systemu, określa dane, które system ten ma zawierać, oraz prawa dostępu do przetwarzanych w nim danych. ECRIS-TCN będzie składał się z systemu centralnego oraz wspólnego repozytorium danych umożliwiających identyfikację (CIR) stworzonego na podstawie *rozporządzenia (UE) 2019/817* i *rozporządzenia (UE) 2019/818*. W związku z objęciem systemu ECRIS-TCN ramami interoperacyjności do systemu będą miały zastosowanie również pozostałe narzędzia, o których mowa w rozdziale 1.7.

W systemie będą przetwarzane dane identyfikujące (dane alfanumeryczne i biometryczne) obywateli państw trzecich, bezpieczeństwa a także osób posiadających jednocześnie obywatelstwo UE i państwa trzeciego skazanych na terytorium państw członkowskich. Informacje o samym wyroku skazującym nadal można będzie uzyskać jedynie od skazującego państwa członkowskiego.

Rozporządzenie ustanawia też podział obowiązków między PCz a Agencją eu-LISA, która jest odpowiedzialna za rozwijanie i obsługę systemu.

Na dzień powstania niniejszego dokumentu termin uruchomienia systemu ECRIS-TCN to **III kwartał 2025 r.**

4.7 Interoperacyjność Wielkoskalowych Systemów Informacyjnych UE (IO)

Wydajność i skuteczność polityk UE w zakresie azylu, imigracji i kontroli granic zewnętrznych oraz zdolność reagowania na stale zmieniające się zagrożenia dla bezpieczeństwa (tj. terroryzm, przestępczość zorganizowana i cyberprzestępczość) zależą od kompleksowej wymiany informacji między właściwymi organami krajowymi i europejskimi. Procesy wymiany informacji ułatwiają nowoczesne systemy informacyjne EES, VIS, ETIAS, Eurodac, SIS i ECRIS-TCN. Systemy te, wraz z nową architekturą interoperacyjności (IO) mają zapewnić zintegrowane inteligentne podejście do zapewnienia bezpieczeństwa wewnętrznego Europy. Zakładane jest, że dzięki nim poprawi się wydajność i skuteczność uzyskiwania informacji, zapewnione będą standardy i narzędzia techniczne, które umożliwią lepszą współpracę. Wzmocnione zostaną technologie w zakresie cyberbezpieczeństwa i odporności, jeszcze bardziej wzmacniając bezpieczeństwo danych oraz bezpieczeństwo fizyczne na obszarze Schengen.

Interoperacyjność będzie realizowana na kilku płaszczyznach. Pierwsza będzie dotyczyć sprawnego przeszukiwania wielkoskalowych systemów centralnych UE w celu uzyskiwania koniecznych informacji, którą umożliwi pojedynczy punkt dostępowy, przy pełnym poszanowaniu zasad kontroli dostępu

i wymogów dotyczących ochrony danych regulujących podstawowe systemy centralne. Drugą będzie stanowić utworzenie wspólnego repozytorium tożsamości, które poprawi jakość przechowywanych danych umożliwiających identyfikację osób oraz zapobiegnie wielokrotnemu dublowaniu danych osobowych w ramach poszczególnych systemów wielkoskalowych.

Podstawę prawną dla interoperacyjności stworzyły rozporządzenia Parlamentu Europejskiego i Rady 2019/817 (w obszarze granic i polityki wizowej) oraz 2019/818 (w obszarze współpracy policyjnej i sądowej, azylu i migracji). Rozporządzenia te obejmują systemy działające:

- **System Informacyjny Schengen (SIS)**, który zawiera szerokie spektrum alertów dotyczących osób (odmowy wjazdu lub pobytu, nakazy aresztowania UE, osoby zaginione, pomoc w postępowaniu sądowym, dyskretne kontrole) i przedmiotów (w tym zgubionych, skradzionych lub unieważnionych dokumentów tożsamości lub podróży);
- system **Eurodac** z danymi odcisków palców osób ubiegających się o azyl i obywateli państw trzecich, którzy nielegalnie przekroczyli granice zewnętrzne lub nielegalnie przebywają w państwie członkowskim;
- **Wizowy System Informacyjny (VIS)** z danymi dotyczącymi posiadaczy wiz krótkoterminowych (po planowanej modernizacji systemu również wiz długoterminowych oraz zezwoleń na pobyt);

oraz uruchamiane lub będące w fazie opracowywania:

- **System wjazdu/wyjazdu (EES)**, który zastąpi obecny system ręcznego stemplowania paszportów oraz będzie elektronicznie rejestrował imię i nazwisko, rodzaj dokumentu podróży, dane biometryczne oraz datę i miejsce wjazdu i wyjazdu obywateli państw trzecich odwiedzających strefę Schengen na krótki pobyt;
- **Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)** będący zautomatyzowanym systemem, który gromadziłby i weryfikował informacje związane z bezpieczeństwem i przekazywane przez obywateli państw trzecich przed ich podróżą do strefy Schengen;
- oraz **Europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN)**, który będzie elektronicznym systemem służącym do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpieczeństwa.

Architektura IO przewiduje również możliwość przeszukiwania baz danych **Interpolu** dotyczących skradzionych i utraconych dokumentów podróży (SLTD) oraz dokumentów podróży powiązanych z notami Interpolu (TDAWN), jak również baz danych **Europolu** – poprzez ESP.

Krajowe systemy informacyjne i zdecentralizowane unijne systemy informacyjne pozostają poza zakresem IO. W razie wykazania takiej potrzeby systemy zdecentralizowane, takie jak te działające na mocy ram z Prüm, dyrektywy w sprawie danych dotyczących przelotu pasażera (PNR) i dyrektywy w sprawie danych pasażera przekazywanych przed podróżą (API), mogą w przyszłości zostać powiązane z jednym lub większą liczbą komponentów IO.

Cztery podstawowe techniczne komponenty IO to:

- **Europejski Portal Wyszukiwania (ESP)** — umożliwi upoważnionym użytkownikom przeprowadzenie pojedynczego wyszukiwania i otrzymanie wyników ze wszystkich systemów, do których mają oni dostęp, zamiast przeszukiwania każdego systemu osobno. Zapewni równoległe przeszukiwanie wszystkich systemów informacyjnych UE, danych Europolu i baz danych Interpolu. Stanowić będzie „pojedyncze okno” lub „pośrednika komunikatów” służące przeglądaniu różnych systemów centralnych i sprawnemu pozyskiwaniu wymaganych informacji, przy pełnym poszanowaniu wymogów związanych z kontrolą dostępu i ochroną danych obowiązujących w systemach podstawowych, zgodnie z instrumentami prawnymi regulującymi te systemy.

- **Wspólny System Porównywania Danych Biometrycznych (sBMS)** – umożliwi użytkownikom skuteczniejsze wyszukiwanie i dopasowywanie danych biometrycznych (odcisków palców i wizerunków twarzy) przechowywanych w systemach, do których mają dostęp (zwłaszcza SIS, Eurodac, VIS, EES i ECRIS-TCN). Obecnie każdy istniejący system centralny dysponuje specjalną, zastrzeżoną wyszukiwarką danych biometrycznych, sBMS zapewni wspólną platformę jednoczesnego przeglądania i porównywania danych. Dane biometryczne, takie jak odciski palców i wizerunki twarzy, są unikalne, a zatem znacznie bardziej niezawodne do celów identyfikacji osób niż dane alfanumeryczne. sBMS stanowić będzie narzędzie techniczne służące identyfikacji osób, które mogą być zarejestrowane w kilku bazach danych, poprzez użycie pojedynczego komponentu technologicznego, zamiast wielu, w celu skojarzenia danych biometrycznych tych osób w różnych systemach. Oprócz obsługi CIR i MID, sBMS przechowuje szablony biometryczne pobrane z CIR i SIS w celu przeszukiwania i porównywania danych biometrycznych.
- **Wspólne Repozytorium Danych Umożliwiających Identyfikację (CIR)** – umożliwi upoważnionym użytkownikom dostęp do informacji o obywatelach spoza UE przechowywanych w różnych systemach, dzięki czemu można ich będzie bardziej niezawodnie zidentyfikować. CIR stanowić będzie wspólny zbiór danych dotyczących tożsamości, dokumentów podróży i danych biometrycznych osób zarejestrowanych w systemach EES, VIS, ETIAS, Eurodac i ECRIS-TCN. Będzie stanowić element struktury technicznej tych systemów i pełnić funkcję wspólnego komponentu łączącego je w celu przechowywania i przeszukiwania przetwarzanych przez nie danych dotyczących tożsamości, danych dokumentu podróży i danych biometrycznych. CIR usprawni dostęp organów ścigania do systemów informacyjnych niezwiązanych ze ściganiem przestępstw przy jednoczesnym utrzymaniu wysokiej jakości zabezpieczeń ochrony danych poprzez funkcję „wynik/brak wyniku”, która umożliwi sprawdzenie obecności (lub braku) danych w dowolnym z systemów objętych repozytorium za pomocą prostego powiadomienia o wyniku lub jego braku.
- **Detektor Wielokrotnych Tożsamości (MID)** – sprawdzi, czy przeszukiwane dane dotyczące osoby (której dotyczy zapytanie) znajdują się również w pozostałych systemach. Rozwiązanie to stanowi uzupełnienie CIR o możliwość przeszukiwania danych SIS. MID przechowywać będzie powiązania między danymi w różnych systemach informacyjnych UE, aby wykrywać wielokrotne tożsamości, w celu ułatwienia kontroli tożsamości osób podróżujących w dobrej wierze i zwalczania oszustw dotyczących tożsamości. Pozwoli wykrywać multiplikację tożsamości powiązaną z tym samym zestawem danych biometrycznych i umożliwi ustalenie, czy różne nazwiska rzeczywiście należą do tej samej osoby. MID będzie zawierać powiązania między danymi dotyczącymi osób obecnych w więcej niż jednym systemie informacyjnym UE. MID jest tworzony wyłącznie w celu wsparcia CIR i zapewnienia dostępu do danych przechowywanych przez organy centralne oraz Biuro SIRENE. MID wprowadza możliwość zapewnienia dostępu do systemów EES, VIS, ETIAS i Eurodac za pomocą dwuetapowego podejścia do przeglądania danych. Jednak dwuetapowe podejście do przeglądania danych wejdzie w życie dopiero po uruchomieniu w pełni elementów IO.

Powstaną także cztery dodatkowe rozwiązania pomagające skuteczniej wdrażać IO:

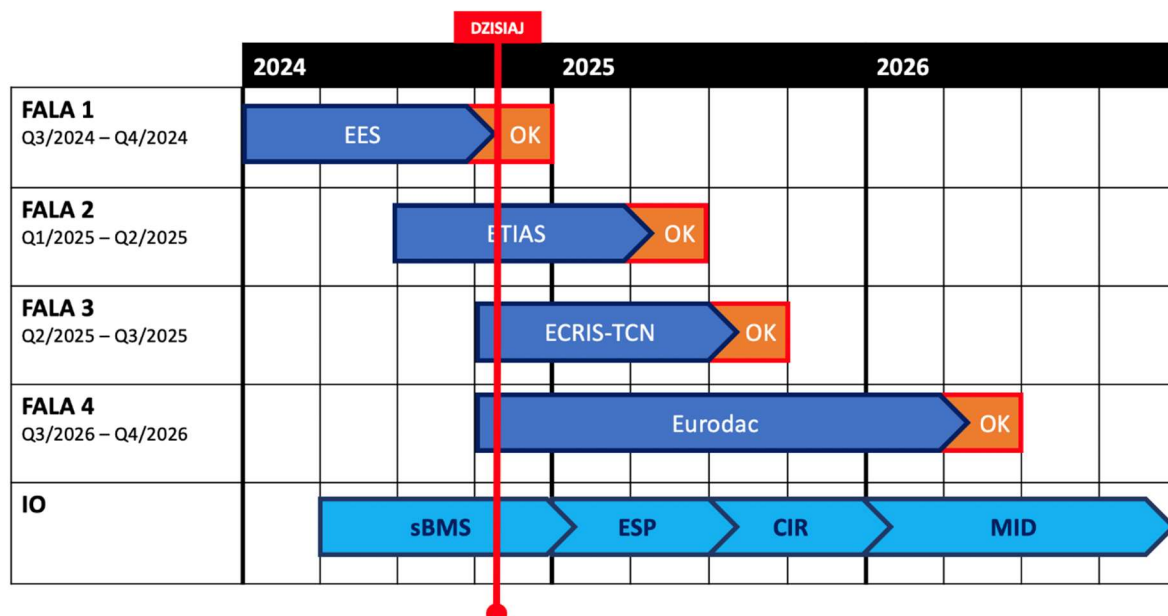
- **Centralne Repozytorium Sprawozdawczo-Statystyczne (CRRS)** – system umożliwiający sporządzanie zestawień danych przechowywanych w systemach wielkoskalowych UE niezbędny do tworzenia i bezpiecznego udostępniania sprawozdań – przygotowywanych na podstawie anonimowych danych statystycznych – na potrzeby polityki, operacji i jakości danych. CRRS będzie odpowiedzialne za anonimowe dostarczanie raportów analitycznych dla polityk i danych statystycznych we wszystkich systemach. Ponieważ renderowanie danych jest anonimowym zautomatyzowanym procesem, dostęp do CRRS będzie zapewniany wyłącznie w celach statystycznych i sprawozdawczych.

- **Uniwersalny Format Wiadomości (UMF)** – wspólny i jednolity język techniczny służący opisywaniu i łączeniu elementów danych, zwłaszcza elementów związanych z osobami i dokumentami (podróży). Co oznacza, że różne systemy mogą łatwiej porównywać dane i współpracować ze sobą. Ułatwi to również integrację nowych systemów informatycznych i uczyni je interoperacyjnymi z istniejącymi systemami.
- **Zautomatyzowane mechanizmy kontroli jakości danych** i wspólnych wskaźników jakości. Kluczowe jest, aby państwa członkowskie zapewniły najwyższy poziom jakości danych podczas zasilania i korzystania z systemów. Aby przezwyciężyć problemy, które mogą wynikać z wprowadzania danych przez operatorów ludzkich, automatyczne zasady walidacji mogą zapobiegać błędom. Celem tych środków jest automatyczne identyfikowanie pozornie nieprawidłowych lub niespójnych przestań danych, aby można je było sprawdzić i poprawić w razie potrzeby;
- **CSLR Central System for Yellow Link Resolution** – w związku z obowiązkiem państw członkowskich do identyfikowania i łączenia tożsamości osób gromadzonych w CIR zostanie przygotowane na poziomie centralnym narzędzie umożliwiające określanie rodzajów powiązań pomiędzy grupami danych, w tym rozwiązywanie tzw. „żółtych linków”.

Wszystkie te składowe, tworząc ekosystem IO, wymagają także wyraźnego skupienia się na cyberbezpieczeństwie i przeciwdziałaniu zagrożeniom w cyberprzestrzeni. Wyzwania, jakie stwarza era cyfrowa oraz trwający konflikt militarny za wschodnią granicą strefy Schengen wymagają, aby wszystkie działania były zgodne z wnioskiem KE w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, tj. ze zmienioną dyrektywą w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa NIS2), która przewiduje szeroki zakres środków zapewniających bezpieczną wymianę informacji i ogólne bezpieczeństwo systemów informatycznych.

Proponowane przez KE fazy rozwoju IO to:

- **Fala 1** od 3. do 4. kwartału 2024 – rozpoczęcie eksploatacji EES + sBMS (pierwszy komponent interoperacyjności) dla EES i VIS;
- **Fala 2** od 1. do 2. kwartału 2025 – rozpoczęcie eksploatacji ETIAS + ESP i CIR (drugi i trzeci komponent interoperacyjności);
- **Fala 3** od 2 do 3. kwartału 2025 – rozpoczęcie eksploatacji ECRIS-TCN + ESP i CIR i sBMS dla ECRIS-TCN;
- **Fala 4** od 3 do 4. kw. 2026 – rozpoczęcie eksploatacji odnowionego VIS oraz Eurodac + Zakończenie architektury interoperacyjności (dostarczenie MID – ostatniego komponentu interoperacyjności) i rozpoczęcie okresu przejściowego MID.



Rysunek 1. Przyjęte przez eu-LISA fale zadań

System wjazdu/wyjazdu (EES) będzie pierwszym systemem, który zostanie dostarczony jesienią 2024 r. Równolegle z EES powstanie Wspólny System Porównywania Danych Biometrycznych (sBMS) jako pierwszy komponent interoperacyjności. Sześć miesięcy później, wiosną 2025 r., nastąpi uruchomienie Europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS), który zostanie połączony z Europejskim Portalem Wyszukiwania (ESP) i Wspólnym Repozytorium Danych Umożliwiających Identyfikację (CIR). Następnie dostarczony będzie Europejski system przekazywania informacji z rejestrów karanych w odniesieniu do obywateli państw trzecich (ECRIS-TCN), jako jednostka centralna wspomagająca poprawną identyfikację osób i tożsamości, danych dokumentów podróży i danych biometrycznych w CIR. Ostatnim elementem IO będzie dostarczenie Detektora Wielokrotnych Tożsamości (MID).

KE zgodnie z rozporządzeniami wpisuje systemy wymiany informacji w cztery obszary:

- **Azyl, migracja i granice** – Eurodac;
- **Bezpieczeństwo wewnętrzne i granice UE** – SIS, Prüm II, API;
- **Schengen, granice i wizy** – VIS, EES, ETIAS;
- **Współpraca wymiaru sprawiedliwości** – ECRIS-TCN, e-CODEX.

Interoperacyjność systemów informacyjnych UE powinna umożliwiać systemom wzajemne uzupełnianie się i ułatwić w ten sposób poprawną identyfikację osób, w tym osób nieznanymi, które nie są w stanie potwierdzić swojej tożsamości, przyczynić się do zwalczania oszustw dotyczących tożsamości, poprawić i zharmonizować wymagania dotyczące jakości danych, wzmocnić gwarancje bezpieczeństwa danych i ochrony danych, usprawnić dostęp do systemów EES, VIS, ETIAS i Eurodac do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych oraz wspierać realizację celów systemów EES, VIS, ETIAS, Eurodac, SIS i ECRIS-TCN.

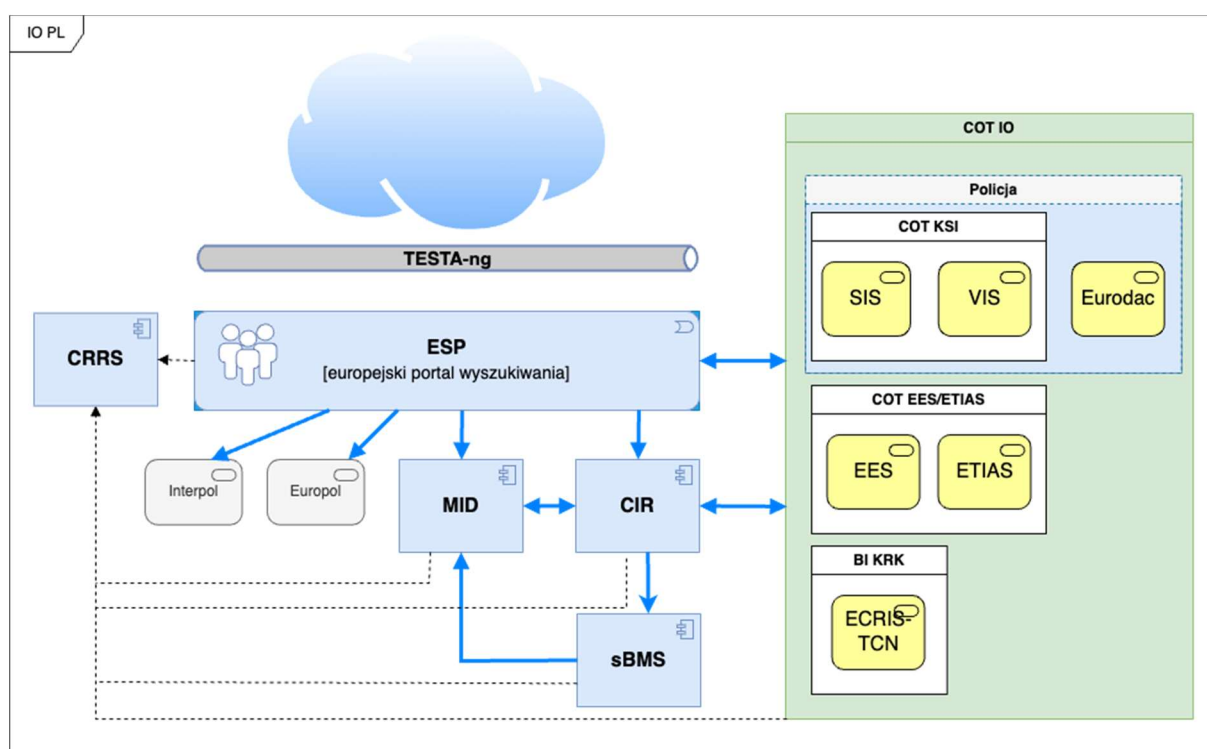
KE podkreśla, że należy jednak pozostawić krajowe połączenia z różnymi systemami informacyjnymi UE, aby zapewnić techniczną opcję awaryjną. Jednocześnie KE pozostawia PCz prawo do wyznaczenia organu odpowiedzialnego za zarządzanie oraz dostarczanie centralnego punktu dostępu lub centralnych punktów dostępu, które jednak winny działać niezależnie od wyznaczonych organów i powinny weryfikować, czy w konkretnym rozpatrywanym przypadku spełnione są warunki wystąpienia o uzyskanie dostępu do systemu centralnego. PCz powiadamiają KE o wyznaczonych przez siebie

organach i centralnych punktach dostępu i mogą w dowolnym czasie zmienić lub zastąpić te powiadomienia.

Szczegółowe kwestie techniczne nie są ostatecznie ustalone i są w ciągłym opracowaniu na poziomie UE dlatego bieżąca wersja dokumentu nie przedstawia ostatecznych założeń w zakresie interoperacyjności.

Za wdrożenie IO odpowiada KGSG, dodatkowo prawodawstwo polskie ustanawia (oraz jest w trakcie ustanawiania), następujące organy techniczne odpowiedzialne za realizację udziału PL w WSIUE:

- **COT KSI** (Centralny Organ Techniczny Krajowego Systemu Informatycznego) - rolę pełni Komendant Główny Policji, obejmuje SIS oraz VIS, a także opiekę techniczną nad Eurodac;
- **COT IO/EES/ETIAS** (Centralny Organ Techniczny dla Interoperacyjności, EES i ETIAS) – rolę tą pełni Komendant Główny Straży Granicznej, obejmuje narzędzia Interoperacyjności, EES i ETIAS;
- **BI KRK** (Biuro Informacyjne Krajowego Rejestru Karnego) – komórka organizacyjna Ministerstwa Sprawiedliwości będąca organem centralnym ECRIS i ECRIS-TCN w Polsce, obejmuje ECRIS-TCN.



Rysunek 2. Systemy krajowe dostępujące do komponentów IO

Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) zarządza istniejącymi Wielkoskalowymi Systemami Informacyjnymi UE. Agencji powierzono odpracowanie, uruchomienie i zarządzanie nowymi WSIUE. W ramach współpracy z eu-LISA Polska ma przedstawicieli w Zarządzie Agencji. Polska jest reprezentowana w Zarządzie przez Dyrektora Departamentu Teleinformatyki MSWiA, w którego kompetencjach leży tematyka wielkoskalowych systemów informacyjnych UE. Przedstawiciele PL służb odpowiedzialnych za techniczne wdrażanie poszczególnych wielkoskalowych systemów informacyjnych UE i ich interoperacyjności uczestniczą w pracach Grup Doradczych Agencji eu-LISA, a także w gremiach Project Management Forum (PMF) na których prace skupione są w głównej

mierze na rozwoju systemów w aspekcie biznesowym i interoperacyjności oraz poruszane są kwestie postępów i głównych wyzwań w prowadzonych przedsięwzięciach. Kwestie omawiane w ramach gremiów doradczych eu-LISA są później przedstawiane Zarządowi Agencji.

4.8 Infrastruktura transportowa (TESTA-ng)

Infrastruktura komunikacyjna Wielkoskalowych Systemów Informacyjnych UE (WSIUE) wykorzystuje sieć TESTA-ng (Trans-European Services for Telematics between Administrations – New Generation), która zapewnia sieć szkieletową oddzieloną od publicznego Internetu. TESTA-ng jest preferowanym rozwiązaniem dla paneuropejskiej wymiany informacji między administracjami wymagającymi gwarantowanych poziomów usług dla dostępności sieci, wydajności i/lub bezpieczeństwa. Infrastruktura TESTA-ng została zbudowana tak, aby podlegała procesowi akredytacji bezpieczeństwa, aby umożliwić wymianę informacji niejawnych UE do poziomu „RESTREINT UE”.

Sieć TESTA-ng jest ogólnoeuropejską platformą teletransmisyjną wykorzystywaną na potrzeby zapewnienia komunikacji pomiędzy PCz a systemami wielkoskalowymi UE, zapewniając szybkość i bezpieczną wymianę informacji w czasie rzeczywistym. Jest to separowany, wydzielony kanał wymiany informacji, który ma wymiar nie tylko transgraniczny, ale także łączy poszczególne resorty i urzędy na terenie PCz. W ramach krajowego segmentu TESTA-ng realizowana jest komunikacja pomiędzy Ministerstwami, jednostkami organizacyjnymi Policji, Straży Granicznej, Państwowej Straży Pożarnej, agencji wywiadowczych i bezpieczeństwa oraz wojska, w tym dostęp użytkowników instytucjonalnych do WSIUE. Wymiana danych przez interfejs komunikacyjny systemów teleinformatycznych sieci TESTA-ng umożliwia dostęp do danych udostępnianych przez inne kraje członkowskie UE oraz kraje stowarzyszone. W ramach TESTA-ng udostępniane są także liczne usługi europejskie. Usługi udostępniają zarówno biura i organizacje UE jak i PCz.

Do obsługi WSIUE w TESTA-ng wykorzystywane są trzy domeny (komponenty interoperacyjności będą wykorzystywane we wszystkich trzech domenach): **domena SIS** dla SIS i SIRENE Mail, **domena VIS** dla VIS (w tym VISMail), EES i ETIAS, **EuroDomain** dla Eurodac, DubliNet i ECRIS-TCN.

Użytkownicy końcowi łączą się z różnymi domenami, fizycznie oddzielonymi w siedzibach użytkowników, przy użyciu oddzielnych gotowych punktów dostępu (Traffic Access Point, TAP), zlokalizowanych w geograficznie odległych obiektach, aby szybko wznowić działanie w przypadku katastrofy lub konserwacji. Aby dodatkowo zapewnić dostępność i niezawodność sieci, same TAP obejmują dodatkowe redundancje. Ministerstwo Spraw Wewnętrznych i Administracji jest odpowiedzialne za administrowanie Polskimi Domenami Lokalnymi (PDL) będącymi bramami dostępowymi pomiędzy Polską a krajami Unii Europejskiej. W latach 2020-2023 PDL przeszedł gruntowną modernizację w celu sprostania zmianom dokonywanym przez EU oraz stale powiększającej się liczbie użytkowników, a co za tym idzie systemów wykorzystywanych przez użytkowników w PL oraz ilość danych przetwarzanych przez te systemy. Z uwagi na wzrastające znaczenie kanałów do bezpiecznej komunikacji, w tym konieczność zapewniania stałej i gwarantowanej dostępności do niezawodnych, bezpiecznych i solidnych usług komunikacyjnych w czasie pokoju, kryzysu i konfliktu w ramach UE, a także umożliwianie dostępu do konkretnych usług dla krajów niewchodzących w skład UE planuje się dalsze modernizacje. Rozbudowywana będzie o nowe urządzenia agregujące ruch sieciowy PDL, powstaną nowe węzły, planowany jest zakup urządzeń dostępowych\końcowych dla nowych użytkowników.

MSWiA jako organ zarządzający TESTA-ng odpowiednio zapewnienia najwyższy poziom zgodności działań modernizacyjnych z unijnymi ramami regulacyjnymi i wymogami bezpieczeństwa, ochronę i ciągłość działania, w tym efektywny system szybkiego przywracania funkcjonalności i odtwarzania na wypadek awarii, ataków oraz innych zdarzeń zakłócających prawidłowe funkcjonowanie.

5 Współpraca polskich instytucji z Wielkoskalowymi Systemami Informacyjnymi UE

5.1 Ramy prawne

Ustawa o SIS i VIS stanowi podstawę prawną działania Systemu Informacyjnego Schengen i Wizowego Systemu Informacyjnego w Polsce oraz określa zasady i sposób realizacji udziału Rzeczypospolitej Polskiej w SIS oraz VIS, w tym organy/służby uprawnione do dostępu do Systemu Informacyjnego Schengen i Wizowego Systemu Informacyjnego, ich obowiązki i uprawnienia dotyczące dokonywania wpisów oraz wglądu do danych zawartych w SIS oraz VIS poprzez Krajowy System Informatyczny (KSI).

Ponadto, wraz ze zmianami ustawy o SIS i VIS i przepisów wykonawczych, organy i służby przyjęły wewnętrzne regulacje zapewniające odpowiednie standardy wykorzystania danych, monitorowania jakości danych przekazywanych do systemów oraz właściwą realizację procedur.

Prace związane z wdrożeniem i przygotowaniem do współpracy z Systemem wjazdu/wyjazdu (EES) prowadzone były w ramach prac Zespołu projektowego do spraw dostosowania przepisów prawnych systemu EES, który opracował projekt ustawy z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu, która została ogłoszona w Dzienniku Ustaw pod poz.1688.

W Ministerstwie Sprawiedliwości trwają prace legislacyjne dotyczące nowelizacji ustawy o KRK. Projektowane przepisy będą regulowały udział Rzeczypospolitej Polskiej w systemie ECRIS-TCN. Projekt ustawy o zmianie ustawy o KRK oraz niektórych innych ustaw, na dzień powstania niniejszego dokumentu, otrzymał w wykazie prac legislacyjnych Rady Ministrów nr UC57.

5.2 Ochrona danych osobowych

Modernizacja systemów SIS II, VIS, Eurodac oraz wdrożenie nowych systemów EES, ETIAS, ECRIS-TCN i Interoperacyjności powinno odbywać się także z poszanowaniem prawa ochrony danych osobowych regulowanego na poziomie unijnym i krajowym, w szczególności z przepisami UE w tym zakresie – rozporządzeniem 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)³ oraz ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości⁴, implementującą dyrektywę 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 uchyłającą decyzję ramową Rady 2008/977/WSiSW⁵.

Stosownie do zaleceń Komisji Europejskiej, na podstawie przeprowadzonej analizy zgodności, tylko część instytucji będzie mogła dokonywać wpisów w ramach dostępu do Wielkoskalowych Systemów Informacyjnych UE. Pozostałe instytucje będą miały jedynie możliwość przeglądania danych. Szczególna uwaga zostanie zwrócona na przetwarzanie danych szczególnie chronionych tj. odbitek linii papilarnych oraz szczególnych grup osób tj. danych migrantów i uchodźców, zwłaszcza małoletnich.

Gromadzenie i wykorzystywanie tego rodzaju danych będzie podlegać także ścisłej analizie zasadności ich przechowywania w bazach danych.

³ Dz. Urz. UE. L 119, z 04.05.2016, s. 1

⁴ Dz. U. z 2019 r. poz. 125 oraz z 2022 r. poz. 1700

⁵ Dz. Urz. UE. L 119, z 04.05.2016, s. 89

Ze względu na skalę i charakter danych, które mają być przetwarzane i przechowywane w bazach danych Wielkoskalowych Systemów Informacyjnych UE konieczne jest stworzenie silnych zabezpieczeń prawnych, technicznych i organizacyjnych.

Dotychczasowe rozwiązania w zakresie ochrony danych osobowych w istniejących przepisach prawnych uregulowane są w rozdz. 3 (art. 8–11) ustawy o SIS i VIS. Zgodnie ze wskazanymi wyżej przepisami Prezes UODO uprawniony jest do bezpośredniego dostępu do Krajowego Systemu Informatycznego (KSI) w celu sprawowania kontroli oraz we wskazanych przypadkach, o których mowa w art. 44 ust. 6 rozporządzenia 2018/1861 oraz art. 59 ust. 6 rozporządzenia 2018/1862, jest organem uprawnionym do przekazania sprawy Europejskiemu Inspektorowi Ochrony Danych w celu podjęcia działań mediacyjnych. Administratorem danych osobowych przetwarzanych poprzez Krajowy System Informatyczny (KSI) jest Centralny Organ Techniczny KSI.

5.3 Cyberbezpieczeństwo

Obszary zarządzania granicami, bezpieczeństwa wewnętrznego, zarządzania migracjami i współpracy sądowej w Unii Europejskiej przechodzą poważną transformację, przechodząc stopniowo ze świata fizycznego do wirtualnego. Wymaga to większej uwagi w zakresie cyberbezpieczeństwa i powiązanych zagrożeń pochodzących z wielu źródeł, zarówno naturalnych, jak i spowodowanych przez człowieka. Zapewnianie cyberodporności infrastruktury cyfrowej, stanowiącej fundament komunikacji, a co za tym idzie podstawę wszelkich działań podejmowanych w obszarach społecznych i gospodarczych stało się warunkiem niezbędnym dla sprawnego działania kluczowych systemów objętych Programem.

Obszar cyberbezpieczeństwa jest gruntownie uregulowany w krajowych aktach prawnych. Jednocześnie przepisy związane z tym obszarem podlegają okresowej ewaluacji i w konsekwencji dość częstym zmianom. Regulacje w różnych obszarach polityk wskazują na wzmożoną koncentrację KE na cyberbezpieczeństwo i bezpieczeństwo informatyczne. Zmieniona dyrektywa NIS (NIS Directive, 2023); nowe akty prawne dotyczące odporności podmiotów krytycznych (CER Directive, 2023), cyfrowej odporności operacyjnej podmiotów finansowych (DORA, 2023) oraz cyberbezpieczeństwa instytucji, organów i agencji UE (EUIBAs, Regulation 2023/2841); ustanowienie europejskiego systemu certyfikacji cyberbezpieczeństwa (Cybersecurity Act, 2019); możliwość kontrolowania eksportu narzędzi do cybernadzoru w określonych okolicznościach (Regulation 2021/821); inicjatywa na rzecz Akademii Umiejętności Cyberbezpieczeństwa (Cybersecurity Skills Academy, 2023); lub zmienione wytyczne wykonawcze Zestawu Narzędzi Dyplomacji Cybernetycznej UE (EU's Cyber Diplomacy Toolbox, 2023) to kilka bardzo znaczących inicjatyw związanych z cyberbezpieczeństwem na szczeblu UE w ciągu ostatnich kilku lat.

Polska ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703), zwana dalej UKSC, była zmieniana od 2018 r. już 12-krotnie, co wskazuje na ciągłe doskonalenie i dostosowywanie przepisów do aktualnych zagrożeń w cyberprzestrzeni. Przepisy krajowe w zakresie cyberbezpieczeństwa w dalszym ciągu podlegać będą wielu zmianom, ponieważ niezbędne jest ich dostosowywanie do przepisów UE.

Projekt IO wpłynie na zmianę paradygmatu związane z podejściem do WSIUE zapoczątkowaną współpracą EES, VIS i sBMS. Interoperacyjność zmieni podstawową architekturę systemów z opartej na silosach (dedykowane elementy) na systemy, które współdzielą podstawowe elementy aplikacji, takie jak front-end query ESP (European Search Portal) i podstawowe bazy danych, takie jak CIR (Common Identity Repository) lub MID (Multiple Identity Detector). Kierując się wytycznymi KE (np. dyrektywy NIS 2 oraz przyszłych rozporządzeń w sprawie cyberbezpieczeństwa i bezpieczeństwa informacji), wymagane będzie wdrażanie dodatkowych środków w celu zapewnienia cyberbezpieczeństwa i ciągłości działania wszystkich systemów informatycznych objętych Programem.

Resort spraw wewnętrznych i administracji posiada duże doświadczenie w obszarze cyberbezpieczeństwa i dostosowywania własnych regulacji do obowiązujących przepisów związanych z zapewnieniem cyberbezpieczeństwa. Ministerstwo Spraw Wewnętrznych i Administracji oraz jednostki podległe Ministrowi SWiA i przez niego nadzorowane, stanowiące w myśl art. 4 pkt 7 UKSC jednostki sektora finansów publicznych, zobowiązane są do wypełniania zadań, o których mowa m.in. w art. 22 UKSC. Zadania te dotyczą m.in. zarządzania incydentami, zgłaszania incydentów, prowadzenia szkoleń oraz akcji uświadamiających, czy też wskazania osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. MSWiA w ramach obsługi incydentów stale współpracuje z funkcjonującym w strukturach ABW zespołem CSIRT GOV.

Ciągła dostępność procesów w obszarze wymiaru sprawiedliwości i spraw wewnętrznych (JHA) obecnie w coraz większym stopniu zależy od wsparcia IT. Wymaga to odpowiednich środków bezpieczeństwa i odporności w celu zapewnienia wsparcia cyklu życia systemów IT. Obejmuje to środki organizacyjne i infrastrukturalne mające na celu prawidłowe zarządzanie ciągłością działania i odzyskiwaniem po awarii. MSWiA odpowiada za cyberbezpieczeństwo infrastruktury telekomunikacyjnej JHA. Infrastruktura ta, pomimo że działa na protokołach internetowych, jest jednak całkowicie odizolowana od publicznego Internetu. Dla zapewnienia maksymalnego bezpieczeństwa wykorzystuje solidne szyfrowanie przy użyciu certyfikowanych urządzeń szyfrujących. W celu ochrony przed zagrożeniami oraz zapewnienia cyberbezpieczeństwa, w tym również bezpieczeństwa danych wymienianych przy jej użyciu, jest ona odpowiednio zarządzana i podlega kontroli. Stały monitoring cyberbezpieczeństwa zasobów odbywa się z wykorzystaniem posiadanych systemów monitorowania. W latach 2024-2026 MSWiA planuje ich sukcesywny rozwój w celu dalszego zapewniania działania w bezpiecznym i zabezpieczonym środowisku oraz zapewnianie adekwatnych poziomów ochrony aktywów i informacji współmiennie do zidentyfikowanych ryzyk.

W latach 2022-2023 w ramach programu modernizacji służb podległych Ministrowi SWiA na lata 2022-2025 rozbudowano systemy cyberbezpieczeństwa Policji oraz Straży Granicznej, a w planach znajdują się rozwiązania wykorzystujące sztuczną inteligencję do wykrywania cyberataków. KGP odpowiedzialny za COT KSI oraz KGSG odpowiedzialny za COT IO/EES/ETIAS w ramach swoich struktur zbudowały zespoły monitorujące wykorzystywaną infrastrukturę teleinformatyczną. W KGSG został powołany Decyzją Komendanta Głównego SG Komitet do spraw Bezpieczeństwa Teleinformatycznego Straży Granicznej oraz Zespół Security Operations Center Straży Granicznej, który realizuje zadania wskazane w regulacjach ustawowych wykorzystując w tym celu komponenty budowanego, modernizowanego i rozwijanego od wielu lat Zintegrowanego Systemu Monitorowania, Reagowania i Ochrony przed incydentami bezpieczeństwa teleinformatycznego Straży Granicznej zapewniającego ochronę przed zagrożeniami z obszaru cyberprzestrzeni dla kluczowych systemów Straży Granicznej jak również dla systemów wielkoskalowych UE. Do zadań SOC SG należy poza obsługą incydentów, zarządzaniem nimi, również wymiana informacji z CSIRT-ami, a także odpowiednie reagowanie w sytuacji potencjalnego lub zaistniałego zagrożenia. Zapewnienie zgodności systemu zarządzania bezpieczeństwem systemów teleinformatycznych eksploatowanych w ramach COT KSI z normą PN-ISO/IEC 27001:2007, szacowanie ryzyk oraz projektowanie i koordynowanie bezpieczeństwa informacji w procesach ciągłości działania centralnych systemów teleinformatycznych spoczywa na dedykowanym zespole Biura Łączności i Informatyki KGP.

W resorcie spraw wewnętrznych i administracji powołani zostali Pełnomocnicy ds. Bezpieczeństwa Cyberprzestrzeni poszczególnych podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, odpowiadający między innymi za monitorowanie stanu bezpieczeństwa sieci i systemów teleinformatycznych, monitorowanie i gromadzenie dostępnych informacji o zagrożeniach cybernetycznych, szacowanie ryzyka w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa, opiniowania procedur reagowania na incydenty, inicjowanie i koordynowanie zadań w zakresie cyberbezpieczeństwa, w tym inicjowanie szkoleń i upowszechnianie wiedzy z zakresu bezpieczeństwa

cyberprzestrzeni, współpraca z organami i jednostkami organizacyjnymi podległymi Ministrowi SWiA i przez niego nadzorowanymi.

Ponadto w strukturze Ministerstwa Sprawiedliwości funkcjonuje Biuro Cyberbezpieczeństwa, którego rolą jest m.in. wykonywanie zadań zapewniających prawidłowe funkcjonowanie systemu ochrony cyberbezpieczeństwa w Ministerstwie Sprawiedliwości oraz jednostkach podległych Ministrowi Sprawiedliwości lub przez niego nadzorowanych, w tym wykrywanie i przeciwdziałanie zagrożeniom cyberbezpieczeństwa oraz monitorowanie i analiza stanu bezpieczeństwa informacji w cyberprzestrzeni Ministerstwa Sprawiedliwości. Działalność Biura Cyberbezpieczeństwa to także współpraca z sądami apelacyjnymi w zakresie realizacji zadań zdefiniowanych przez Zarządzenie Ministra Sprawiedliwości z dnia 20 listopada 2019 r. w sprawie powołania Zespołu do spraw Cyberbezpieczeństwa w sądach apelacyjnych. W wymiarze zewnętrznym Biuro współpracuje m.in. z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, prowadzonym przez Szefa Agencji Bezpieczeństwa Wewnętrznego.

5.4 Ramy organizacyjne

5.4.1 Zarządzanie Programem

Koordinację działań związanych ze strategicznym rozwojem i modernizacją Wielkoskalowych Systemów Informacyjnych UE po stronie krajowej prowadzi Pełnomocnik Rządu do spraw Wielkoskalowych Systemów Informacyjnych Unii Europejskiej ustanowiony Rozporządzeniem Rady Ministrów z dnia 10 listopada 2020 r. *w sprawie ustanowienia Pełnomocnika Rządu do spraw Wielkoskalowych Systemów Informacyjnych Unii Europejskiej* (Dz. U. poz. 2049). Odpowiada on w szczególności za koordynowanie działań organów administracji rządowej w zakresie:

- zapewnienia ich współpracy z Wielkoskalowymi Systemami Informacyjnymi UE SIS, VIS, Eurodac;
- zapewnienia wdrażania i przygotowania do współpracy z nowo powstającymi Wielkoskalowymi Systemami Informacyjnymi Unii Europejskiej EES, ETIAS, ECRIS-TCN oraz ich interoperacyjności.

Transformacja architektury Wielkoskalowych Systemów Informacyjnych UE wiąże się z modernizacją systemów krajowych oraz infrastruktury sieciowej, dlatego, w celu efektywnej realizacji tych zadań z inicjatywy Pełnomocnika Rządu ds. WSIUE, zarządzeniem nr 2 z dnia 13 stycznia 2021 r. Prezesa Rady Ministrów powołano Zespół do spraw Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi Unii Europejskiej, zwany dalej Zespołem, będący Radą Programu.

Głównymi zadaniami Zespołu są:

- przygotowywanie projektów dokumentów i rozstrzygnięć mających znaczenie dla Wielkoskalowych Systemów Informacyjnych Unii Europejskiej oraz ich Interoperacyjności w Rzeczypospolitej Polskiej, przedstawianych Prezesowi Rady Ministrów celem przedłożenia Radzie Ministrów;
- przygotowanie oraz przedstawienie do akceptacji Radzie Ministrów projektu MasterPlanu;
- opracowanie harmonogramu prac Zespołu;
- identyfikacja zadań oraz ustalenie, w celu zarekomendowania Radzie Ministrów, które organy administracji rządowej oraz podległe im jednostki organizacyjne lub przez nie nadzorowane będą realizowały zadania jako wiodące lub współpracujące w kwestiach związanych z Wielkoskalowymi Systemami Informacyjnymi Unii Europejskiej oraz ich Interoperacyjnością;
- przeprowadzenie szczegółowej analizy zadań administracji rządowej zmierzających do zapewnienia współpracy organów oraz podległych im jednostek organizacyjnych lub przez

nie nadzorowanych z Wielkoskalowymi Systemami Informacyjnymi Unii Europejskiej oraz ich Interoperacyjnością;

- przeprowadzenie analizy kosztów działań związanych z realizacją zadań administracji rządowej zmierzających do zapewnienia współpracy organów oraz podległych im jednostek organizacyjnych lub przez nie nadzorowanych, z Wielkoskalowymi Systemami Informacyjnymi Unii Europejskiej oraz ich Interoperacyjnością.

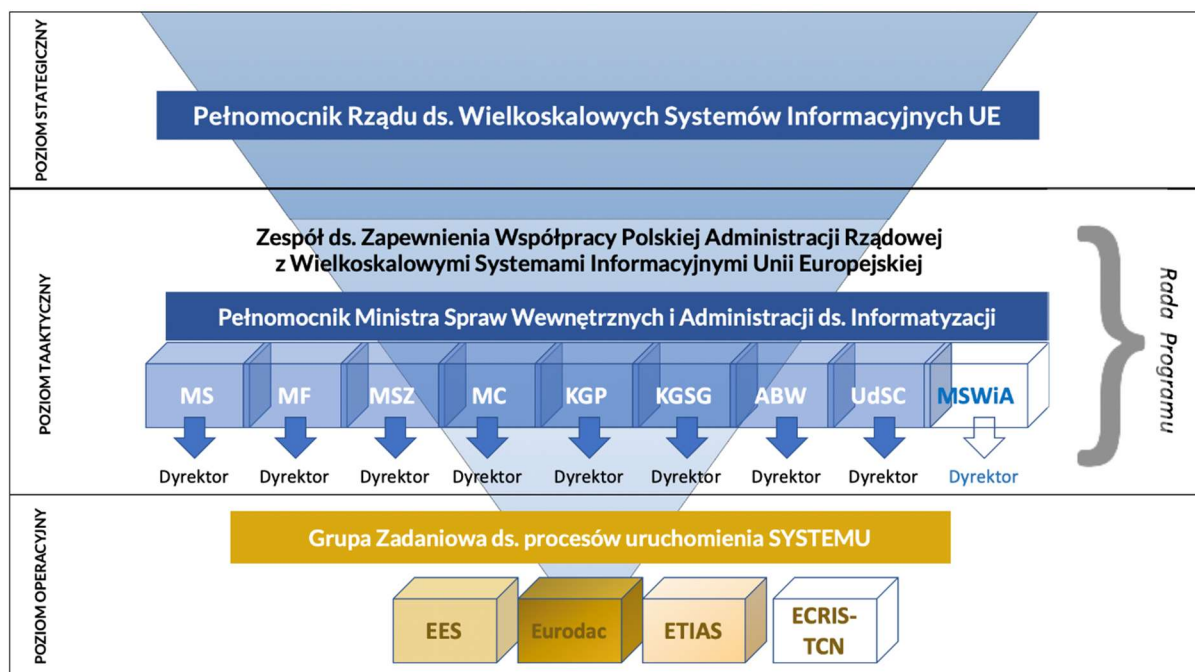
Pracami Zespołu kieruje Pełnomocnik Rządu ds. WSIUE jako Przewodniczący Rady Programu. Koordynuje on działania organów administracji rządowej w zakresie zapewnienia ich współpracy z Wielkoskalowymi Systemami Informacyjnymi Unii Europejskiej w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz Interoperacyjności między organami administracji rządowej a organami Unii Europejskiej. Rada Programu podejmuje decyzje na poziomie wykonawczym. Podejmowane są one przez delegowanych przez poszczególne ministerstwa i organy dyrektorów komórek merytorycznych dla realizacji zadań technologicznych. Operacyjnie pracami Rady Programu zarządza Pełnomocnik Ministra Spraw Wewnętrznych i Administracji ds. Informatyzacji. Pełnomocnika wspiera Wydział Wielkoskalowych Systemów Informatycznych UE Departamentu Teleinformatyki MSWiA.

Zgodnie ze standardami zarządzania projektami umożliwiającymi efektywne zarządzanie projektem, minimalizację ryzyka niepowodzeń oraz zapewniając przejrzystość procesu dla nadzoru nad procesem budowy i uruchamiania systemu zmieniono sposób zarządzania Programem i poszczególnymi projektami. Dzięki przyjętemu rozwiązaniu pojawiła się możliwość rozwiązywania na bieżąco pojawiających się problemów już na poziomie operacyjnym, a także możliwość, w sytuacji zaistnienia zagadnień wymagających decyzji politycznych ich eskalacji, za pośrednictwem Pełnomocnika Rządu ds. WSIUE, na poziom ministerialny.

Jednym z elementów zarządzania projektami jest powoływanie tzw. Grup Zadaniowych, których celem jest bardziej efektywne i merytoryczne podejście do poszczególnych zadań. Skutkuje to szybkim przekazywaniem na poziom Rady Programu pojawiających się, sprecyzowanych problemów.

Kwestie dotyczące poszczególnych systemów na poziomie roboczym są omawiane w ramach prac Grup Zadaniowych. Planowane jest powołanie Grup Zadaniowych do każdego systemu.

Opis struktury Zespołu przedstawia rysunek nr 3.



Rysunek 3. Diagram struktury zarządczej Programu

5.4.2 Interesariusze

Proces współpracy polskich instytucji z Wielkoskalowymi Systemami Informacyjnymi UE obejmuje szereg zadań, które można podzielić na dwa obszary:

- współpracę (w szczególności wymianę danych) z Wielkoskalowymi Systemami Informacyjnymi UE, którą prowadzą polskie instytucje zgodnie z zapisami ustawy o SIS i VIS.
- działania związane ze strategicznym rozwojem i modernizacją Wielkoskalowych Systemów Informacyjnych UE i odwzorowaniem ich w systemach krajowych.

Tabela 1. Jednostki administracji współpracujące z Wielkoskalowymi Systemami Informacyjnymi UE za pośrednictwem interfejsów do własnych systemów

Działania strategiczne	Działania operacyjne	System
Komendant Główny Policji	Policja	<ul style="list-style-type: none"> Krajowy System Informacyjny Policji – KSIP System Poszukiwawczy Policji – SPP System Teleinformatyczny Biura SIRENE – STBS II SI Pojazd – aplikacja OR-COT KSI WWW SIS AFIS WWW VIS Aplikacja Reja 24 – COT KSI
Komendant Główny Straży Granicznej	Straż Graniczna	Centralne Systemy Informatyczne SG
Szef Urzędu do Spraw Cudzoziemców	Urząd do Spraw Cudzoziemców	Pobyt 3 w tym KSK
Szef Agencji Wywiadu	Agencja Wywiadu	System Udostępniania Danych – SUD
Minister Sprawiedliwości	Sądy	SIS2-SAD
Minister Spraw Zagranicznych	Konsulowie, MSZ	WIZA KONSUL
Minister Obrony Narodowej	Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego	System Udostępniania Danych – SUD
Szef Centralnego Biura Antykorupcyjnego	Centralne Biuro Antykorupcyjne	System Analiz Rejestrów Państwowych – SARP
Prokuratura Krajowa/Prokurator Krajowy	Prokuratury	PROK-SYS
Minister właściwy do spraw wewnętrznych	Ministerstwo Spraw Wewnętrznych i Administracji	<ul style="list-style-type: none"> Centralna Ewidencja Pojazdów i Kierowców – CEPiK Rejestr Dowodów Osobistych/System Rejestrów Państwowych – RDO-SRP

Źródło: Opracowanie własne

Tabela 2. Systemy będące w fazie projektowania lub planowania współpracujące z Wielkoskalowymi Systemami Informacyjnymi UE

Instytucja	Nazwa systemu	Powiązanie z systemem UE
Ministerstwo Sprawiedliwości	ST KRK	ECRIS-TCN
KGSG	KSI ETIAS	ETIAS
KGSG	KSI EES	EES
KGSG	CSI SG	Eurodac
UdSC	Mikroserwisy Eurodac SI Pobyt	Eurodac
UdSC	KSK 2.0	SIS, VIS, EES, ETIAS, Eurodac

Źródło: Opracowanie własne

5.4.3 Centralny Organ Techniczny KSI – Komendant Główny Policji

Krajowy System Informatyczny (KSI), zgodnie z treścią art. 2 pkt 11 ustawy o SIS i VIS, stanowi zespół współpracujących ze sobą urządzeń, procedur przetwarzania informacji i narzędzi programowych (oprogramowania) zastosowanych w celu przetwarzania danych oraz infrastrukturę telekomunikacyjną, umożliwiające organom administracji publicznej i organom wymiaru sprawiedliwości przetwarzanie danych gromadzonych w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Organem odpowiedzialnym za eksploatację techniczną oraz utrzymanie KSI jest Centralny Organ Techniczny (COT KSI), którego funkcję, zgodnie z zapisami art. 2 pkt 3 przywołanej wyżej ustawy o SIS i VIS, pełni Komendant Główny Policji.

Zgodnie z art. 26–34 ustawy o SIS i VIS organem odpowiedzialnym za system krajowy N.SIS jest COT KSI. Do jego zadań należy:

- utworzenie, uruchomienie, eksploatacja techniczna oraz utrzymanie KSI;
- zapewnienie sprawnego działania i bezpieczeństwa SIS w ramach systemu krajowego N.SIS.

Zadania COT KSI realizuje:

- Biuro Łączności i Informatyki Komendy Głównej Policji w zakresie utworzenia, uruchomienia, eksploatacji systemów teleinformatycznych oraz zapewnienia bezpieczeństwa przetwarzanych danych;
- Biuro Wywiadu i Informacji Kryminalnych Komendy Głównej Policji w zakresie administrowania danymi.

5.4.4 Centralny Organ Techniczny IO/EES/ETIAS – Komendant Główny Straży Granicznej

Komendant Główny Straży Granicznej pełni rolę Centralnego Organu Technicznego IO/EES/ETIAS (COT IO/EES/ETIAS). Głównymi zadaniami COT IO/EES/ETIAS są przede wszystkim integracja istniejącej krajowej infrastruktury granicznej oraz jej połączenie z jednolitym interfejsem krajowym systemów EES/ETIAS (tzw. National Uniform Interface – NUI), a także podłączenie do narzędzi Interoperacyjności. Ponadto COT IO/EES/ETIAS organizuje, zarządza, utrzymuje krajową infrastrukturę graniczną, w tym gromadzi i przetwarza dane EES/ETIAS, a także dane przetwarzane w poszczególnych narzędziach Interoperacyjności, w tym prowadzi działalność sprawozdawczą, wymaganą przez Komisję Europejską. Dodatkowo zapewnia podłączenie Centralnego Punktu Dostępu do krajowej infrastruktury granicznej, zapewnia opracowanie, rozwój i utrzymanie interfejsów programowych oraz teleinformatycznych umożliwiających integrację systemów innych użytkowników instytucjonalnych i indywidualnych.

W ramach prowadzonych prac są rozwijane i utrzymywane aplikacje WWW EES oraz WWWETIAS. Do zadań COT IO/EES/ETIAS należy również zapewnienie wydajnej, bezpiecznej i dostępnej infrastruktury służącej do przeprowadzenia kontroli granicznej, z którą powiązane jest właściwe i efektywne działanie systemów EES i ETIAS, a także właściwe działanie krajowych komponentów Interoperacyjności, dostępność i prawidłowa komunikacja z centralnymi narzędziami Interoperacyjności, udostępnienie rozwiązań umożliwiających dokonywanie zapytań w ESP. COT IO/EES/ETIAS jest również odpowiedzialny za wsparcie procesów systemowych/technicznych związanych z zarządzaniem „żółtymi linkami”, a także przygotowanie/dostosowanie do wymogów unijnych rozwiązań komunikacyjnych (narzędzie do komunikacji pomiędzy państwami członkowskimi) w kontekście z zarządzania „żółtymi linkami”.

Zadania COT IO/EES/ETIAS realizuje/będzie realizować:

- Biuro Łączności i Informatyki Komendy Głównej Straży Granicznej w zakresie utworzenia, uruchomienia, eksploatacji systemów teleinformatycznych oraz zapewnienia bezpieczeństwa przetwarzanych danych;
- Zarząd Graniczny Komendy Głównej Straży Granicznej oraz Zarząd do Spraw Cudzoziemców Komendy Głównej Straży Granicznej w zakresie administrowania danymi, zarządzania użytkownikami.

5.4.5 Biuro SIRENE

Biuro SIRENE działa w strukturze Policji. Podstawowym zadaniem Biura SIRENE jest wymiana informacji uzupełniających (zgodnie z wytycznymi zawartymi w Podręczniku SIRENE), niezbędnych przy wprowadzaniu wpisów i w celu umożliwienia podjęcia odpowiednich działań w przypadku trafienia w SIS, (gdy w wyniku sprawdzenia w SIS odnaleziono osoby lub przedmioty wprowadzone do systemu).

Biuro SIRENE jest jedynym punktem kontaktowym działającym przez całą dobę każdy dzień w roku – 365/7/24 – właściwym w zakresie wymiany informacji uzupełniających do wpisów wprowadzanych do Systemu Informacyjnego Schengen.

Biura SIRENE funkcjonują w każdym z państw Strefy Schengen, dzięki czemu organy i służby uprawnione do przetwarzania danych SIS mają stały, bezpośredni kontakt z organami państw całego obszaru Schengen.

Wymiana informacji odbywa się poprzez wymianę elektronicznych formularzy. Zgodnie z decyzją Ministra Spraw Wewnętrznych i Administracji z dnia 9 sierpnia 2004 r. zadania Biura SIRENE w Polsce realizuje komórka organizacyjna Biura Międzynarodowej Współpracy Policji Komendy Głównej Policji. Polskie Biuro SIRENE stało się w pełni operacyjne 10 września 2007 r. Służba dyżurna Biura SIRENE PL pełniona jest wspólnie z funkcjonariuszami Straży Granicznej. Obecnie w Biurze SIRENE działa STBS – System Informacyjny Biura SIRENE, który stanowi zintegrowany system zarządzania i obiegu dokumentów, w tym korespondencji krajowej i zagranicznej również dla Krajowego Biura Interpolu oraz dla Jednostki Krajowej Europolu. System workflow dla Biura SIRENE został odpowiednio zmodernizowany dla projektu *SIS Recast* oraz będzie wymagał opracowania nowych rozwiązań teleinformatycznych, które będą odpowiadały na wyzwania pozostałych projektów istniejących systemów wielkoskalowych UE, nowo budowanych systemów wielkoskalowych UE oraz narzędzi ich interoperacyjności. Ponadto z uwagi na wyeksploatowanie, muszą zostać wymienione wszystkie stanowiska dostępne wraz z wyposażeniem (jednostka centralna, monitory, klawiatury, myszki, czytniki, oprogramowanie) używane do obsługi STBS.

5.4.6 Krajowy Punkt Dostępu do systemu Eurodac – Komendant Główny Policji

Każde państwo członkowskie posiada jeden krajowy punkt dostępu do systemu Eurodac. Do zadań krajowego punktu dostępu do systemu Eurodac należy:

- przysyłanie do systemu Eurodac danych daktyloskopijnych wraz z właściwymi numerami referencyjnymi zgodnie z art. 24 ust. 1 *rozporządzenia (UE) 603/2013*;
- weryfikowanie wyników porównania zgodnie z art. 25 ust. 4 *rozporządzenia (UE) 603/2013*;
- komunikowanie się z systemem Eurodac zgodnie z art. 26 *rozporządzenia (UE) 603/2013*;
- przekazywanie wyników porównania danych daktyloskopijnych z danymi Eurodac właściwym organom.

Powyższe zadania Komendant Główny Policji wykonuje przy pomocy Centralnego Laboratorium Kryminalistycznego Policji (CLKP).

Tryb przekazywania wniosków o porównanie danych daktyloskopijnych z danymi przechowywanymi w systemie Eurodac określa Zarządzenie nr 23 Komendanta Głównego Policji z dnia 16 lipca 2015 r. w sprawie trybu przysyłania wniosków o porównanie danych daktyloskopijnych z danymi Eurodac (Dz. Urz. KGP z 2015 r. poz. 56).

Zgodnie z Zarządzeniem nr 28 Komendanta Głównego Policji z dnia 11 sierpnia 2020 w sprawie zbiorów danych daktyloskopijnych (Dz. Urz. KGP z 2020 r. poz. 44) Dyrektor CLKP wykonuje zadania administratora danych i informacji zgromadzonych w zbiorach danych daktyloskopijnych, a także do nadzoru nad realizacją zadań Krajowego Punktu Dostępu do systemu Eurodac.

Zgodnie z art. 21h ust. 1 *ustawy o Policji*, Komendant Główny Policji prowadzi zbiory danych daktyloskopijnych, których jest administratorem w rozumieniu przepisów o ochronie danych osobowych:

- Centralną Registraturę Daktyloskopijną, w której są gromadzone karty daktyloskopijne i chejroskopijne zawierające odfitki linii papilarnych osób;
- zbiór automatycznie przetwarzający dane daktyloskopijne, w którym są przetwarzane informacje, w tym dane osobowe, o odfitkach linii papilarnych osób, niezidentyfikowanych śladach linii papilarnych z miejsc przestępstw oraz śladach linii papilarnych, które mogą pochodzić od osób zaginionych (AFIS).

W zbiorach danych daktyloskopijnych przetwarzane są m.in. informacje dotyczące cudzoziemców w trakcie procedury o udzielenie ochrony międzynarodowej. Biuro Łączności i Informatyki KGP odpowiedzialne jest za utworzenie, uruchomienie, utrzymanie AFIS i jego interfejsów (w tym Eurodac) oraz zapewnienie bezpieczeństwa przetwarzanych danych.

5.4.7 Krajowa Jednostka ds. EES – Komendant Główny Straży Granicznej

Komendant Główny Straży Granicznej pełni funkcję Krajowej Jednostki ds. EES oraz wyznacza komórkę organizacyjną Komendy Głównej Straży Granicznej realizującą jej zadania. W ramach Krajowej Jednostki ds. EES funkcjonuje Centralny Punkt Dostępu.

Głównymi zadaniami Krajowej Jednostki ds. EES jest m.in. pełnienie roli centralnego punktu dostępu, prowadzenie ewidencji upoważnień do dostępu do KSI EES oraz przetwarzania danych poprzez KSI EES dla użytkowników indywidualnych oraz osób posiadających upoważnienia w ramach centralnego punktu dostępu. Zarządzanie dostępem użytkowników indywidualnych, w tym nadawanie i cofanie uprawnień do dostępu do KSI EES, przetwarzanie danych poprzez KSI EES, prowadzenie ewidencji uprawnień tych użytkowników, monitorowanie jakości danych oraz czasu trwania odpraw granicznych pod kątem spełniania wymogów związanych z właściwym działaniem EES i efektywnymi procedurami odpraw granicznych, przygotowywanie oraz przekazywanie do Komisji Europejskiej i agencji eu-LISA informacji z zakresu funkcjonowania oraz wykorzystania EES.

Ponadto Krajowa Jednostka ds. EES odpowiedzialna będzie za przeprowadzanie konsultacji z odpowiedzialnym państwem członkowskim w zakresie prawidłowości, kompletności oraz zgodności z prawem przetwarzania danych w EES, a także dokonywanie sprostowania, uzupełniania, usuwania lub ograniczania przetwarzania danych osobowych, w przypadku gdy dane zarejestrowane w EES są niezgodne ze stanem faktycznym, niekompletne lub zostały zarejestrowane niezgodnie z prawem.

5.4.8 Jednostka Krajowa ETIAS – Komendant Główny Straży Granicznej

Zgodnie z rozporządzeniem (UE) 2018/1240, każde państwo członkowskie wyznacza właściwy organ jako Jednostkę Krajową ETIAS. Komendant Główny Straży Granicznej będzie odpowiadał za organizację, funkcjonowanie, zarządzanie i utrzymywanie Jednostki Krajowej ETIAS oraz wyznacza komórkę organizacyjną Komendy Głównej Straży Granicznej realizującą jej zadania, tj. Zarząd do Spraw Cudzoziemców Komendy Głównej Straży Granicznej.

Jednostka Krajowa ETIAS w szczególności odpowiadać będzie za analizowanie i podejmowanie decyzji w sprawie wniosków o zezwolenie na podróż w przypadkach, w których automatyczny proces przetwarzania wniosków wygenerował trafienie, a jednostka centralna ETIAS zainicjowała ręczne przetwarzanie wniosku, podejmowanie decyzji o wydaniu zezwolenia na podróż o ograniczonej ważności terytorialnej oraz zapewnienie koordynacji działań z innymi jednostkami krajowymi ETIAS i z Europolem w odniesieniu do próśb o konsultacje. Unieważnianie i cofanie zezwoleń na podróż, a także zarządzanie krajowymi wpisami na liście ostrzegawczej ETIAS. Odpowiadać będzie również za ręczną weryfikację trafień na liście ostrzegawczej ETIAS, wywołanych zautomatyzowanymi zapytaniami dokonywanymi przez VIS oraz za podejmowanie działań w przypadku takich trafień oraz realizację zadań centralnego punktu dostępu ETIAS związanego z pośrednim dostępem wyznaczonych organów do systemu centralnego ETIAS do celów ochrony porządku publicznego.

Uruchomienie systemu ETIAS oraz prowadzenie wyżej wymienionych czynności przez Jednostkę Krajową ETIAS, ma na celu zwiększenie bezpieczeństwa wewnętrznego oraz poprawę skuteczności ochrony granic zewnętrznych Unii Europejskiej poprzez zagwarantowanie możliwości wyprzedzającej oceny podróży, pod kątem występowania ryzyka dla bezpieczeństwa, ryzyka nielegalnej imigracji lub wysokiego ryzyka epidemiologicznego dla PCz, bezpośrednio przed ich przybyciem na przejście graniczne, zlokalizowane na granicy zewnętrznej. Wydane w stosownych przypadkach przez Jednostkę Krajową ETIAS, ważne zezwolenie na podróż stanowi zatem potwierdzenie, że nie istnieją faktyczne wskazania, ani uzasadnione powody, by uznać, że obecność osoby na terytorium państw członkowskich stwarza takie ryzyko.

Skuteczna realizacja nowych zadań nałożonych na Straż Graniczną jako organu właściwego tj. Jednostkę Krajową ETIAS, jest możliwa tylko i wyłącznie poprzez wdrożenie zapisów wskazanego rozporządzenia (UE) 2018/1240 do krajowego porządku prawnego, co umożliwi utworzenie, organizację oraz wyposażenie Jednostki Krajowej ETIAS, stworzenie krajowego komponentu informatycznego ETIAS, jak również dostosowanie krajowych rozwiązań organizacyjnych, proceduralnych i technicznych do wymiany informacji pomiędzy Jednostką Centralną ETIAS, Europolem i Jednostką Krajową ETIAS oraz właściwymi krajowymi organami.

5.4.9 Organ centralny ECRIS-TCN – Biuro Informacyjne Krajowego Rejestru Karnego w Ministerstwie Sprawiedliwości

Wchodzące w skład Ministerstwa Sprawiedliwości Biuro Informacyjne Krajowego Rejestru Karnego pełni w Polsce funkcję organu centralnego ECRIS wyznaczonego do celów wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi. BI KRK będzie pełniło również funkcję polskiego organu centralnego ECRIS-TCN.

Jako organ centralny ECRIS-TCN BI KRK w szczególności będzie odpowiedzialne za tworzenie i aktualizację w systemie ECRIS-TCN wpisów w odniesieniu do każdego skazanego przez polski sąd obywatela państwa trzeciego, bezpaństwowca lub osoby, której obywatelstwo nie jest znane.

Z uwagi na to, że ww. wpisy będą obejmowały oprócz danych alfanumerycznych również dane daktyloskopijne, na BI KRK zostanie nałożony nowy obowiązek pozyskiwania danych o odciskach linii papilarnych z bazy AFIS w celu zamieszczenia ich w systemie ECRIS-TCN.

Ponadto zadaniem BI KRK będzie wysyłanie zapytań do systemu ECRIS-TCN w przypadku wystąpienia o informację z rejestru karnego dotyczącą obywatela państwa trzeciego, bezpaństwowca lub osoby, której obywatelstwo nie jest znane, a w przypadku trafienia w systemie ECRIS-TCN - występowanie z zapytaniem o udzielenie informacji o osobie do organów centralnych państw członkowskich Unii Europejskiej, które posiadają informacje zawarte w rejestrach karnych na temat danej osoby. BI KRK będzie również wykonywało zadania wynikające z rozporządzenia (WE) 767/2008, rozporządzenia (UE) 2018/1240 i rozporządzenia (UE) 2024/1356 w procedurze weryfikacji w rejestrze karnym traień w systemie ECRIS-TCN.

BI KRK będzie rozpatrywało również wnioski obywateli państw trzecich (bezpaństwowców, osób, których obywatelstwo jest nieznane) dotyczące praw dostępu do danych osobowych, do sprostowania, usunięcia oraz do ograniczenia przetwarzania danych osobowych zgromadzonych w systemie ECRIS-TCN. Ponadto, BI KRK, na wniosek innego państwa członkowskiego, będzie odpowiedzialne za weryfikację prawidłowości danych zgromadzonych w ECRIS-TCN oraz zgodności ich przetwarzania z prawem w przypadku gdy państwem skazującym obywatela państwa trzeciego (bezpaństwowca lub osoby, której obywatelstwo jest nieznane) jest RP.

6 Koncepcja dostosowania polskiej administracji do zmian

6.1 Cele przedsięwzięcia

Celem strategicznym Programu, jako przedsięwzięcia zarządzanego w spójny i skoordynowany sposób jest pełne wdrożenie do krajowego systemu współpracy instytucjonalnej Strefy Schengen zmian technicznych, organizacyjnych i prawnych w obszarze systemów wielkoskalowych UE w przestrzeni wolności, bezpieczeństwa i sprawiedliwości UE, w określonych ramach czasowych i merytorycznych.

Przekłada się to na następujące **cele operacyjne** dotyczące systemów krajowych współdziałających z systemami wielkoskalowymi UE:

- A. Zapewnienie współpracy polskich instytucji ze zmodernizowanym systemem SIS zgodnie z rozporządzeniem (UE) 2018/1860, rozporządzeniem (UE) 2018/1861 oraz rozporządzeniem (UE) 2018/1862;
- B. Zapewnienie współpracy polskich instytucji ze zmodernizowanym systemem VIS zgodnie z rozporządzeniem (UE) 2021/1133 oraz rozporządzeniem (UE) 2021/1134;
- C. Zapewnienie współpracy polskich instytucji do zmodernizowanego systemu Eurodac zgodnie z rozporządzeniem (UE) 2024/1358;
- D. Zapewnienie współpracy polskich instytucji z systemem EES zgodnie z rozporządzeniem (UE) 2017/2226 oraz rozporządzeniem (UE) 2017/2225;
- E. Zapewnienie współpracy polskich instytucji z systemem ETIAS zgodnie z rozporządzeniem (UE) 2018/1240;
- F. Wdrożenie w systemach krajowych niezbędnych funkcji do integracji ST KRK z systemem ECRIS-TCN, zgodnie z rozporządzeniem (UE) 2019/816;
- G. Wdrożenie narzędzi Interoperacyjności Wielkoskalowych Systemów Informacyjnych UE, zgodnie z rozporządzeniem (UE) 2019/817 oraz rozporządzeniem (UE) 2019/818.

6.2 Potwierdzenie osiągnięcia celów

W przypadku celów operacyjnych A – G tj. modyfikacji istniejących lub wdrożenia nowych systemów informacyjnych, potwierdzeniem osiągnięcia danego **celu** jest pozytywny wynik testów danego systemu, realizowanych przez jednostki krajowe wraz z Agencją eu-LISA.

Tabela 3. Parametry osiągnięcia celów

	Cel	Opis
A	Skuteczne wdrożenie na gruncie krajowym nowych funkcjonalności SIS zgodnie z rozporządzeniem (UE) 2018/1860, rozporządzeniem (UE) 2018/1861 oraz rozporządzeniem (UE) 2018/1862	<ul style="list-style-type: none">• Dostosowany N.SIS II/KSI oraz system dla Biura SIRENE• Wykonane niezbędne modyfikacje w systemach dziedzicznych poszczególnych instytucji lub wdrożone nowe rozwiązania systemowe• Dostosowana aplikacja WWW SIS• Pozytywny wynik testów z UE
B	Realizacja i uruchomienie dostępu polskich instytucji do zmodernizowanego systemu VIS zgodnie z rozporządzeniem (UE) 2021/1133 oraz rozporządzeniem (UE) 2021/1134	<ul style="list-style-type: none">• Wykonane niezbędne modyfikacje w systemach dziedzicznych poszczególnych instytucji lub wdrożone nowe rozwiązania systemowe• Dostosowana aplikacja WWW VIS• Dostosowanie przepisów prawnych• Pozytywny wynik testów z UE

	Cel	Opis
C	Realizacja i uruchomienie dostępu polskich instytucji do zmodernizowanego systemu Eurodac	<ul style="list-style-type: none"> Dostosowanie interfejsu Eurodac oraz systemu AFIS Wykonane niezbędne modyfikacje w systemach dziedzicznych poszczególnych instytucji lub wdrożone nowe rozwiązania systemowe Dostosowanie przepisów prawnych Pozytywny wynik testów z UE
D	Dołączenie polskich instytucji do systemu EES zgodnie z rozporządzeniem (UE) 2017/2226 i rozporządzeniem (UE) 2017/2225	<ul style="list-style-type: none"> Uruchomienie krajowego komponentu EES Zapewnienie dostępu do danych EES właściwym organom i instytucjom, poprzez interfejs krajowy oraz aplikację WWW <ul style="list-style-type: none"> Wykonanie niezbędnych modyfikacji w istniejących systemach Pozytywny wynik testów z UE Wejście w życie ustawy o udziale RP w Systemie Wjazdu/Wyjazdu wraz z aktami wykonawczymi
E	Dołączenie polskich instytucji do systemu ETIAS zgodnie z rozporządzeniem (UE) 2018/1240	<ul style="list-style-type: none"> Uruchomienie krajowego komponentu ETIAS (ETIAS NU), Wdrożenie wymiany informacji z Europolem, ETIAS CU (Frontex) ETIAS NU innych PCz UE oraz JKE z krajowymi organami i instytucjami. Zapewnienie dostępu do danych ETIAS właściwym organom i instytucjom, w tym zapewnienie komunikacji z Biurem SIRENE oraz JKE. Wejście w życie ustawy o udziale RP w Systemie ETIAS wraz z aktami wykonawczymi Pozytywny wynik testów z UE
F	Wdrożenie w systemach krajowych niezbędnych funkcji do integracji ST KRK z systemem ECRIS-TCN zgodnie z rozporządzeniem 2019/816;	<ul style="list-style-type: none"> Wdrożenie ECRIS-RI-INT oraz ECRIS-TCN IS narzędzia pośredniczącego w integracji ST KRK z centralnym systemem ECRIS-TCN i narzędziami interoperacyjności Uruchomienie integracji ST KRK z ECIRS-TCN <ol style="list-style-type: none"> gotowość do przesyłania danych alfanumerycznych gotowość do przesyłania danych biometrycznych zapewnienie wymiany informacji pomiędzy systemami MS a CLKP (AFIS) w celu realizacji 1b Pozytywny wynik testów z UE
G	Wdrożenie w systemach krajowych niezbędnych funkcji do integracji z narzędziami Interoperacyjności zgodnie z rozporządzeniem (UE) 2019/817 oraz rozporządzeniem (UE) 2019/818	<ul style="list-style-type: none"> Uruchomienie krajowego komponentu ESP Zapewnienie dostępu do danych wielkoskalowych systemów informacyjnych UE wchodzących w skład IO właściwym organom i instytucjom poprzez interfejs krajowy ESP Dostosowanie interfejsów krajowych wielkoskalowych systemów informacyjnych UE do nowych wersji ICD zgodnych z IO Wykonane niezbędne modyfikacje w systemach dziedzicznych poszczególnych instytucji lub wdrożenie nowych rozwiązań systemowych Wdrożenie rozwiązania informatycznego umożliwiającego określanie rodzajów powiązań pomiędzy tożsamościami, w tym tzw. „żółtych linków” Pozytywny wynik testów z UE

6.3 Projekty do realizacji

W ramach przedsięwzięcia będą realizowane następujące projekty:

- A. Modernizacja systemu SIS II (jednostka odpowiedzialna KGP);
- B. Modernizacja VIS systemu (jednostka odpowiedzialna KGP);
- C. Modernizacja Eurodac systemu (jednostka odpowiedzialna KGP);
- D. Wdrożenie systemu EES (jednostka odpowiedzialna KGSG);
- E. Wdrożenie systemu ETIAS (jednostka odpowiedzialna KGSG);
- F. Wdrożenie systemu ECRIS-TCN (jednostka odpowiedzialna MS);
- G. Wdrożenie narzędzi Interoperacyjności Systemów (jednostka odpowiedzialna KGSG);
- H. Dostosowanie przepisów prawnych systemu EES (jednostka odpowiedzialna KGSG);
- I. Dostosowanie przepisów prawnych systemu ETIAS (jednostka odpowiedzialna KGSG);
- J. Dostosowanie przepisów prawnych systemu VIS (na dzień powstania niniejszego dokumentu brak wyznaczonej jednostki odpowiedzialnej)
- K. Dostosowanie przepisów prawnych systemu Eurodac (jednostka odpowiedzialna KGP);
- L. Modernizacja infrastruktury TESTA-ng.

Lista ta może zostać zmodyfikowana (w szczególności poszerzona) o nowe projekty, których potrzeba realizacji uwidoczni się w trakcie realizacji przedsięwzięcia.

6.4 Zakres zmian prawnych

Zgodnie z potrzebą adekwatnego dostosowania przepisów krajowych zakres zmian prawnych będzie obejmował:

- nowelizację *ustawy o SIS i VIS* oraz odpowiednich przepisów z innych ustaw oraz rozporządzeń w zakresie zmian dot. SIS Recast - nowelizacja ww. ustawy weszła w życie w dn.7 marca 2023 r.
- ponowną nowelizację *ustawy o SIS i VIS* w zakresie zmian dot. EES i ETIAS;
- nowelizacja *ustawy o Krajowym Rejestrze Karnym* wraz ze zmianą innych ustaw w zakresie ECRIS-TCN;
- uchwalenie odrębnych ustaw dla każdego z systemów: EES, ETIAS (wraz z KRC), Interoperacyjności;
- nowelizację przepisów dot. Eurodac; oraz
- nowelizację przepisów dot. VIS w szczególności ponowną nowelizację *ustawy o SIS i VIS* w zakresie zmian dot. VIS (*VIS Revised*).

Prowadzenie procesu legislacyjnego ustaw oraz krajowych aktów wykonawczych odbywa się w MSWiA (w zakresie ECRIS-TCN w MS) a gestorzy i użytkownicy poszczególnych systemów zaangażowani są w tworzenie projektów ww. przepisów. Wszystkie instytucje uprawnione do korzystania z Wielkoskalowych Systemów Informacyjnych UE dostosowują przepisy i wypracowują procedury związane z wszelkimi aspektami odnoszącymi się do korzystania z systemów.

7 Szczegółowy opis projektów

7.1 PROJEKT 1: Modernizacja systemu SIS II (SIS Recast)

Koordinator: Komenda Główna Policji.

Uczestnicy: organy i służby uprawnione do dostępu do SIS II, wymienione w art. 3 i 4 *ustawy o SIS i VIS* oraz nowe podmioty których dostęp wynika z nowo przyjętego pakietu rozporządzeń (art. 44–47 *rozporządzenia (UE) 2018/1862* i art. 34 *rozporządzenia (UE) 2018/1861*) oraz organy niewymienione w ustawie, które muszą otrzymać uprawnienia dostępu do danych SIS w związku z regulacjami art. 44–47 *rozporządzenia (UE) 2018/1862* a także Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Zapewnienie współpracy polskich instytucji ze zmodernizowanym systemem SIS II zgodnie z *rozporządzeniem (UE) 2018/1860*, *rozporządzeniem (UE) 2018/1861* oraz *rozporządzeniem (UE) 2018/1862*.

Wdrożenie nowej wersji systemu SIS nastąpiło w dniu 7 marca 2023 r.

Zrealizowano większość zadań nałożonych na Kierownika Projektu ds. modernizacji systemu SIS II⁶.

Do realizacji pozostał zakup i budowa przez Komendę Główną Policji Systemu Wymiany Informacji Międzynarodowych i Krajowych.

⁶ MasterPlan w wersji 2.0 nie zawiera szczegółowego opisu zrealizowanych zadań zakończonego projektu modernizacji systemu SIS II widniejących w wersji 1.2 ani głównych ryzyk w tym projekcie.

7.2 PROJEKT 2: Modernizacja systemu VIS (VIS Revised)

Koordynator: Komenda Główna Policji.

Uczestnicy: organy i służby uprawnione do dostępu do VIS, wymienione w art. 5–7 ustawy o SIS i VIS a także Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Zapewnienie współpracy polskich instytucji ze zmodernizowanym systemem VIS zgodnie z rozporządzeniem (UE) 2021/1133 oraz rozporządzeniem (UE) 2021/1134.

Zakłada się, że uruchomienie zmodernizowanego VIS nastąpi po pełnej implementacji komponentów interoperacyjności, czyli najwcześniej w 2026 r.

Tabela 4. Zakres projektu Modernizacja systemu VIS

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01VIS	Przygotowanie specyfikacji interfejsu KSI dla Użytkowników Instytucjonalnych (UI)	KGP	12.2025 r.
02VIS	Opracowanie regulacji prawnych: ustawy i akty wykonawcze do ustaw	MSWiA, wszyscy użytkownicy VIS oraz Prezes UODO	12.2025 r.
03VIS	Opracowanie regulacji prawnych: przepisy wewnętrzne/procedury.	Wszyscy użytkownicy VIS	06.2026 r.
04VIS	Dostosowanie systemu KSI do obsługi nowego interfejsu krajowego oraz interfejsu systemu centralnego VIS	KGP	12.2025 r. (test)/06.2026 r. (produkcja)
05VIS	Dostosowanie aplikacji WWW VIS do najnowszej dostępnej wersji ICD w tym m.in. w celu realizacji zadania w trybie pośrednim poprzez CPD	KGP	12.2025 r. (test)/06.2026 r. (produkcja)
06VIS	Dostosowanie Systemów Centralnych UI do współpracy z KSI w zakresie zmodernizowanego VIS	UI	I połowa 2026 r.
07VIS	Przeprowadzenie testów KSI w zakresie współpracy z C.VIS	KGP	I połowa 2026 r.
08VIS	Przeprowadzenie testów Systemów Centralnych UI z KSI i aplikacji WWW VIS	KGP, UI, UIIn	I połowa 2026 r.
09VIS	Gotowość Systemów Centralnych UI do pełnej współpracy ze zmodernizowanym VIS (środowisko produkcyjne).	UI	I połowa 2026 r.
10VIS	Infrastruktura komunikacji krajowej pomiędzy COW (albo organami wizowymi) a centralnymi jednostkami ETIAS, EES, ECRIS-TCN i Biurem SIRENE	MSWiA, wszyscy użytkownicy VIS i podmioty odpowiedzialne za wdrożenie poszczególnych projektów systemów UE – KGP, KGSG, UdSC (COW), MS	I połowa 2026 r.

11VIS	Dostosowanie narzędzia audytowo-statystycznego do VIS Revised	KGP	I połowa 2026 r.
12VIS	Dostosowanie PKI KSI w tym Panelu administratora do zmian w VIS Revised	KGP	I połowa 2026 r.
13VIS	Szkolenia użytkowników	KGP, wszyscy użytkownicy	I połowa 2026 r.
14VIS	Kampania informacyjna	MSZ, KGSG, wojewodowie	2026 r.
15VIS	Interoperacyjność EES/ETIAS-VIS Dostęp do EES i ETIAS poprzez VIS zgodnie z rozporządzeniem (UE) 2017/2226 oraz rozporządzeniem (UE) 2018/1240	KGP we współpracy z KGSG oraz organami wizowymi	2026 r.
16VIS	Przeprowadzenie testów infrastruktury sprzętowo-programowej w zakresie cyberbezpieczeństwa.	KGP	I połowa 2026 r.

Tabela 5. Główne ryzyka w projekcie Modernizacja systemu VIS

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Zarządcze					
1	Problemy z koordynacją wdrażania (obszar zarządzania – ze względu na zaangażowanie w projekt różnych instytucji niezbędna jest koordynacja na szczeblu krajowym)	Zespół ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE	średnie	duży	Bieżące monitorowanie.
2	Zmiany w zespole odpowiedzialnym za zarządzanie projektem	KGP	średnie	średni	Bieżące monitorowanie.
Finansowe					
3	Niedoszacowanie wartości projektu	KGP, UI	duże	duży	Bieżące monitorowanie kolejnych etapów szacowania wartości projektu.
4	Brak środków w budżecie Błłil KGP na zawarte umowy, w ramach których	KGP	duże	duży	Bieżące monitorowanie, zapewnienie środków z innych źródeł.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
	realizowane będą zadania projektu				
5	Brak funduszy w ramach przyznanego budżetu państwowego	MSWiA (jako instytucja koordynująca) MF KGP, (jako instytucja wdrażająca) Właściwe instytucje uczestniczące	duże	duży	Bieżące monitorowanie sytuacji; Przekazanie środków z funduszy celowych; Monitorowanie sprawnego uruchomienia środków na poziomie krajowych, nadanie najwyższego priorytetu w Programach Krajowych współfinansowanych ze środków unijnych (nowa perspektywa finansowa). Eskalowanie na wyższy poziom
Organizacyjno-prawne					
6	Przewlekłość procesu legislacyjnego po stronie UE	Zespół ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE	duże	duży	Bieżące monitorowanie sytuacji. Podnoszenie tego tematu na forach UE.
7	Przewlekłość procesu legislacyjnego realizowanego na poziomie krajowym mająca wpływ na aktualizację przepisów wewnętrznych użytkowników VIS	Zespół ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE, wszyscy użytkownicy mający dostęp do VIS, KGP	duże	duży	Nadanie priorytetu działaniom legislacyjnym.
8	Długotrwałe procedury przetargowe mogące wpłynąć na terminowość realizacji zadań	KGP, UI	duże	duży	Wybór właściwych procedur przetargowych i bieżący monitoring.
9	Opóźnienia związane z realizacją umowy przez wykonawcę	UI	średnie	średni	Odpowiednie zapisy/kary w umowie.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
10	Brak odpowiednich zasobów kadrowych	KGP, wszyscy użytkownicy VIS	duże	duży	Opracowanie szczegółowego planu potrzeb kadrowych w celach przekazania szczegółowi zarządzającemu projektem. Dodatki motywacyjne.
11	Rotacja członków zespołu projektowego	Wszyscy użytkownicy VIS, KGP	duże	duży	Dodatki motywacyjne.
12	Brak odpowiedniej wiedzy użytkowników końcowych oraz innych podmiotów zaangażowanych	Wszyscy użytkownicy VIS, KGP	średnie	średni	Działania informacyjne, zalecenia i szkoleniowe, w tym działania podejmowane w zakresie uruchomienia projektów szkoleniowych finansowanych np. z FBW.
13	Utrudnienia na gruncie organizacyjnym wynikające ze złożoności VIS Recast	Wszyscy użytkownicy VIS, KGP	średnie	duży	Zadbanie o właściwy przepływ informacji i program szkoleniowy.
Techniczne					
14	Niedostosowanie systemów użytkowników instytucjonalnych	UI	średnie	średni	Bieżące monitorowanie; Priorytetyzacja działań, w szczególności terminowe i odpowiednio wczesne przekazanie dokumentacji technicznej dla UI oraz uzgodnienia na wysokim poziomie kierowniczym.
15	Opóźnienie w przygotowaniu i dostarczeniu końcowej dokumentacji technicznej CWPK VIS, wynikające z opóźnień na szczeblu UE	Zespół ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE	duże	duży	Bieżące monitorowanie i podnoszenie na forum UE konieczności dotrzymania terminów realizacji tego zadania.
Środowiskowe					
16	Kłęski żywiołowe, katastrofy, akty kryminalne, terroryzm, epidemia/pandemia	Wszyscy użytkownicy, MSWiA	średnie	średni	Bieżące monitorowanie.

7.3 PROJEKT 3: Modernizacja systemu Eurodac (Eurodac Recast)

Koordynator: Komenda Główna Policji.

Uczestnicy: Komenda Główna Straży Granicznej, Urząd do Spraw Cudzoziemców, Rada do Spraw Uchodźców, Prezes Urzędu Ochrony Danych Osobowych, inne instytucje korzystające z dostępu do zmodernizowanego Eurodac zgodnie nowymi przepisami Eurodac.

Cel operacyjny: Zapewnienie współpracy polskich instytucji ze zmodernizowanym systemem Eurodac zgodnie z rozporządzeniem (UE) 2024/1358.

Na dzień powstania niniejszego dokumentu zakłada się, że wdrożenie zmodernizowanego Eurodac nastąpi w **czerwcu 2026 r.**

Tabela 6. Zakres projektu Modernizacja systemu Eurodac

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01Eurodac	Dostosowanie systemu AFIS oraz Interfejsu Eurodac do nowej wersji ICD Eurodac	KGP	01.2026 r.
02Eurodac	Testy akceptacyjne nowego Interfejsu Eurodac w środowisku testowym oraz produkcyjnym	KGP	I kwartał 2026 r.
03Eurodac	Przygotowanie specyfikacji interfejsu AFIS/Eurodac dla Użytkowników Instytucjonalnych	KGP	I kwartał 2026 r.
04Eurodac	Doposażenie/wymiana urządzeń wykorzystywanych do rejestracji danych biometrycznych właściwych do przetwarzania danych w ramach zmodernizowanego Eurodac w Policji	KGP	I kwartał 2026 r.
05Eurodac	Modernizacja krajowych systemów teleinformatycznych KGP, KGSG, UdSC pod kątem dostosowania ich do przetwarzania danych w ramach nowego Eurodac	KGP, KGSG, UdSC	I kwartał 2026 r.
06Eurodac	Przeprowadzenie testów krajowych systemów KGP, KGSG, UdSC z AFIS/Interfejs Eurodac,	KGP, KGSG, UdSC	I kwartał 2026 r.
07Eurodac	Gotowość krajowych systemów teleinformatycznych KGP, KGSG, UdSC do pełnej współpracy ze	UI	06.2026 r.

	zmodernizowanym Eurodac (środowisko produkcyjne)		
08Eurodac	Uruchomienie produkcyjne przetwarzania danych w ramach zmodernizowanego Eurodac	KGP	06.2026 r.
09Eurodac	Przygotowanie regulacji prawnych/przepisów wewnętrznych/procedur	UI, KGP, Prezes UODO	12.2025 r.
10Eurodac	Przeprowadzenie testów infrastruktury sprzętowo-programowej w zakresie cyberbezpieczeństwa.	KGP	I kwartał 2026 r.
11Eurodac	Szkolenie użytkowników	KGP, KGSG, UdSC, UI	I kwartał 2026 r.
12Eurodac	Przeprowadzenie testów zmodernizowanego Eurodac na poziomie UE	KGP, KGSG, UdSC	I kwartał 2026 r.

Tabela 7. Główne ryzyka w projekcie Modernizacja systemu Eurodac

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Zarządcze					
1	Problemy z koordynacją wdrażania (obszar zarządzania – ze względu na zaangażowanie w projekt różnych instytucji niezbędna jest koordynacja na szczeblu krajowym)	MSWiA	średnie	duży	Bieżące monitorowanie.
2	Zmiany w zespole odpowiedzialnym za zarządzanie projektem	KGP	średnie	średni	Bieżące monitorowanie.
Finansowe					
3	Niedoszacowanie wartości projektu	KGP	średnie	duży	Bieżące monitorowanie kolejnych etapów szacowania wartości projektu.
4	Brak funduszy w ramach przyznanego budżetu państwowego	MSWiA (jako instytucja koordynująca) MF	duże	duży	Bieżące monitorowanie sytuacji; Przekazanie środków z funduszy celowych; Monitorowanie sprawnego uruchomienia środków na poziomie krajowych, nadanie

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
		KGP (jako instytucja wdrażająca) Właściwe instytucje uczestniczące			najwyższego priorytetu w Programach Krajowych współfinansowanych ze środków unijnych (nowa perspektywa finansowa); Eskalowanie na wyższy poziom
Organizacyjno-prawne					
5	Przewlekłość procesu legislacyjnego realizowanego na poziomie krajowym	KGP, Zespół ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE, wszyscy użytkownicy mający dostęp do Eurodac	duże	duży	Nadanie priorytetu działaniom legislacyjnym.
6	Długotrwałe procedury przetargowe mogące wpłynąć na terminowość realizacji zadań	KGP, UI	duże	duży	Wybór właściwych procedur przetargowych i bieżący monitoring.
7	Opóźnienia związane z realizacją umowy przez Wykonawcę	KGP	średnie	średni	Kary finansowe dla wykonawcy za opóźnienia/niedotrzymanie terminów umowy.
8	Niewystarczające zasoby kadrowe do realizacji projektu	KGP	duże	duży	Opracowanie szczegółowego planu potrzeb kadrowych w celach przekazania szczeblowi zarządzającemu projektem.
9	Rotacja członków zespołu projektowego	KGP	średnie	średni	Dodatki motywacyjne.
Techniczne					
10	Niedostosowanie systemów KGP powiązanych z Eurodac	KGP	średnie	średni	Bieżące monitorowanie.
11	Niedostosowanie systemów użytkowników instytucjonalnych do przetwarzania danych w ramach nowego Eurodac	KGSG, UdSC	średnie	średni	Bieżące monitorowanie; Priorytetyzacja działań oraz uzgodnienia na wysokim poziomie kierowniczym.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
12	Opóźnienie w przygotowaniu i dostarczeniu końcowej dokumentacji technicznej, wynikające z opóźnień na szczęblu UE	KGP	średnie	duży	Bieżące monitorowanie i podnoszenie na forum UE konieczności dotrzymania terminów realizacji tego zadania.
Środowiskowe					
13	Kłęski żywiołowe, katastrofy, akty kryminalne, terroryzm, epidemia/pandemia, wojna	Wszyscy użytkownicy, MSWiA,	średnie	średni	Bieżące monitorowanie.

7.4 PROJEKT 4: Wdrożenie systemu EES

Koordynator: Komenda Główna Straży Granicznej.

Uczestnicy: Komenda Główna Policji (Policja), Urząd do Spraw Cudzoziemców, Urzędy Wojewódzkie (województwa) lub MSWiA, Ministerstwo Spraw Zagranicznych (konsulowie), Krajowa Administracja Skarbowa, sądy, prokuratury, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Ochrony Państwa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Służba Wywiadu Wojskowego oraz przewoźnicy realizujący transport międzynarodowy przez granicę państwową a także Ministerstwo Infrastruktury i Urząd Lotnictwa Cywilnego oraz Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Zapewnienie współpracy polskich instytucji z systemem EES zgodnie z rozporządzeniem (UE) 2017/2226 oraz rozporządzeniem (UE) 2017/2225.

Na dzień powstania niniejszego dokumentu zakłada się, że wdrożenie EES nastąpi w listopadzie 2024 r.

Tabela 8. Zakres projektu Wdrożenie systemu EES

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01EES	Gotowość serwerowni do rozbudowy architektury krajowej	KGP/KGSG	04.2020 r. – 06.2020 r. - Zrealizowane
02EES	Gotowość krajowych zmian w VIS (interoperacyjność EES z VIS)	KGP/KGSG	04.2023 r. - Zrealizowane
03EES	Gotowość systemu centralnego EES/VIS – możliwość testowania, podłączenie infrastruktury granicznej do EES NUI	Agencja eu-LISA, KGSG, UI	12.2020 r. - Zrealizowane
04EES	Uruchomienie krajowej infrastruktury granicznej	KGSG	01.2021 r. – 09.2021 r. - Zrealizowane
05EES	Uruchomienie krajowych interfejsów dostępu do EES w celu dostosowania systemów informatycznych przez UI	KGSG, UI	11.2021 r. - Zrealizowane
06EES	Zapewnienie dostępu do EES za pośrednictwem aplikacji WWW	KGSG, UI i krajowi użytkownicy aplikacji webowej EES	02.2022 r. - Zrealizowane
07EES	Dostosowanie systemów KGSG do obsługi EES	KGSG	12.2022 r. - Zrealizowane
08EES	Gotowość infrastruktury przejść granicznych do prowadzenia rejestracji biometrycznych na potrzeby EES	KGSG	05.2022 r. - Zrealizowane
09EES	Szkolenie kadr	KGSG + inne instytucje	od 10.2022 r.
10EES	Integracja systemów użytkowników instytucjonalnych z systemem KGSG	KGSG, systemy informatyczne użytkowników instytucjonalnych Użytkownicy mający mieć dostęp do EES za pośrednictwem	od 11.2021 r. zakończenie uzależnione od możliwości poszczególnych UI

		własnych systemów informatycznych	
11EES	Uruchomienie systemu EES	KGSG	11.2024 r.
12EES	Zapewnienie dostępu innym UI do danych i informacji w EES (nadawanie uprawnień, konfiguracja)	KGSG + inne instytucje	od 12.2022 r.
13EES	Regulacje prawne/przepisy wewnętrzne/procedury	KGSG, krajowe organy posiadające dostęp do EES oraz Prezes UODO	10.2024 r.
14EES	Kampania informacyjna ⁷	KGSG	Termin zależny od harmonogramu KE.
15EES	Przeprowadzenie testów infrastruktury sprzętowo-programowej w zakresie cyberbezpieczeństwa.	KGSG	10.2024 r.

Tabela 9. Główne ryzyka w projekcie Wdrożenie systemu EES

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Zarządcze					
1	Problemy z koordynacją wdrażania (obszar zarządzania – ze względu na zaangażowanie w projekt różnych instytucji niezbędna jest koordynacja na szczeblu krajowym)	MSWiA	średnie	duży	Bieżące monitorowanie.
2	Zmniejszenie liczby osób w zasobie realizującym projekt EES w związku z odejściami z pracy/służby	KGSG	duże	duże	Zwiększenie stopnia czynnika motywacyjnego
3	Opór przed wprowadzaniem zmian (obszar kadr – wdrożenie systemu w znaczący sposób wpłynie na sposób dokonywania odpraw granicznych)	KGSG	średnie	duży	Działania informacyjne, szkolenia.

⁷ Zgodnie z art. 51 rozporządzenia 2017/2226 Komisja Europejska – we współpracy z organami nadzorczymi i Europejskim Inspektorem Ochrony Danych – organizuje kampanię informacyjną towarzyszącą uruchomieniu EES.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Finansowe					
4	Niedoszacowanie wartości projektu	KGSG	średnie	duży	Bieżące monitorowanie kolejnych etapów szacowania wartości projektu.
5	Brak funduszy (krajowych i unijnych) w ramach przyznanego budżetu (limitu wydatków)	MSWiA (jako instytucja koordynująca) MF KGSG, (jako instytucja wdrażająca) Właściwe instytucje uczestniczące	duże	duży	Zwiększenie przydzielonych limitów wydatków Bieżące monitorowanie sytuacji; Przekazanie środków z funduszy celowych; Monitorowanie sprawnego uruchomienia środków na poziomie krajowych, nadanie najwyższego priorytetu w Programach Krajowych współfinansowanych ze środków unijnych (nowa perspektywa finansowa); Eskalowanie na wyższy poziom
Organizacyjno-prawne					
6	Przewlekłość procesu legislacyjnego realizowanego na poziomie krajowym mających wpływ na przepisy wewnętrzne EES	MSWiA, KGSG, krajowe organy mające dostęp do EES	duże	duży	Nadanie priorytetu działaniom legislacyjnym.
7	Opóźnienia w realizacji postępowań przetargowych, opóźnienia w dostawie/montażu sprzętu na granicy	KGSG	średnie	średni	Terminowe opracowanie dokumentacji przetargowej Wybór właściwych procedur przetargowych i bieżący monitoring; Kary finansowe dla wykonawcy za opóźnienia/niedotrzymanie terminów umowy.
8	Brak zrozumienia sposobu działania systemu przez użytkowników końcowych, brak odpowiedniej liczby szkoleń	KGSG/UI	średnie	średni	Działania informacyjne, szkolenia.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
9	Niegotowość/brak świadomości/wiedzy/informacji zarządzających przejściami granicznymi (porty lotnicze, wojewodowie) dot. nowych regulacji i konieczności wprowadzenia zmian organizacyjnych, infrastrukturalnych, finansowych związanych z zainstalowaniem sprzętu oraz ewentualną koniecznością przebudowy istniejącej infrastruktury lub budowy nowej	KGSG	średnie	średni	Działania informacyjne.
10	Fluktuacja kadr w związku z niedostosowaniem siatki płac pracowników w porównaniu do sektora prywatnego.	Wszyscy użytkownicy, KGSG	duże	duży	Dostosowanie wynagrodzeń pracowników np. poprzez dodatki zdaniowe, motywacyjne. Podnoszenie kwalifikacji zawodowych w związku z nałożeniem nowych zadań poprzez m. in. szkolenia dofinansowywane np. z FBW.
Techniczne					
11	Wzrost kolejek/wydłużenie czasu oczekiwania na odprawę graniczną na przejściach granicznych, w związku z koniecznością pobierania danych biometrycznych na potrzeby rejestracji w EES oraz obowiązkową weryfikacją biometryczną cudzoziemców również na kierunku wyjazdowym	KGSG	duże	średni	Opracowanie wewnętrznych procedur zapobiegawczych i procedur awaryjnych.
12	Opóźnienia w wprowadzaniu zmian dot. VIS po stronie krajowej mających wpływ na uruchomienie EES	KGSG	duże	średni	Bieżące monitorowanie i wymiana informacji.
13	Niedostosowanie systemu odpraw	KGSG	średnie	średni	Bieżące monitorowanie.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
	granicznych oraz aplikacji dostępowej dla innych użytkowników (obszar problemów technicznych) – dostosowania na czas wymaga aplikacja służąca do dokonywania odpraw w przejściach granicznych				
14	Niedostosowanie procesu odpraw granicznych do wymagań systemu EES (pobieranie danych biometrycznych w różnych warunkach – granica lądowa, morska, powietrzna)	KGSG	średnie	średni	Bieżące monitorowanie.
15	Niedostosowanie systemów informatycznych KGSG oraz systemów informatycznych innych instytucji do systemu EES	KGSG	duże	średni	Bieżące monitorowanie.
Środowiskowe					
16	Kłęski żywiołowe, katastrofy, akty kryminalne, terroryzm, epidemia/pandemia	Wszyscy użytkownicy, MSWiA	średnie	średni	Bieżące monitorowanie.

7.5 PROJEKT 5: Wdrożenie systemu ETIAS

Koordynator: Komenda Główna Straży Granicznej.

Uczestnicy: Komenda Główna Policji, Urząd do Spraw Cudzoziemców, Ministerstwo Spraw Zagranicznych (konsulowie), Ministerstwo Sprawiedliwości (Biura Informacyjnego Krajowego Rejestru Karnego, sądy, prokuratury), Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Ochrony Państwa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa oraz Służba Wywiadu Wojskowego, Krajowa Administracja Skarbowa, Ministerstwo Spraw Wewnętrznych i Administracji/Urzędy Wojewódzkie (wojewodowie), Ministerstwo Infrastruktury (wraz z przewoźnikami realizującymi transport międzynarodowy przez granicę państwową) oraz Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Zapewnienie współpracy polskich instytucji z systemem ETIAS zgodnie z rozporządzeniem (UE) 2018/1240.

Na dzień powstania niniejszego dokumentu zakłada się, że wdrożenie ETIAS nastąpi w II połowie 2025 r.

Tabela 10. Zakres projektu Wdrożenie systemu ETIAS

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01ETIAS	Rozbudowa infrastruktury teleinformatycznej (serwery, niezbędne oprogramowanie) na potrzeby podłączenia do ETIAS NUI	KGSG	Do końca I kwartału 2023 r. - Zrealizowane
02ETIAS	Gotowość systemu centralnego ETIAS – możliwość testowania, podłączenie infrastruktury granicznej do ETIAS NUI	Agencja eu-LISA, KGSG, UI	III/IV kwartał 2024 r. – zidentyfikowano w lipcu 2024 r. opóźnienia ze strony Agencji eu-LISA (w przypadku opóźnień ze strony wykonawcy systemu na gruncie unijnym termin może ulec przesunięciu przez KE i Agencję eu-LISA)
03ETIAS	Ukompletowanie i doposażenie ETIAS NU	KGSG	Do końca IV kwartału 2023 r. – doposażenie – zrealizowano Do końca I kwartału 2025 r./początek II kwartału 2025 r. – ukompletowanie osobowe
04ETIAS	Implementacja regulacji prawnych w formie ustawy i rozporządzeń/przepisy wewnętrzne/procedury/nowelizacja innych przepisów powiązanych	MSWiA, KGSG, , inne właściwe organy oraz Prezes UODO	Do końca I kwartału 2025 r./początek II kwartału 2025 r.
05ETIAS	Stworzenie krajowego komponentu N-ETIAS/krajowa infrastruktura ETIAS (aplikacja SG oraz aplikacja internetowa) wraz z zapewnieniem integracji z systemem centralnym oraz listą ostrzegawczą ETIAS oraz narzędziem komunikacyjnym. Dostosowanie pozostałych systemów oraz platformy	KGSG	Do momentu uruchomienia systemu centralnego w wersji produkcyjnej (termin zależny od udostępnienia przez eu-LISA ostatecznej wersji dokumentacji technicznej)

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
	integrującej SG do współpracy z systemem ETIAS.		ETIAS ICD oraz terminowego zakończenia zadania 02ETIAS)
06ETIAS	Udostępnienie przez SG interfejsu (usługi sieciowej) umożliwiającego dostęp typu system-system do danych ETIAS użytkownikom instytucjonalnym oraz dostosowanie przez nich swoich systemów dziedzinowych	KGSG, inne właściwe organy krajowe i instytucje (użytkownicy instytucjonalni).	Do końca I kwartału 2025 r. (powiązane z terminowym zakończeniem zadania 02ETIAS i 05ETIAS oraz wdrożeniem systemu EES)
07ETIAS	Zapewnienie dostępu do danych ETIAS poprzez udostępnioną przez SG aplikację internetową wyznaczonym upoważnionym organom na gruncie krajowym	KGSG, inne właściwe organy krajowe i instytucje (użytkownicy instytucjonalni).	6 miesięcy przed uruchomieniem systemu centralnego w wersji produkcyjnej (powiązane z terminowym zakończeniem zadania 02ETIAS i 05ETIAS)
08ETIAS	Obszar testowy (grunt krajowy i UE) – przeprowadzenie testów z wykorzystaniem symulatora testowego systemu ETIAS	KGSG, właściwe krajowe organy i instytucje, eu-LISA, Frontex, Europol	6-9 miesięcy od czasu uruchomienia systemu centralnego w wersji testowej (możliwe przesunięcia z powodu opóźnień związanych z przygotowaniem przez Agencję eu-LISA symulatora testowego i obszaru testowego)
09ETIAS	Obszar szkoleniowy (grunt krajowy i UE) – przeprowadzenie szkoleń dla użytkowników końcowych i personelu krajowej jednostki ETIAS	KGSG, właściwe krajowe organy i instytucje, eu-LISA, Frontex, Europol, CEPOL	6 miesięcy przed uruchomieniem systemu centralnego w wersji produkcyjnej.
10ETIAS	Dostosowanie systemów informatycznych UI do realizacji zadań związanych z bezpośrednim dostępem do ETIAS. W szczególności zapewnienie integracji systemu Biura SIRENE z systemem centralnym ETIAS w kontekście odbierania zautomatyzowanych notyfikacji generowanych przez system centralny ETIAS	KGSG + KGSG Pozostałe właściwe krajowe organy i instytucje	3 miesiące przed uruchomieniem systemu centralnego w wersji produkcyjnej
11ETIAS	Zapewnienie i uruchomienie komunikacji dwukierunkowej pomiędzy Polskim ETIAS NU a EUROPOLEM (Polski ENU) za pośrednictwem systemu SIENA (SWIZE)	KGSG, KGP, ABW – w zakresie czynności akredytacyjnych	Do czasu uruchomienia systemu centralnego

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
12ETIAS	Kampania informacyjna ⁸	KGSG, MSZ	Termin zależny od przyjętego przez KE ostatecznego terminu uruchomienia systemu tj. początek kampanii na 6 miesięcy przed uruchomieniem systemu
13ETIAS	Pełna gotowość operacyjna komponentu krajowego, testy akceptacyjne (poziom krajowy i UE)	KGSG, właściwe organy krajowe i instytucje, Agencja eu-LISA, Frontex, Europol	Data zostanie wskazana na podstawie szczegółowego terminu uruchomienia systemu wskazanego przez KE
14ETIAS	Uruchomienie systemu ETIAS	KE, Agencja Frontex, Agencja eu-LISA, KGSG	II połowa 2025 r. data bez oficjalnego potwierdzenia – właściwa data zostanie wskazana w formie decyzji na około 7 tygodni przed dniem uruchomienia uwzględniając min. 6 miesięcy odstępu czasowego od uruchomienia EES.
15ETIAS	Przeprowadzenie testów infrastruktury sprzętowo-programowej w zakresie cyberbezpieczeństwa.	KGSG	I połowa 2025 r.

Tabela 11. Główne ryzyka w projekcie Wdrożenie systemu ETIAS

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Zarządcze					
1	Problemy z koordynacją wdrażania (obszar zarządzania – ze względu na zaangażowanie w projekt różnych instytucji niezbędna jest koordynacja na szczeblu krajowym)	MSWiA	średnie	duży	Bieżące monitorowanie.
2	Zmniejszenie liczby osób w zasobie realizującym projekt ETIAS w związku z odejściami z pracy/służby	KGSG	duże	duże	Zwiększenie stopnia czynnika motywacyjnego

⁸ Zgodnie z art. 72 rozporządzenia 2018/1240 Komisja Europejska – we współpracy z Europejską Służbą Działań Zewnętrznych, jednostką centralną ETIAS i państwami członkowskimi, w tym z ich konsulatami w odnośnych państwach trzecich, zapewnia, aby rozpoczęciu działalności ETIAS towarzyszyła kampania informacyjna.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
3	Opór przed wprowadzaniem zmian (obszar kadr – wdrożenie systemu w znaczący sposób wpłynie na sposób dokonywania odpraw granicznych)	KGSG	średnie	duży	Działania informacyjne, szkolenia.
Finansowe					
4	Niedoszacowanie wartości projektu	KGSG	średnie	duży	Bieżące monitorowanie kolejnych etapów szacowania wartości projektu.
5	Brak funduszy (krajowych i unijnych) w ramach przyznanego budżetu (limitu wydatków)	MSWiA (jako instytucja koordynująca) MF KGSG, (jako instytucja wdrażająca) Właściwe instytucje uczestniczące	duże	duży	Zwiększenie przydzielonych limitów wydatków Bieżące monitorowanie sytuacji; Przekazanie środków z funduszy celowych; Monitorowanie sprawnego uruchomienia środków na poziomie krajowych, nadanie najwyższego priorytetu w Programach Krajowych współfinansowanych ze środków unijnych (nowa perspektywa finansowa); Eskalowanie na wyższy poziom
Organizacyjno-prawne					
6	Nieadekwatne zaplanowanie procesu szkoleniowego	KGSG	średnie	średni	Analiza potrzeb szkoleniowych; Priorytetyzacja na szczeblu kierowniczym.
7	Utrudnienia w koordynacji działań organizacyjno-technicznych wynikające z zaangażowania zbyt wielu podmiotów na poziomie krajowym	KGSG	średnie	mały	Opracowanie odpowiednich procedur; Priorytetyzacja na szczeblu kierowniczym.
8	Opóźnienia w realizacji postępowań przetargowych, opóźnienia w dostawie sprzętu	KGSG	średnie	średni	Terminowe opracowanie dokumentacji przetargowej Wybór właściwych procedur przetargowych i bieżący monitoring;

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
					Kary finansowe dla wykonawcy za opóźnienia/niedotrzymanie terminów umowy.
9	Przewlekłość procedur prowadzonych przez organy zewnętrzne w zakresie certyfikacji stanowisk niejawnych (np. SIENA) i wydawania poświadczeń bezpieczeństwa funkcjonariuszom SG	KGSG	średnie	średni	Priorytetyzacja na szczeblu kierowniczym.
10	Brak zrozumienia na poziomie organizacyjno-kadrowym, sposobu działania systemu oraz jego celów przez użytkowników końcowych oraz inne podmioty zaangażowane	KGSG + inne podmioty zaangażowane (właściwe organy takie jak KGP, ABW, KAS, MS – KRK, MSZ – konsulatory RP)	średnie	mały	Działania informacyjne; Priorytetyzacja na szczeblu kierowniczym; Właściwa wymiana informacji.
11	Fluktuacja kadr w związku z niedostosowaniem siatki płac pracowników w porównaniu do sektora prywatnego.	Wszyscy użytkownicy, KGSG	duże	duży	Dostosowanie wynagrodzeń pracowników np. poprzez dodatki zdaniowe, motywacyjne. Podnoszenie kwalifikacji zawodowych w związku z nałożeniem nowych zadań poprzez m. in. szkolenia dofinansowywane np. z FBW.
Techniczne					
12	Opóźnienia w terminowym uruchomieniu EES uniemożliwią uruchomienie systemu ETIAS	KGSG	wysokie	średni	Bieżące monitorowanie.
13	Brak współpracy i problemy z integracją przewoźników z systemem ETIAS, jak i problemy z ich certyfikacją	KGSG + przewoźnicy	średnie	średni	Koordinacja i wymiana informacji; Priorytetyzacja na szczeblu kierowniczym; Właściwa wymiana informacji.
14	Niedostosowanie dziedziny systemów teleinformatycznych do współpracy z systemem	KGSG + podmioty, w gestii których są dziedziny	średnie	średni	Koordinacja i wymiana informacji; Priorytetyzacja na szczeblu kierowniczym;

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
	centralnym ETIAS oraz utrudnienia w zakresie współpracy i wymiany informacji z podmiotami zaangażowanymi w ramach krajowego komponentu ETIAS	systemy + podmioty zaangażowane w ramach krajowego komponentu ETIAS			Właściwa wymiana informacji.
Środowiskowe					
15	Kłęski żywiołowe, katastrofy, akty kryminalne, terroryzm, epidemia/pandemia	Wszyscy użytkownicy, MSWiA	średnie	średni	Bieżące monitorowanie.

7.6 PROJEKT 6: Wdrożenie systemu ECRIS-TCN

Koordynator: Ministerstwo Sprawiedliwości.

Uczestnicy: Komenda Główna Straży Granicznej, Komenda Główna Policji, Ministerstwo Spraw Wewnętrznych i Administracji, Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Wdrożenie w systemach krajowych niezbędnych funkcji do integracji z systemem ECRIS-TCN zgodnie z *rozporządzeniem (UE) 2019/816 oraz dyrektywą (UE) 2019/884*.

Na dzień powstania niniejszego dokumentu zakłada się, że wdrożenie ECRIS-TCN nastąpi **w III kwartale 2025 r.**

Tabela 12. Zakres projektu Wdrożenie systemu ECRIS-TCN

Nr zadania	Nazwa Zadania	Odpowiedzialność za realizację zadania	Termin*
01ECRIS-TCN	Zapewnienie zgodności przepisów prawa polskiego pozostającego we właściwości poszczególnych organów administracji państwowej z przepisami <i>rozporządzenia (UE) 2019/816</i>	Ministerstwo Sprawiedliwości	Wejście w życie ustawy o zmianie ustawy o Krajowym Rejestrze Karnym oraz niektórych innych ustaw (projekt został wpisany do wykazu prac Rady Ministrów pod numerem UC57); II kwartał 2025 r.
02ECRIS-TCN	Integracja ST KRK z ECRIS-TCN	Ministerstwo Sprawiedliwości	I kwartał 2025 r.
03ECRIS-TCN	Rozbudowa ST KRK o dane niezbędne do realizacji procesów związanych z zasilaniem bazy ECRIS-TCN (numer AFIS ID)	Ministerstwo Sprawiedliwości	I-II kwartał 2025 r.
04ECRIS-TCN	Implementacja procesów zasilania ECRIS-TCN danymi alfanumerycznymi	Ministerstwo Sprawiedliwości	I kwartał 2025 r.
05ECRIS-TCN	Implementacja procesów zasilania ECRIS-TCN danymi daktyloskopijnymi wraz z rozwiązaniem technicznym	Ministerstwo Sprawiedliwości oraz CLKP i Komenda Główna Policji (Błil) w zakresie umożliwienia pobierania odcisków palców przez BKRK dla celów realizacji procesów zasilania ECRIS-TCN	I-II kwartał 2025 r.
06ECRIS-TCN	Implementacja procesów przeszukiwania ECRIS-TCN	Ministerstwo Sprawiedliwości	I kwartał 2025 r.
07ECRIS-TCN	Zasilenie ECRIS-TCN danymi historycznymi	Ministerstwo Sprawiedliwości	II kwartał 2025 r. (Komisja Europejska określi dzień rozpoczęcia wprowadzania danych alfanumerycznych)
08ECRIS-TCN	Dostosowanie Polish Gateway do przetwarzania wniosków na potrzeby ECRIS-TCN	Komendant Główny Policji, CLKP	IV kwartał 2024 r. – I kwartał 2025 r.

09ECRIS-TCN	Szkolenie kadr	Ministerstwo Sprawiedliwości oraz inni uczestnicy procesów,	II kwartał 2025 r.
10ECRIS-TCN	Stworzenie konwertera dla plików NIST	Ministerstwo Sprawiedliwości	IV kwartał 2024 r.
11ECRIS-TCN	Przeprowadzenie testów infrastruktury sprzętowo-programowej w zakresie cyberbezpieczeństwa.	Ministerstwo Sprawiedliwości	II kwartał 2025 r.

* Terminy zadań 02ECRIS-TCN – 12ECRIS-TCN uzależnione są od prac legislacyjnych oraz technicznych na szczelbu krajowym i UE.

Tabela 13. Główne ryzyka w projekcie Wdrożenie systemu ECRIS-TCN

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Zarządcze					
1	Jednoczesna realizacja zadań rozwojowych w kilku obszarach ST KRK niezwiązanych z ECRIS-TCN	MS	duże	duży	Bieżące zarządzanie ryzykami projektu, zarządzanie zleceniami, elastyczne planowanie, dobra współpraca z Wykonawcą, eskalowanie problemów
2	Brak zasobów do realizacji projektu (brak lub opóźnienia w procedowaniu niezbędnych umów wykonawczych)	MS	średnie	duży	Zapewnienie właściwego nadzoru nad procedurami ze strony kierowników odpowiedzialnych komórek organizacyjnych MS;
Finansowe					
3	Brak funduszy w ramach przyznanego budżetu państwowego	MF	średnie	duży	Brak funduszy w ramach przyznanego budżetu państwowego
Organizacyjno-prawne					
4	Utrudniona współpraca z interesariuszami na poziomie krajowym oraz z instytucją koordynującą program Interoperacyjności (MSWiA)	Inne	duże	duży	Zapewnienie właściwego obiegu informacji poprzez spotkania statusowe oraz organizowanie telekonferencji według regularnego harmonogramu; Bezpośredni kontakt z najważniejszymi interesariuszami. Uczestnictwo w spotkaniach krajowego zespołu ds. interoperacyjności.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
					<p>Konieczność uwzględnienia w pracach krajowego zespołu ds. interoperacyjności innych obszarów niż tylko</p> <p>Weryfikator linków – MID (zależne od MSWiA)</p> <p>Eskalowanie problemów z brakiem transparentności w działaniach realizowanych w krajowym Programie Interoperacyjności. Eskalowanie problemów dot. silosowości realizowanych prac na styku systemów krajowych i interoperacyjności</p>
5	Opóźnienie w przyjęciu aktów wykonawczych i delegowanych na podstawie odpowiednich Rozporządzeń (ECRIS-TCN i interoperacyjność) oraz zmian Rozporządzenia ETIAS i innych rozporządzeń wprowadzających integrację ECRIS-TCN i ETIAS	KE (UE)	średnie	duży	<p>Dokonanie analizy i przygotowanie metod postępowania w odpowiedzi na możliwe rozwiązania legislacyjne; Ścisła współpraca z organami UE i monitoring na spotkaniach komitetu oraz właściwej grupy roboczej UE.</p>
6	Opóźnienie w dostarczeniu przez eu-LISA produktów niezbędnych do prac developerskich (dokumentacja, symulator ECRIS-TCN, ICD itd.)	eu-LISA	duże	duży	<p>Ścisła współpraca z organami eu-LISA i monitoring na spotkaniach grupy doradczej oraz rady zarządzającej programem ECRIS-TCN w ramach struktur powołanych przez eu-LISA. Określanie z Wykonawcą sposobów pracy z niepełną z założenia dokumentacją centralną</p>
7	Opóźnienie we wprowadzeniu niezbędnych zmian prawnych w prawie krajowym	Inne	duże	duży	<p>Zintensyfikowanie prac nad przygotowaniem niezbędnych zmian w ustawie o KRK oraz innych ustawach; Możliwie najszybsze przeprowadzenie konsultacji roboczych;</p> <p>Ścisła współpraca wewnętrznych komórek organizacyjnych MS w pracach legislacyjnych.</p>

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
					<p>Konieczność zintensyfikowania prac legislacyjnych w II półroczu 2024 r.</p> <p>Monitoring procesu legislacyjnego w zakresie nowelizacji ustawy o Krajowym Rejestrze Karnym,</p> <p>Eskalowanie do MSWiA i SG konieczności jak najwcześniejszego poznania propozycji przepisów dot. ustaw implementujących Interoperacyjność i system ETIAS</p>
8	Brak wystarczającej transparentności we wdrażaniu przepisów dotyczących interoperacyjności na poziomie krajowym	MSWiA/MS/SG /KGP/Inni	duże	duży	Macierz powiązań legislacyjnych - dyskusja na forum zespołu o założeniach ustawy implementującej rozporządzenia dotyczące interoperacyjności
Techniczne					
9	Opóźnienia na gruncie UE w kontekście wdrażania Wielkoskalowych Systemów Informacyjnych UE	Wszyscy użytkownicy	duże	duży	Informowanie i monitorowanie.
10	Brak pewności co do daty wdrożenia ECRIS-TCN. Obecnie projektowy termin wskazywany przez eu-LISA to przełom II/III kwartału 2025 r.	Wszyscy użytkownicy	duże	duży	<p>Współpraca z eu-LISA w ramach PMB i AG Monitorowanie procesów, elastyczne zarządzanie harmonogramami realizacji zadań.</p> <p>Założenie możliwości wydłużenia realizacji ECRIS-TCN.</p>
11	Opóźnienia we wdrożeniu w PL systemu ECRIS-TCN w planowanym przez eu-LISA terminie	MS/inni zaangażowani interesariusze	średni	duże	<p>Sprawną realizacją zadań, Eskalacja opóźnień w realizacji zadań po stronie Wykonawców Zewnętrznych realizujących prace rozwojowe w ST KKK,</p> <p>Współpraca z KGP w zakresie przetwarzania danych biometrycznych,</p> <p>Postęp prac legislacyjnych,</p> <p>Przygotowanie rozwiązań backupowych i MVP na start wymiany produkcyjnej. W oparciu o te priorytety zlecenie zadań Wykonawcy</p>

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
12	Kwestie architektoniczne, które mogą wpłynąć na sposób integracji MS/KRK z systemem ECRIS-TCN	MS/SG/MSWiA	duże	średni	Eskalacja potrzeby większej transparentności w pracach krajowych na poziomie interoperacyjności, Współpraca z SG - konieczność wyjaśnienia z PL i w eu-LISIA wątków związanych z : - ilością National Gateways, które mają łączyć systemy krajowe z narzędziami interoperacyjności - sposobem zarządzania profilami na poziomie National Domain i na poziomie ESP
13	Brak pewności co do sposobu zarządzania profilami w National Domain, co może skutkować brakiem możliwości przeprowadzenia testów integracji w IV kwartale	MSWiA/SG/MS	duże	duży	Współpraca z SG, pozyskanie wyjaśnień na polu PL i eu-LISA Pismo do eu-LISA
Środowiskowe					
14	Kłęski żywiołowe, katastrofy, akty kryminalne, terroryzm, epidemia/pandemia	Wszyscy użytkownicy, MSWiA	średnie	średni	Bieżące monitorowanie.

7.7 PROJEKT 7: Wdrożenie narzędzi Interoperacyjności Systemów (IO)

Koordynator: Komenda Główna Straży Granicznej

Uczestnicy: Policja, Urząd do Spraw Cudzoziemców, Urzędy Wojewódzkie, Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Sprawiedliwości, Ministerstwo Spraw Zagranicznych, Krajowa Administracja Skarbowa, sądy, prokuratury, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Ochrony Państwa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Służba Wywiadu Wojskowego oraz Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Wdrożenie narzędzi Interoperacyjności Wielkoskalowych Systemów Informacyjnych UE zgodnie z rozporządzeniem (UE) 2019/817 oraz rozporządzeniem (UE) 2019/818.

Na dzień powstania niniejszego dokumentu zakłada się, że pełne wdrożenie Interoperacyjności nastąpi po 2026 r.

Tabela 14. Zakres projektu IO

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01IO	Przygotowanie planu projektu	KGSG	do 10.2024 r.
02IO	Powołanie zespołu projektowego	KGSG	05.2023 r.
03IO	Przygotowanie projektu ustawy	KGSG	III kw. 2025 r.
04IO	Dostosowanie krajowej infrastruktury informatycznej do wdrożenia narzędzi Interoperacyjności	KGSG	IV kw. 2025 r.
05IO	Stworzenie na poziomie krajowym macierzy uprawnień	KGSG, UI	IV kw. 2024 r.
06IO	Uruchomienie krajowych interfejsów dostępu do ESP oraz przekazanie opisu krajowego interfejsu w celu dostosowania systemów informatycznych przez UI	KGSG, UI	IV kw. 2025 r.
07IO	Uruchomienie krajowego interfejsu umożliwiającego aktualizację powiązań pomiędzy tożsamościami oraz przekazanie opisu krajowego interfejsu w celu dostosowania systemów informatycznych przez UI	KGSG, UI	początek okresu przejściowego MID
08IO	Zapewnienie dostępu do ESP za pośrednictwem aplikacji WWW	UI i krajowi użytkownicy aplikacji webowej ESP	do końca okresu przejściowego ESP
09IO	Zapewnienie dostępu do krajowego interfejsu umożliwiającego aktualizację powiązań pomiędzy tożsamościami za pośrednictwem aplikacji WWW	UI i krajowi użytkownicy aplikacji webowej	do końca okresu przejściowego MID
10IO	Szkolenie kadr	KGSG, inne instytucje	od dostarczenia wersji szkolnych narzędzi do końca

			okresów przejściowych MID i ESP
11IO	Integracja systemów użytkowników instytucjonalnych z ESP	KGSG, systemy informatyczne użytkowników instytucjonalnych Użytkownicy mający mieć dostęp do ESP za pośrednictwem własnych systemów informatycznych	od I kw. 2026 r. do końca okresu przejściowego ESP
12IO	Integracja systemów użytkowników instytucjonalnych z krajowego interfejsu umożliwiającego aktualizację powiązań pomiędzy tożsamościami	KGSG, systemy informatyczne użytkowników instytucjonalnych Użytkownicy planujący mieć dostęp do krajowego interfejsu umożliwiającego aktualizację powiązań pomiędzy tożsamościami za pośrednictwem własnych systemów informatycznych	do końca okresu przejściowego MID
13IO	Regulacje przepisy wewnętrzne/procedury	KGSG	IV kw. 2025 r.
14IO	Uruchomienie odpowiednich procesów zarządzania jakością danych oraz dostosowanie narzędzi oraz procedur administratorów danych	KGSG	
15IO	Zapewnienie dostępu do centralnego narzędzia do rozwiązywania powiązań CSLR instytucjom krajowym	KGSG, UI	
16IO	Przeprowadzenie testów infrastruktury sprzętowo-programowej w zakresie cyberbezpieczeństwa	KGSG	

Tabela 15. Główne ryzyka w projekcie IO

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Zarządcze					
1	Problemy z koordynacją wdrażania (obszar)	MSWiA	średnie	duży	Bieżące monitorowanie.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
	zarządzania – ze względu na zaangażowanie w projekt różnych instytucji niezbędna jest koordynacja na szczeblu krajowym)				
2	Fluktuacja kadr w związku z niedostosowaniem siatki płac pracowników w porównaniu do sektora prywatnego	KGSG	duże	duży	Zwiększenie stopnia czynnika motywacyjnego
Finansowe					
3	Niedoszacowanie wartości projektu	KGSG	średnie	duży	Bieżące monitorowanie kolejnych etapów szacowania wartości projektu.
4	Brak funduszy (krajowych i unijnych) w ramach przyznanego budżetu (limitu wydatków)	MSWiA (jako instytucja koordynująca) MF KGSG, (jako instytucja wdrażająca) Właściwe instytucje uczestniczące	duże	duży	Zwiększenie przydzielonych limitów wydatków Bieżące monitorowanie sytuacji; Przekazanie środków z funduszy celowych; Monitorowanie sprawnego uruchomienia środków na poziomie krajowych, nadanie najwyższego priorytetu w Programach Krajowych współfinansowanych ze środków unijnych (nowa perspektywa finansowa); Eskalowanie na wyższy poziom
Organizacyjno-prawne					
5	Utrudniona współpraca z interesariuszami na poziomie krajowym)	Inne	duże	duży	Zapewnienie właściwego obiegu informacji, dostosowanie się przedstawicieli instytucji i służb wyznaczonych do podzespołów roboczych do sposobu prowadzenia projektów przez SG
6	Opóźnienie we wprowadzeniu niezbędnych zmian prawnych w prawie krajowym	Inne	średnie	duży	Zintensyfikowanie prac nad przygotowaniem niezbędnych zmian w przepisach. Możliwie najszybsze przeprowadzenie konsultacji roboczych; Ścisła współpraca wewnętrznych komórek organizacyjnych KGSG w pracach legislacyjnych.
7	Brak zrozumienia sposobu działania systemu przez użytkowników	KGSG/UI	średnie	średni	Działania informacyjne, szkolenia.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
	końcowych, brak odpowiedniej liczby szkoleń				
8	Konieczność długotrwałego utrzymywania zespołów projektowych – inżynierskich i analitycznych. Realizacja projektu w okresie kilku lat powoduje częste zmiany w składach zespołów – utrata ciągłości działania i zdolności do podejmowania wiążących decyzji, brak możliwości realizacji zadań na wysokim poziomie	KGSG	duże	średnie	Umożliwić zwiększenie ilości osób w zespołach (szczególnie inżynierów) co zapewni pełną zastępowalność
9	Opóźnienia w realizacji postępowań przetargowych, opóźnienia w dostawie sprzętu	KGSG	średnie	średni	Terminowe opracowanie dokumentacji przetargowej Wybór właściwych procedur przetargowych i bieżący monitoring; Kary finansowe dla wykonawcy za opóźnienia/niedotrzymanie terminów umowy.
Techniczne					
10	Opóźnienia na gruncie UE w kontekście wdrażania wielkoskalowych systemów informacyjnych UE	Wszyscy użytkownicy	duże	duży	Informowanie i monitorowanie.
11	Niedostosowanie systemów informatycznych KGSG oraz systemów informatycznych innych instytucji do narzędzi interoperacyjności	Wszyscy użytkownicy	małe	średni	Bieżące monitorowanie.
Środowiskowe					
12	Kłęski żywiołowe, katastrofy, akty kryminalne, terroryzm, epidemia/pandemia	Wszyscy użytkownicy, MSWiA	średnie	średni	Bieżące monitorowanie.

7.8 PROJEKT 8: Dostosowanie przepisów prawnych systemu EES

Koordinator: Komenda Główna Straży Granicznej.

Uczestnicy: Policja, Urząd do Spraw Cudzoziemców, Urzędy Wojewódzkie, Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Spraw Zagranicznych, Krajowa Administracja Skarbowa, sądy, prokuratury, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Ochrony Państwa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Służba Wywiadu Wojskowego oraz Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Przyjęcie krajowych przepisów regulujących funkcjonowanie systemu EES w Polsce.

Tabela 16. Dostosowanie przepisów prawnych systemu EES

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01PEES	Przekazanie projektu ustawy do uzgodnień wewnątrzresortowych. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas konsultacji wewnątrzresortowych.	MSWiA/KGSG	Zrealizowane
02PEES	Przekazanie projektu ustawy do uzgodnień międzyresortowych. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas konsultacji międzyresortowych.	MSWiA/KGSG	Zrealizowane
03PEES	Przekazanie projektu ustawy pod obrady Komitetu RM ds. Cyfryzacji. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KRMC	MSWiA/KGSG	Zrealizowane
04PEES	Przekazanie projektu pod obrady Komitetu RM ds. Europejskich. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KSE	MSWiA/KGSG	Zrealizowane
05PEES	Opracowanie projektów aktów wykonawczych	KGSG	Zrealizowane
06PEES	Przekazanie projektu pod obrady Stałego Komitetu Rady Ministrów. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas SKRM	MSWiA/KGSG	Zrealizowane
07PEES	Przekazanie projektu pod obrady Rady Ministrów. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas RM	MSWiA/KGSG	Zrealizowane
08PEES	Przekazanie projektu pod obrady Sejmu i Senatu.	MSWiA/KGSG	Zrealizowane

	Uzgodnienia uwag do projektu ustawy zgłoszonych przez Sejm i Senat		
09PEES	Opracowanie przepisów wewnętrznych (procedury związane z wszystkimi aspektami odnoszącymi się do korzystania z EES).	Wszyscy użytkownicy EES	12.2024 r.

Tabela 17. Główne ryzyka w projekcie dostosowania przepisów prawnych systemu EES

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Organizacyjno-prawne					
1	Ograniczone zasoby kadrowe SG	KGSG	duże	duży	Potrzeba odpowiedniego zarządzania priorytetami przydzielonych zadań, uzyskanie wsparcia kadrowego, ustanowienie odpowiedniego systemu motywacyjnego.
2	Wieloaspektowa złożoność przedmiotu regulacji pozostająca w zakresie właściwości wielu organów	MSWiA/KGSG	średnie	duży	Właściwa koordynacja wymiany informacji
3	Potrzeba dostosowania projektu do innych powstających systemów teleinformatycznych w ramach interoperacyjności	KGSG	średnie	duży	Ścisła współpraca z zespołami odpowiedzialnymi za pozostałym systemy wielkoskalowe UE
4	Przewlekłość procesu legislacyjnego realizowanego na poziomie krajowym mających wpływ na przepisy wewnętrzne.	MSWiA, KGSG, krajowe organy mające dostęp do EES	duże	duży	Nadanie priorytetu działaniom legislacyjnym.

7.9 PROJEKT 9: Dostosowanie przepisów prawnych systemu ETIAS

Koordynator: Komenda Główna Straży Granicznej.

Uczestnicy: Komenda Główna Policji, Urząd do Spraw Cudzoziemców, Rada ds. Uchodźców, Ministerstwo Spraw Zagranicznych (oraz konsulowie), Ministerstwo Sprawiedliwości (sądy, prokuratury), Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Ochrony Państwa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa oraz Służba Wywiadu Wojskowego, Krajowa Administracja Skarbowa, Ministerstwo Spraw Wewnętrznych i Administracji, Urzędy Wojewódzkie (wojewodowie), Ministerstwo Infrastruktury (wraz z przewoźnikami realizującymi transport międzynarodowy przez granicę państwową) oraz Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Przyjęcie krajowych przepisów regulujących funkcjonowanie systemu ETIAS w Polsce.

Tabela 18. Dostosowanie przepisów prawnych systemu ETIAS

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01PETIAS	Przygotowanie założeń oraz zakresu przedmiotowego do projektu ustawy na podstawie zapisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2018/1240 oraz jego aktów wykonawczych	ZdsC KGSG	Zrealizowano
02PETIAS	Przygotowanie wstępnego planu i zakresu merytorycznego ustawy	ZdsC KGSG	Zrealizowano
03PETIAS	Opracowywanie propozycji projektu ustawy i przekazanie go do Biura Prawnego KGSG	ZdsC KGSG	Zrealizowano
04PETIAS	Prace nad projektem ustawy prowadzone w ramach SG – konsultacje wewnętrzne w ramach SG	ZdsC KGSG/BP KGSG	Zrealizowano
05PETIAS	Przekazanie uzgodnionego w ramach KGSG projektu ustawy wraz z uzasadnieniem i OSR do MSWiA	BP KGSG	Zrealizowano
06PETIAS	Przekazanie projektu ustawy do uzgodnień wewnątrzresortowych. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas konsultacji wewnątrzresortowych.	KGSG/MSWiA	Zrealizowano
07PETIAS	Przekazanie projektu ustawy do uzgodnień międzyresortowych. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas konsultacji międzyresortowych.	KGSG/MSWiA	11.2024 r.
08PETIAS	Skierowanie projektu do opiniowania oraz konsultacji publicznych.	KGSG/MSWiA	01.2025 r.

09PETIAS	Opracowanie projektów aktów wykonawczych	KGSG	01.2025 r.
10PETIAS	Przekazanie projektu ustawy pod obrady Komitetu RM ds. Cyfryzacji Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KRMC.	MSWiA/KGSG	02.2025 r.
11PETIAS	Przekazanie projektu pod obrady Komitetu RM ds. Europejskich. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KSE.	MSWiA/KGSG	02.2025 r.
12PETIAS	Przekazanie projektu pod obrady Stałego Komitetu Rady Ministrów. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas SKRM.	MSWiA/KGSG	03.2025 r.
13PETIAS	Przekazanie projektu pod obrady Komisji Prawniczej. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KP.	MSWiA/KGSG	03.2025 r.
14PETIAS	Przekazanie projektu pod obrady Rady Ministrów. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas RM.	MSWiA/KGSG	04.2025 r.
15PETIAS	Przekazanie projektu pod obrady Sejmu i Senatu. Uzgodnienia uwag do projektu ustawy zgłoszonych przez Sejm i Senat.	MSWiA/KGSG	04.2025
16PETIAS	Opracowanie przepisów wewnętrznych (procedury związane z wszystkimi aspektami odnoszącymi się do korzystania z ETIAS).	Wszyscy użytkownicy ETIAS	04.2025 r.

Tabela 19. Główne ryzyka w projekcie dostosowania przepisów prawnych systemu ETIAS

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Organizacyjno-prawne					
1	Związki z innymi projektami prawnymi i systemowymi prowadzonymi równolegle przez SG	KGSG	Średnie	Średni	Realizacja innych projektów prawnych i systemowych równolegle przez różne jednostki organizacyjne KGSG może powodować opóźnienia, rozbieżności oraz brak spójności opracowywanych zagadnień dotyczących wspólnych kwestii.

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
					Dostosowanie na szczeblu centralnym SG harmonogramów prac oraz ich celów, prowadzonych w związku z realizacją równoległych projektów, uzgodnienie współpracy i koordynacji merytorycznej pomiędzy poszczególnymi biurami/zarządami KGSG.
2	Fluktuacja kadr/zmiany kadrowe/ograniczenie zasobów kadrowych	KGSG	Duże	Duży	<p>W ostatnich latach obserwuje się wysoki wskaźnik zmian kadrowych na zajmowanych stanowiskach związany z migracją kadry do innych komórek bądź odejściem na świadczenia emerytalne doświadczonych funkcjonariuszy posiadających wiedzę ekspercką i duże doświadczenie praktyczne.</p> <p>Potrzeba ustanowienia odpowiedniego systemu motywacyjnego, wdrożenia form gratyfikacji związanych z wykonywaniem dodatkowych zadań, wymagających specjalistycznej wiedzy i dodatkowych umiejętności. Podniesienie konkurencyjności obecnej formy zatrudnienia oraz udzielanie wsparcia kadrowego z pozycji Kierownictwa SG.</p>
3	Ograniczone zasoby kadrowe SG	KGSG	duże	duży	<p>Odejścia ze służby wysoko wykwalifikowanej kadry, posiadającej szeroką wiedzę i doświadczenie. Brak dostępnych funkcjonariuszy w ramach SG posiadających odpowiednią wiedzę i umiejętności do prowadzenia projektów w ramach powiązanych obszarów legislacyjnych oraz technicznych.</p> <p>Potrzeba zapewnienia odpowiednich szkoleń, studiów, warsztatów, spotkań konsultacyjnych, w celu podniesienia kwalifikacji związanych z zarządzaniem i realizacją projektu dla właściwych funkcjonariuszy zaangażowanych w prowadzenie projektów od strony merytoryczno-analitycznej w ramach ww. obszarów.</p>
4	Wieloaspektowa złożoność przedmiotu regulacji pozostająca w zakresie właściwości wielu organów	MSWiA/KGSG	średnie	duży	<p>Zaangażowanie zbyt wielu organów krajowych i służb podległych różnym ministerstwom w realizację zadań ETIAS.</p> <p>Potrzeba właściwej koordynacji w zakresie wymiany informacji z poziomem horyzontalnym.</p>

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
5	Potrzeba dostosowania projektu do innych powstających systemów teleinformatycznych w ramach interoperacyjności	KGSG	średnie	duży	<p>Zbyt wiele projektów systemowych prowadzonych równolegle w jednym czasie.</p> <p>Zagwarantowanie ścisłej i efektywnej współpracy z zespołami odpowiedzialnymi za pozostałe systemy wielkoskalowe oraz narzędzia IO.</p>
6	Przewlekłość procesu legislacyjnego realizowanego na poziomie krajowym mających wpływ na przepisy wewnętrzne.	MSWiA, KGSG, krajowe organy mające dostęp do ETIAS	duże	duży	<p>Zakres ustawy zawiera bardzo złożone kwestie merytoryczne, których uzgodnienie na poziomie krajowym jest czasochłonne.</p> <p>Potrzeba priorytetyzacji działań.</p> <p>Nadanie z poziomu ministerstwa priorytetu działaniom legislacyjnym.</p>

7.10 PROJEKT 10: Dostosowanie przepisów prawnych systemu VIS

Koordynator: na dzień powstania niniejszego dokumentu brak wyznaczonego koordynatora.

Uczestnicy: Komenda Główna Policji, Urząd do Spraw Cudzoziemców, Rada ds. Uchodźców, Ministerstwo Spraw Zagranicznych (oraz konsulowie), Ministerstwo Sprawiedliwości, sądy, prokuratury, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Ochrony Państwa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa oraz Służba Wywiadu Wojskowego, Krajowa Administracja Skarbowa, Ministerstwo Spraw Wewnętrznych i Administracji, Urzędy Wojewódzkie (wojewodowie) oraz Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Przyjęcie krajowych przepisów regulujących funkcjonowanie zmodernizowanego systemu VIS w Polsce.

Tabela 20. Dostosowanie przepisów prawnych systemu VIS

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01PVIS	Przygotowanie założeń oraz zakresu do projektu ustawy		
02PVIS	Przygotowanie wstępnego planu i zakresu merytorycznego ustawy		
03PVIS	Zakończenie wewnętrznych prac w instytucji wiodącej		
04PVIS	Przekazanie projektu ustawy do uzgodnień wewnątrzresortowych. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas konsultacji wewnątrzresortowych.		
05PVIS	Przekazanie projektu ustawy do uzgodnień międzyresortowych. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas konsultacji międzyresortowych.		
06PVIS	Skierowanie projektu do opiniowania oraz konsultacji publicznych.		
07PVIS	Opracowanie projektów aktów wykonawczych		
08PVIS	Przekazanie projektu ustawy pod obrady Komitetu RM ds. Cyfryzacji Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KRMC.		
09PVIS	Przekazanie projektu pod obrady Komitetu RM ds. Europejskich. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KSE.		
10PVIS	Przekazanie projektu pod obrady Stałego Komitetu Rady Ministrów.		

	Uzgodnienia uwag do projektu ustawy zgłoszonych podczas SKRM.		
11PVIS	Przekazanie projektu pod obrady Komisji Prawniczej. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas KP.		
12PVIS	Przekazanie projektu pod obrady Rady Ministrów. Uzgodnienia uwag do projektu ustawy zgłoszonych podczas RM.		
13PVIS	Przekazanie projektu pod obrady Sejmu i Senatu. Uzgodnienia uwag do projektu ustawy zgłoszonych przez Sejm i Senat.		
14PVIS	Opracowanie przepisów wewnętrznych (procedury związane z wszystkimi aspektami odnoszącymi się do korzystania z VIS).	Wszyscy użytkownicy VIS	

Tabela 21. Główne ryzyka w projekcie dostosowania przepisów prawnych systemu VIS

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe przeciwdziałania	sposoby
Organizacyjno-prawne						
1	Ograniczone zasoby kadrowe		duże	duży	Potrzeba odpowiedniego zarządzania priorytetami przydzielonych zadań, uzyskanie wsparcia kadrowego, ustanowienie odpowiedniego systemu motywacyjnego.	
2	Wieloaspektowa złożoność przedmiotu regulacji pozostająca w zakresie właściwości wielu organów		średnie	duży	Właściwa koordynacja wymiany informacji	
3	Potrzeba dostosowania projektu do innych powstających systemów teleinformatycznych w ramach interoperacyjności		średnie	duży	Ścisła współpraca z zespołami odpowiedzialnymi za pozostałym systemy wielkoskalowe UE	
4	Przewlekłość procesu legislacyjnego realizowanego na poziomie krajowym mających wpływ na przepisy wewnętrzne.		duże	duży	Nadanie priorytetu działaniom legislacyjnym.	

7.11 PROJEKT 11: Dostosowanie przepisów prawnych systemu Eurodac

Koordynator: Komenda Główna Policji.

Uczestnicy: Komenda Główna Straży Granicznej, Urząd do Spraw Cudzoziemców, Rada do Spraw Uchodźców, Prezes Urzędu Ochrony Danych Osobowych.

Cel operacyjny: Przyjęcie krajowych przepisów regulujących funkcjonowanie zmodernizowanego systemu Eurodac w Polsce.

Kwestie zależne od decyzji co do podziału kompetencji w zakresie wdrażania rozporządzeń w ramach Paktu o Migracji i Azylu oraz Polityki Migracyjnej Państwa. Eurodac służy realizacji rozporządzenia UE 2024/1350 oraz rozporządzenia UE 2024/1351 objętych ww. Paktem migracyjnym, których wdrożenie nie wchodzi w zakres MasterPlanu. Analizie podlegać będzie uregulowanie kwestii technicznych oraz dostępu do systemu Eurodac przez polskie organy w zależności od wdrożenia do polskiego porządku prawnego ww. rozporządzeń UE, które odzwierciedlone zostaną najprawdopodobniej w Ustawie o Cudzoziemcach oraz ustawie o Udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej.

Tabela 22. Główne ryzyka w projekcie dostosowania przepisów prawnych systemu Eurodac

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe przeciwdziałania	sposoby
Organizacyjno-prawne						
1	Dostosowanie przepisów krajowych do rozporządzeń UE (2024/1350 oraz 2024/1351), których realizacji System Eurodac służy.	UdSC	duże	duży	Potrzeba zarządzania priorytetami przydzielonych zadań	
2	Wieloaspektowa złożoność przedmiotu regulacji pozostająca w zakresie właściwości wielu organów	Organy zaangażowane we wdrażanie Eurodac	średnie	duży	Właściwa koordynacja wymiany informacji	
3	Potrzeba dostosowania projektu do innych powstających systemów teleinformatycznych w ramach interoperacyjności	KGP	średnie	duży	Ścisła współpraca z zespołami odpowiedzialnymi za pozostałe systemy wielkoskalowe UE	
4	Przewlekłość procesu legislacyjnego realizowanego na poziomie krajowym mających wpływ na przepisy wewnętrzne.	MSWiA, KGP, krajowe organy mające dostęp do Eurodac	duże	duży	Nadanie priorytetu działaniom legislacyjnym.	

7.12 PROJEKT 12: Modernizacja infrastruktury TESTA-ng

Koordynator: Ministerstwo Spraw Wewnętrznych i Administracji

Uczestnicy: Organy administracji publicznej, służby, urzędy obsługujące organy oraz jednostki organizacyjne podległe tym organom lub przez nie nadzorowane.

Cel operacyjny: Umożliwienie dynamicznego zwiększania ilości użytkowników sieci TESTA-ng oraz zaspokojenie potrzeb sektora rządowego w obszarze zagwarantowania dostępu do usług teleinformatycznych UE przy zapewnieniu najwyższego poziomu zgodności z ramami regulacyjnymi UE i wymogami bezpieczeństwa, a także wzmocnienie cyberobrony i zwiększenie zdolności do szybkiego wykrywania i reagowania na operacje cybernetyczne.

Tabela 23. Zakres projektu Rozbudowa sieci TESTA-ng do poziomu ogólnokrajowego

Nr zadania	Nazwa Zadania	Odpowiedzialny	Termin
01TESTA	Rozbudowa węzłów o nowe moduły technologiczne	MSWiA	IV kwartał 2024 r.
02TESTA	Rozbudowa Polskiej Domeny Lokalnej (PDL) o nowe urządzenia agregujące ruch sieciowy	MSWiA	W oczekiwaniu na potwierdzenie terminu przez UE (prawdopodobnie II połowa 2025 r.)
03TESTA	Zmiana licencjonowania poszczególnych systemów odpowiadających za zarządzanie oraz bezpieczeństwo sieci	MSWiA	W oczekiwaniu na potwierdzenie terminu przez UE (prawdopodobnie II połowa 2025 r.)
04TESTA	Zakup urządzeń dostępowych\końcowych dla nowych użytkowników	MSWiA	W oczekiwaniu na potwierdzenie terminu przez UE (prawdopodobnie II połowa 2025 r.)

Tabela 24. Główne ryzyka w projekcie Rozbudowa sieci TESTA-ng do poziomu ogólnokrajowego

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
Zarządcze					
1	Problemy z koordynacją wdrażania	MSWiA	średnie	duży	Bieżące monitorowanie
2	Niewystarczające zasoby przeznaczone do realizacji zadania	MSWiA	średnie	średni	Zatrudnienie dodatkowych osób
Finansowe					
3	Koszty związane z zakupem urządzeń	MSWiA	średnie	duży	Zewnętrzne finansowanie, zwiększenie środków finansowych Ministerstwa
4	Koszty związane z dzierżawą łączy	MSWiA	średnie	duży	Zewnętrzne finansowanie, zwiększenie środków finansowych Ministerstwa

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe sposoby przeciwdziałania
5	Koszty związane z utrzymaniem sieci	MSWiA	średnie	duży	Zewnętrzne finansowanie, zwiększenie środków finansowych Ministerstwa
Organizacyjno-prawne					
6	Procedowanie porozumień	MSWiA + inne instytucje	małe	mały	Bieżące monitorowanie
Techniczne					
7	Czas realizacji/konfiguracji/dostarczenia urządzeń do miejsc docelowych	MSWiA	średnie	średni	Bieżące monitorowanie
8	Planowane terminy zadań 02-04 mogą pokrywać się z terminami testów w ramach projektu Eurodac oraz z testami oraz produkcyjnym startem ECRIS-TCN	MSWiA, KGP	małe	średni	Dokładne harmonogramowanie prac
Środowiskowe					
9	Kłęski żywiołowe, katastrofy, akty kryminalne, terroryzm, epidemia/pandemia	Wszyscy użytkownicy, MSWiA	średnie	średni	Bieżące monitorowanie.

8 Plan realizacji

8.1 Harmonogram realizacji

Poniższa tabela prezentuje ramowy harmonogram realizacji Programu.

Tabela 25. Ramowy harmonogram realizacji Programu

Nr	Nazwa Projektu	Termin	Uwagi
1	Modernizacja systemu SIS II	7 marzec 2023 r.	Zrealizowany
2	Modernizacja systemu VIS	II połowa 2026 r.	Nie można wykluczyć wystąpienia opóźnienia terminu wdrożenia spowodowanego problemami technicznymi po stronie Agencji eu-LISA bądź któregoś z państw członkowskich
3	Modernizacja systemu Eurodac	Czerwiec 2026 r.	Nie można wykluczyć wystąpienia opóźnienia terminu wdrożenia spowodowanego problemami technicznymi po stronie Agencji eu-LISA bądź któregoś z państw członkowskich
4	Wdrożenie systemu EES	Listopad 2024 r.	Nie można wykluczyć wystąpienia opóźnienia terminu wdrożenia spowodowanego problemami technicznymi po stronie Agencji eu-LISA bądź któregoś z państw członkowskich.
5	Wdrożenie systemu ETIAS	II połowa 2025 r.	Nie można wykluczyć wystąpienia opóźnienia terminu wdrożenia spowodowanego problemami technicznymi po stronie Agencji eu-LISA bądź któregoś z państw członkowskich.
6	Wdrożenie systemu ECRIS-TCN	III kwartał 2025 r.	Nie można wykluczyć wystąpienia opóźnienia terminu wdrożenia spowodowanego problemami technicznymi po stronie Agencji eu-LISA bądź któregoś z państw członkowskich.
7	Wdrożenie narzędzi Interoperacyjności Systemów	po 2026 r.	Nie można wykluczyć wystąpienia opóźnienia terminu wdrożenia spowodowanego problemami technicznymi po stronie Agencji eu-LISA bądź któregoś z państw członkowskich.
8	Dostosowanie przepisów prawnych systemu EES	Listopad 2024 r.	Zrealizowany
9	Dostosowanie przepisów prawnych systemu ETIAS	Kwiecień 2025 r.	

10	Dostosowanie przepisów prawnych systemu VIS	2026 r.	
11	Dostosowanie przepisów prawnych systemu Eurodac	Maj 2026 r.	
12	Modernizacja infrastruktury TESTA-ng	II połowa 2025 r.	

8.2 Prognoza finansowa

Istotną kwestią jest zapewnienie finansowania przedsięwzięcia. W załączniku nr 1 przedstawione są szacunki finansowe. Dokument nie przewiduje centralnego mechanizmu finansowania zadań. Realizacja przedsięwzięć powinna opierać się na otrzymanych limitach finansowych oraz pozyskanych środkach budżetowych i funduszy UE, zgodnie z standardową procedurą pozyskiwania dodatkowych środków finansowych.

8.3 Główne ryzyka

W wyniku dokonanej analizy została opracowana poniższa tabela zawierająca główne ryzyka przedsięwzięcia, które ujęte zostały w pięciu obszarach: zarządcze, finansowe, organizacyjno-prawne, techniczne oraz środowiskowe.

Ponadto istnieje ryzyko związane z opóźnieniem przyjęcia odpowiednich przepisów na szczeblu UE, opracowaniem dokumentacji technicznej (ICD) dla poszczególnych systemów, a także terminowym uruchomieniem systemów. W związku z tym, że ww. ryzyka nie można przydzielić do konkretnej instytucji na szczeblu krajowym, to nie zostało ono przedstawione w poniższej tabeli.

Tabela 26. Główne ryzyka dla Programu

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe przeciwdziałania sposoby
Zarządcze					
1	Przesunięcie terminów na poziomie unijnym	MSWiA, Zespół ds. Zapewnienia Współpracy Polskiej Administracji Rządowej z Wielkoskalowymi Systemami Informacyjnymi UE, Wszystkie instytucje wdrażające systemy	duże	duży	Monitorowanie

Nr	Opis ryzyka	Obszar kompetencji	Prawdopodobieństwo wystąpienia (małe/średnie/duże)	Wpływ (mały/średni/duży)	Możliwe przeciwdziałania sposoby
Finansowe					
2	Niewystarczające środki finansowe na realizację projektów z funduszy UE	Wszystkie instytucje wdrażające systemy	duże	duży	Opracowanie szczegółowego planu potrzeb finansowych
3	Niewystarczające środki finansowe na realizację projektów ze środków krajowych	Wszystkie instytucje wdrażające systemy	duże	duży	Opracowanie szczegółowego planu potrzeb finansowych
Organizacyjno-prawne					
4	Niewystarczające zasoby kadrowe do realizacji projektu	Wszystkie instytucje wdrażające systemy	duże	duży	Opracowanie szczegółowego planu potrzeb kadrowych w celach przekazania szczeblowi zarządzającemu programem; Dodatki motywacyjne
5	Długotrwałe procedury przetargowe mogące wpłynąć na terminowość realizacji zadań	Wszystkie instytucje wdrażające systemy	duże	duży	Wybór właściwych procedur przetargowych i bieżący monitoring; Kary finansowe dla wykonawcy za opóźnienia/niedotrzymanie terminów umowy
6	Przedłużające się prace legislacyjne na szczeblu krajowym	Wszystkie instytucje wdrażające systemy	duże	duży	Nadanie priorytetu działaniom legislacyjnym
Techniczne					
7	Niewystarczające możliwości/rozwiązania technologiczne po stronie potencjalnych wykonawców	Wszystkie instytucje wdrażające systemy	średnie	średni	Monitorowanie rynku usług IT w zakresie dostępnych rozwiązań technologicznych