

Bruksela, 6 czerwca 2016 r.
(OR. en)

9368/1/16
REV 1

LIMITE

JAI 478
COSI 92
FRONT 224
ASIM 80
DAPIX 80
ENFOPOL 157
SIRIS 90
DATAPROTECT 57
VISA 165
FAUXDOC 23
COPEN 172

NOTA

Od:	Prezydencja
Do:	Rada
Nr poprz. dok.:	8437/2/16 REV 2
Dotyczy:	Plan działania na rzecz intensyfikacji wymiany informacji i udoskonalenia zarządzania nimi, w tym na rzecz rozwiązań interoperacyjnych w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych

Niedawne zamachy terrorystyczne w Paryżu i Brukseli, ciągle zamachy terrorystyczne poza UE i obecny kryzys migracyjny pokazały, jak ważne dla sprostania wyzwaniom związanym z migracją, terroryzmem i przestępczością jest zaangażowanie na rzecz szybkiego, skutecznego i profesjonalnego zarządzania informacjami, ich wymieniania oraz podejmowania dalszych powiązanych z nimi działań. Już wcześniej potwierdziła to Rada w dniu 20 listopada 2015 r., Rada Europejska – w dniach 17 i 18 grudnia 2015 r., ministrowie sprawiedliwości i spraw wewnętrznych i przedstawiciele instytucji UE – w swoim oświadczeniu z dnia 24 marca, i wreszcie Rada w dniu 21 kwietnia 2016 r.

Wyzwania w zakresie bezpieczeństwa i migracji są złożone i powiązane ze sobą. Wysiłki mające na celu sprostanie im są już podejmowane w różnych dziedzinach WSiSW. Chodzi na przykład o skuteczne zarządzanie granicami będące integralnym elementem architektury bezpieczeństwa UE w dziedzinie zwalczania nielegalnej imigracji, terroryzmu i przestępczości.

Prezydencja podjęła ambitną inicjatywę zmierzającą do ustanowienia planu działania zawierającego niezbędne działania w celu poprawy zarządzania informacjami i transgranicznej wymiany informacji, w tym współdziałania systemów. Celem jest operacyjne wsparcie dochodzeń, zwłaszcza w dziedzinie zwalczania terroryzmu – z uwagi na fakt, że istnieje ścisły związek między terroryzmem a przestępczością – oraz szybkie przekazanie praktykom pierwszego kontaktu, takim jak policjanci, straż graniczna, oskarżyciele publiczni, urzędnicy imigracyjni i inni kompleksowych, aktualnych i rzetelnych informacji, co ma służyć skutecznej współpracy i działaniu.

Prezydencja rozpoczęła omawianie działań związanych ze zwalczaniem terroryzmu podczas nieformalnego posiedzenia Rady ds. WSiSW w dniu 25 stycznia 2016 r.; rozmawiała o tej kwestii także podczas posiedzenia Rady ds. WSiSW w dniu 21 kwietnia – część debaty była poświęcona komunikatowi Komisji pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”. Owocem tych wspólnych wysiłków – opartych również na wynikach i rozwoju sytuacji w UE – jest dokument zawarty w załączniku do niniejszej noty prezydencji.

Niniejszy dokument prezydencji to prezentacja **planu działania zawierającego konkretne, praktyczne krótko- i średnioterminowe działania, a także długoterminowe wytyczne mające usprawnić zarządzanie informacjami i wymianę informacji w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (WSiSW)**. Podstawą planu działania jest owocna współpraca prowadzona w ostatnich latach¹. Dokument ten ma być **dokumentem dynamicznym**.

¹ Chodzi np. o konkluzje Rady z 2013 r. oraz działania następcze związane z komunikatem Komisji na temat europejskiego modelu wymiany informacji (EIXM).

Dokument bierze pod uwagę wyniki niedawnych dyskusji w Radzie (Wymiar Sprawiedliwości i Sprawy Wewnętrzne w dniu 21 kwietnia², wspólne posiedzenie COSI i SCIFA w dniu 17 kwietnia, COSI w dniach 3–4 marca³ oraz DAPIX w dniach 26 stycznia i 15 marca 2016 r.⁴), jak również niedawno zaktualizowaną strategię w zakresie zarządzania informacjami⁵ i niedawny komunikat Komisji pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” z dnia 6 kwietnia 2016 r.⁶

Opracowanie niniejszego planu działania, wprowadzanie go w życie i monitorowania jego wyników, a także jego przeglądy i aktualizacje wymagają **wspólnego podejścia ze strony Rady, Komisji, Koordynatora UE ds. Zwalczania Terroryzmu oraz agencji UE w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych. Dokument ma być wsparciem w dochodzeniach operacyjnych i wsparciem dla praktyków – pracujących na ulicach, na przejściach granicznych, prowadzących dochodzenia, pomagających migrantom oraz rozpatrującym wnioski wizowe – w skutecznym i wydajnym pełnieniu ich codziennych obowiązków.**

Niniejszy plan działania to dokument dynamiczny – przedstawiono w nim **spójne ramy bardziej zintegrowanej architektury informacyjnej UE⁷ w dziedzinie WSiSW** oraz zawarto analizę najważniejszych poważnych wyzwań w tym obszarze, zasady i wytyczne horyzontalne oraz sposoby monitorowania i kontynuacji działań w nim opisanych (**Rozdział 1**). Plan przewiduje również specjalne działania dotyczące wymiany informacji i zarządzania informacjami w niżej wymienionych dziedzinach, przy czym bierze pod uwagę różnice w przepisach regulujących te obszary:

- **egzekwowanie prawa, w tym współpraca wymiarów sprawiedliwości w sprawach karnych (rozdział 2),**
- **wykrywania osób zaangażowanych w działalność terrorystyczną i ich podróży (rozdział 3),**
- **zarządzanie granicami i migracja (rozdział 4).**

² Dok. 7711/16 JAI 264 COSI 54, 7726/16 JAI 266 COSI 55.

³ Dok. DS 1129/16.

⁴ Dok. 5180/16 JAI 20 DAPIX 5.

⁵ Konkluzje Rady z 2014 r. i działania następcze w sprawie aktualizacji strategii zarządzania informacjami do celów ochrony bezpieczeństwa wewnętrznego UE.

⁶ Dok. 7665/16 JAI 258 ASIM 50 RELEX 239.

⁷ Tworzenie zintegrowanej architektury informacyjnej jest procesem podlegającym ciągłej ewolucji, co wymaga wspólnego wysiłku i czasu, oraz uwzględnienia różnic pomiędzy państwami członkowskimi, obszarami polityki, warunkami prawnymi, wymogami technicznymi i finansowymi, a także czynnika ludzkiego.

Chociaż wspomniane trzy rozdziały (rozdziały 2, 3 i 4) koncentrują się na różnych obszarach, ważne jest, aby w planie działania zwrócić uwagę na ich wzajemne powiązania. Przyczyni się to do zapewnienia współpracy między organami i agencjami, które zajmują się tymi trzema dziedzinami polityki oraz do interoperacyjności systemów informacyjnych.

Prezydencja proponuje następujące strategiczne kwestie, które mają posłużyć jako punkt wyjścia do dalszej dyskusji politycznej i i jako wytyczne polityczne, w pełni świadoma faktu, że ministrowie sprawiedliwości i spraw wewnętrznych w dniu 24 marca 2016 r. podjęli decyzję o dalszej intensyfikacji wdrażania już przyjętych środków:

- Przede wszystkim prezydencja dąży do ustanowienia zobowiązania politycznego do zasilania danymi i wykorzystywania systemów informacyjnych w maksymalnym zakresie, jako bezwzględnego warunku skutecznej wymiany informacji. Zobowiązanie polityczne do zasilania danymi i wykorzystywania istniejących systemów danych oraz do innych stosownych działań zwiększy zaufanie między podmiotami operacyjnymi (zmiany w wyzwaniach w dziedzinie WSiSW, którym czoła stawić muszą państwa członkowskie, mogą mieć wpływ na ilość wymienianych informacji). Prezydencja dąży do ustanowienia zobowiązania politycznego zakładającego wymianę wszelkich stosownych informacji, chyba że wymiana taka nie jest wskazana ze względów prawnych lub operacyjnych. Przy ocenie, czy takie względy mają zastosowanie, w pełni uwzględniane jest to, jaki interes operacyjny w otrzymaniu informacji mają inne państwa członkowskie i w stosownych przypadkach agencje UE. Koordynator UE ds. Zwalczenia Terroryzmu powinien regularnie przedstawiać informacje na temat faktycznego zasilania danymi i wykorzystywania istniejących systemów danych z uwzględnieniem informacji przekazywanych przez Komisję i właściwe agencje, co ma służyć świadomemu wyciąganiu wniosków i wspieraniu stałej poprawy. W tym kontekście oczywiste jest, że ogromne znaczenie ma zdolność państw członkowskich do zbierania informacji, zwłaszcza w następstwie wskazówek wywiadowczych na temat potencjalnych terrorystów, oraz do oceny ogólnego zagrożenia terroryzmem.

- Ochrona prywatności i ochrona danych to podstawowe wartości, podstawowe prawa i normy w UE. Państwa członkowskie są zobowiązane chronić obywateli UE i zapewniać im bezpieczeństwo. Dlatego ochrona obywateli i zasady ochrony prywatności i ochrony danych uzupełniają się i wzajemnie wzmacniają. W celu zachowania równowagi należy wziąć w pełni pod uwagę nowe metody ochrony informacji i możliwość udzielania zróżnicowanych praw dostępu do jednego systemu. Należy to poprzedzić dogłębną analizą potrzeb informacyjnych wynikających z procedur stosowanych w kontekście egzekwowania prawa, walki z terroryzmem, migracji i zarządzania granicami. Warunki te są uwzględniane przez Komisję przy opracowywaniu nowych wniosków ustawodawczych dotyczących SIS, VIS i Eurodac, w szczególności jeśli chodzi o dostęp do tych systemów do celów egzekwowania prawa i zwalczania terroryzmu.
- W kontekście interoperacyjności, która jest kwestią złożoną, duże znaczenie ma pojedynczy interfejs wyszukiwania. Powinno to być realizowane przede wszystkim poprzez rozwiązania na szczeblu krajowym i europejskim dotyczące punktów kompleksowej informacji służących za pojedyncze interfejsy dla państw członkowskich wykorzystywane do zasilania danymi i przeszukiwania krajowych i międzynarodowych systemów informacyjnych. Biorąc pod uwagę potrzeby informacyjne poszczególnych organów, pojedynczy interfejs wyszukiwania to znaczne ułatwienie dla funkcjonariuszy straży granicznej, policji, urzędników imigracyjnych i celnych, którzy prowadzą kontrole, także w kontekście dochodzeń operacyjnych. W komunikacie Komisji pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” wymieniono trzy inne wymiary interoperacyjności (czyli: wzajemne połączenia między systemami informacyjnymi, stworzenie wspólnej funkcji porównywania danych biometrycznych, która obsługiwałaby różne systemy informacyjne, oraz wspólne repozytorium danych dla różnych systemów informacyjnych), które również muszą zostać przeanalizowane w średniej i dłuższej perspektywie czasowej. Powołana przez Komisję grupa ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności powinna przeanalizować i rozwinąć wnioski dotyczące konsekwencji prawnych, technicznych, operacyjnych i finansowych wszystkich czterech wymiarów, a także kwestię priorytetowego traktowania inicjatyw dotyczących interoperacyjności. Postępy prac i wyniki należy omówić na forum COSI oraz, w stosownych przypadkach, na forum innych organów Rady.

- Do czasu znalezienia ostatecznych rozwiązań konieczne jest znalezienie możliwych rozwiązań krótko- i długoterminowych w zakresie dostarczania informacji i dostępu do unijnych baz danych, aby wypełnić lukę istniejącą między państwami członkowskimi należącymi do strefy Schengen, państwami członkowskimi spoza tej strefy i państwami członkowskimi, które częściowo korzystają z dorobku Schengen. Powinno to zostać wzięte pod uwagę przez Komisję w nowym wniosku legislacyjnym dotyczącym SIS i VIS. Do tego czasu nie należy jednak ustawać w poszukiwaniu rozwiązań technicznych pozwalających wypełnić tę lukę.
- Istnieje wyraźna potrzeba postępów na rzecz aktywnej i systematycznej wymiany, w szczególności z właściwymi organami na granicach, danych z rejestrów karnych osób skazanych za przestępstwa związane z terroryzmem oraz z poważną i zorganizowaną przestępczością. Należy rozważyć, jakie praktyczne kroki mogą pomóc to osiągnąć, w tym jakie systemy (poza systemem ECRIS) oferują najskuteczniejsze rozwiązania w tej kwestii.

Ponieważ do zapewnienia, że informacje są wymieniane w sposób skuteczny i w czasie rzeczywistym, konieczne są konkretne działania, prezydencja zwraca się do Rady o:

- ***zatwierdzenie ram polityki, zwłaszcza zasad wymiany informacji, oraz zatwierdzenie działań (będących w toku i nowych), a następnie terminów, biorąc pod uwagę, że jest to dokument dynamiczny, który może podlegać korektom w obliczu przyszłych wydarzeń i wiedzy.***
Postępy mają być strategicznie monitorowane przez COSI we współpracy z innymi stosownymi organami przygotowawczymi Rady, Komisją i Koordynatorem UE ds. Zwalczania Terroryzmu, na podstawie sprawozdań z postępów przygotowywanych przez COSI we współpracy z Koordynatorem ds. Zwalczania Terroryzmu, prezydencją i Komisją. Rada będzie regularnie informowana o poczynionych postępach oraz w każdym przypadku, gdy niezbędne będą decyzje polityczne; oraz
- *wyrażenie zgody na zapewnienie, by unijne i międzynarodowe bazy danych były prawidłowo wypełniane i wykorzystywane przez krajowe organy odpowiedzialne za walkę z terroryzmem, egzekwowanie prawa, migrację i zarządzanie granicami. Jakość wymienianych informacji jest równie ważna co ich ilość. Monitorowanie będzie prowadzone przez COSI, z uwzględnieniem ocen Schengen, w ścisłej współpracy z Komisją i Koordynatorem UE ds. Zwalczania Terroryzmu. COSI będzie składać sprawozdania Radzie ds. WSiSW.*

ROZDZIAŁ 1: RAMY BARDZIEJ ZINTEGROWANEJ UNIJNEJ ARCHITEKTURY INFORMACYJNEJ

1. *Wyzwania*

Funkcjonariusze pierwszej linii muszą sprostać szeregowi wyzwań i aby podjąć skuteczne działania, potrzebują dostępu do informacji. Często potrzebują podobnych lub nawet identycznych informacji, np. szczegółowych informacji na temat osób lub towarów, które osoby te mają przy sobie lub które przewożą, środków finansowych czy bardziej szczegółowych informacji o sytuacji osób i ewentualnych sieci powiązań. Aby skutecznie wykonywać swoje zadania, funkcjonariusze muszą stosować wszystkie uzgodnione gwarancje, zwłaszcza te dotyczące praw podstawowych, a także gromadzić, weryfikować i dopasowywać właściwe informacje we właściwym czasie i w odpowiednim miejscu, by podejmowane przez nich działania były skuteczne.⁸

Do tych celów na szczeblu krajowym, unijnym i międzynarodowym udostępniono im instrumenty prawne, polityczne, operacyjne i techniczne. Jednak zarówno na szczeblu krajowym, jak i europejskim istnieją różne prawne, techniczne i operacyjne problemy, jeśli chodzi o interoperacyjność systemów, różne grupy użytkowników oraz różne okresy przechowywania danych osobowych i biometrycznych w tych systemach. Ponadto wszechobecne jest ryzyko polegające na lukach w istotnych informacjach dostępnych wśród (kategorii) praktyków, na przykład ze względu na

- a) ograniczoną dostępność informacji (np. o konkretnych kategoriach podróżujących terrorystów);
- b) ograniczony dostęp do informacji lub ograniczone terminy na identyfikację i kontrolę osób na granicach (np. z powodu złożonej podstawy prawnej lub ze względów technicznych);
- c) fakt, że państwa członkowskie i ich organy nie są połączone z systemami;
- d) nieoptymalną wymianę informacji z powodu zbyt restrykcyjnego stosowania zasady ograniczonego dostępu, co ma wpływ zwłaszcza na prowadzone dochodzenia oraz na możliwość podjęcia natychmiastowych działań.

⁸ Na podstawie konkluzji Rady w sprawie unijnej strategii dotyczącej zarządzania informacjami.

Sytuację tę wywołują następujące czynniki:

1. **Czynnik ludzki:** informacje mogą być skutecznie wymieniane tylko wtedy, gdy między praktykami na szczeblu krajowym i międzynarodowym istnieje zaufanie (w tym zaufanie między różnymi strukturami organizacyjnymi/institutionalnymi). Ponadto przyczynami błędów mogą być złożoność dostępnych narzędzi i procedur, różne tradycje w obszarze egzekwowania prawa, a także różny poziom wiedzy praktyków.
2. **Wymogi prawne (konstytucyjne),** takie jak prawo karne procesowe, wymogi z zakresu ochrony danych, zasada celowości itp. Systemy informacyjne i procedury wymiany informacji zostały opracowane w różnych kontekstach instytucjonalnych, prawnych i politycznych. Warunki te mają charakter wiążący, są merytorycznie ważne i dobrze uzasadnione przez proces legislacyjny w oparciu o wspólnie określone potrzeby. Mają jednak wpływ na to, co jest i powinno być możliwe w zakresie wymiany informacji i działań następczych, które należy podjąć, na przykład ze względu na różne parametry baz danych, rozbieżności w dostępie do danych właściwych organów i brak informacji o trafieniu/braku trafienia.
3. **Ograniczone zasoby** (personel, środki finansowe i czas) na szczeblu krajowym i europejskim. W rezultacie praktycy i reprezentowane przez nich organy mogą mieć trudności ze stawieniem czoła wszystkim wyzwaniom.
4. Brak ustalonych w niezbędnym stopniu **wymogów technicznych/systemowych** w odniesieniu do szybkich i skutecznych działań w zakresie zarządzania informacjami i wymiany informacji, w szczególności w zakresie międzyinstytucjonalnej wymiany danych; istnieją ponadto niedociągnięcia, jeśli chodzi o funkcje istniejących systemów informacyjnych. Ta druga kwestia wynika częściowo z tego, że obecnie użytkowane systemy (np. SIS II, VIS, Eurodac, ECRIS i inne) nie zostały stworzone w oparciu o podejście systemowe ani o pełne analizy procesów pracy planowanych użytkowników, lecz jako rozwiązanie konkretnych problemów w określonych dziedzinach.

5. **Istniejące ustawodawstwo⁹, polityki¹⁰ i procedury¹¹ w zakresie zarządzania informacjami i wymiany informacji przez UE w dziedzinie WSiSW nie są w pełni wdrażane**, a zdolności agencji WSiSW nie są w pełni wykorzystywane do wspierania państwa członkowskich.

2. *Zasady*

Aby usprawnić zarządzanie informacjami i ich wymianę oraz działania następcze prowadzone w oparciu o uzyskane dane wywiadowcze, należy wypracować spójne zintegrowane podejście zgodnie z następującymi zasadami:

A. **Pełne poszanowanie praw podstawowych i zasad ochrony danych**

Wymogi: poddawanie stałej ocenie konieczności zastosowania danego środka; stosowanie zasad pomocniczości i proporcjonalności oraz właściwe zarządzanie ryzykiem. W tym celu konieczne będzie również uwzględnienie ochrony danych osobowych w podstawie technicznej proponowanego instrumentu (zasada uwzględniania ochrony prywatności już w fazie projektowania), ograniczenie przetwarzania danych do tego, co jest niezbędne do określonego celu, a jednocześnie niepomijanie informacji istotnych z operacyjnego punktu widzenia oraz operacyjne i prawne uzasadnienie potrzeby posiadania przez (daną kategorię) praktyków (danego zakresu) dostępu do informacji.

⁹ Np. decyzje Prüm, szwedzka decyzja ramowa.

¹⁰ Np. konkluzje Rady w sprawie komunikatu Komisji na temat europejskiego modelu wymiany informacji (EIXM) (z 6–7 czerwca 2013 r. – dok. 9811/13), konkluzje Rady w sprawie zaktualizowanej strategii zarządzania informacjami do celów ochrony bezpieczeństwa wewnętrznego UE (z 5 grudnia 2014 r. – dok. 15701/1/14 REV 1), konkluzje Rady UE i państw członkowskich zebranych w Radzie w sprawie zwalczania terroryzmu (20 listopada 2015 r.).

¹¹ Podręcznik dotyczący wymiany informacji między organami ścigania, podręcznik Sirene.

B. Podejście ukierunkowane na informacje, oparte na analizie procesów

Warunek wstępny: ciągłe dążenie do przestrzegania zasady dostępności, w tym warunków towarzyszących¹², zasady równego dostępu oraz jakości informacji na szczeblu krajowym, europejskim i międzynarodowym. Wymogi: dostępność informacji dla wszystkich odpowiednich właściwych organów, z należyтым uwzględnieniem kwestii ochrony danych, która to dostępność służy także wspieraniu strategicznego wykorzystania informacji do celów zapobiegania zagrożeniom, analizy (ryzyka), podejmowania decyzji i ustalania priorytetów działania, większe skupienie się na jakości danych, w tym jasność co do tego, jaki rodzaj informacji (pod względem tematycznym) należy udostępniać i do jakich celów, z poszanowaniem przejrzystych kryteriów i w sposób umożliwiający skuteczne działania następcze; skupienie się na pozostałych elementach nakreślonych w niedawno zaktualizowanej strategii zarządzania informacjami do celów ochrony bezpieczeństwa wewnętrznego UE.¹³

C. Podejście ukierunkowane na praktyków, oparte na zaufaniu i potrzebach operacyjnych

Wymogi: ciągłe inwestowanie we wzajemne zaufanie na wszystkich szczeblach; projektowanie oddolne aktywnie koncentrujące się na procesach informacyjnych i instrumentach towarzyszących przyjaznych dla użytkownika, w których punktem wyjścia dla organów opracowujących rozwiązania jest codzienna praktyka w terenie; położenie nacisku na szkolenie w zakresie skutecznego wypełniania poszczególnych ról w przekazywaniu informacji (na szczeblu międzynarodowym); refleksja nad skutecznością istniejących praktyk oraz podstawowymi przyczynami nieprawidłowości powinna mieć charakter ciągły; między państwami członkowskimi powinna mieć miejsce wymiana – poprzez szkolenia, spotkania, katalogi i z wykorzystaniem internetu – dobrych praktyk w kwestii przyjazności systemów i procesów informacyjnych dla użytkowników.

¹² Te warunki towarzyszące to: a) wymiana może mieć miejsce wyłącznie w celu umożliwienia wykonania zadań prawnych, które są proporcjonalne i niezbędne; b) należy zagwarantować integralność danych, które mają być wymieniane; c) potrzeba ochrony źródeł informacji i zapewnienia poufności danych na wszystkich etapach wymiany; d) należy zapewnić nadzór nad przestrzeganiem ochrony danych oraz odpowiednią kontrolę przed wymianą i po jej przeprowadzeniu; e) poszczególne osoby muszą być chronione przed nadużyciem danych oraz mają prawo do domagania się korekty niepoprawnych danych.

¹³ Dok. 15701/1/14.

D. Pełne wdrożenie i wykorzystywanie istniejących narzędzi w zakresie zarządzania informacjami i wymiany informacji oraz podejmowanie uzasadnionych decyzji w kwestii nowych inicjatyw

Warunek wstępny: zgromadzenie wystarczających doświadczeń płynących z pełnego wykorzystania potencjału instrumentów już istniejących oraz ocena ich skuteczności; spójność we wdrażaniu i stosowaniu instrumentów. Wymogi: stałe monitorowanie na szczeblu Komisji (np. poprzez oceny Schengen i mechanizmy monitorowania) oraz Rady. Działania te powinny być dla władz podstawą wiedzy przy opracowywaniu nowych inicjatyw w odpowiedzi na zmieniające się potrzeby operacyjne.

E. Skuteczne zapewnianie wzajemnych połączeń między inicjatywami europejskimi a procesami krajowymi

Warunek wstępny: istnienie spójnych zintegrowanych krajowych architektur informacyjnych. Wymogi: dążenie do standaryzacji wymogów, np. dotyczących jakości, dostarczania i przeszukiwania danych, oraz zapewnianie specjalnie dostosowanych (krajowych) rozwiązań służących włączaniu systemów międzynarodowych do krajowego środowiska informacyjnego, a jednocześnie uwzględnianie podczas opracowywania tych rozwiązań dwustronnych i międzynarodowych procesów wymiany informacji. To państwa członkowskie są przede wszystkim odpowiedzialne za gwarantowanie spójności w ramach wszystkich tych procesów, reagowanie na potrzeby operacyjne i zapewnianie niezbędnych specjalnie dostosowanych rozwiązań.

F. Dążenie do systematycznej wymiany informacji z innymi państwami członkowskimi oraz agencjami i organami UE

Warunki wstępne: systematyczna wymiana informacji umożliwiająca dokonywanie analizy w czasie rzeczywistym, przy uwzględnieniu niezbędnych zdolności i transgranicznych działań operacyjnych – służąca uniknięciu luk informacyjnych i niepowielaniu działań; efektywna wymiana informacji między agencjami UE (chodzi zwłaszcza o Europol, Eurojust i Frontex), w przypadkach gdy ich mandaty oraz przepisy prawne przewidują taką możliwość. Wymogi: pełne wzięcie pod uwagę odnośnych mandatów, uzasadnione powody operacyjne i prawne nieudostępniania informacji (zwolnienia¹⁴), stosowanie stale krytycznego podejścia do takich zwolnień, uwzględniającego fakt, że okoliczności szybko się zmieniają oraz że należy wykorzystać dogodny moment na dokonaną w odpowiednim czasie wymianę informacji, gdyż może się on nie powtórzyć.

¹⁴ Art. 4 TUE oraz art. 72 i 73 TFUE oraz ochrona źródeł, ochrona trwającego dochodzenia, unikanie sytuacji zagrażających życiu, brak zezwolenia na wymianę informacji dostarczonych przez stronę trzecią.

G. Zarządzanie informacjami i wymiana informacji pozostają środkiem do osiągnięcia celu¹⁵

Wymogi: określone priorytety w zakresie zarządzania informacjami i wymiany informacji muszą odpowiadać potrzebom i priorytetom operacyjnym; należy dążyć do jak najbardziej operacyjnych i opłacalnych rozwiązań i do jasnego podziału obowiązków również na szczeblu krajowym i do skutecznego wspierania i monitorowania międzynarodowej wymiany informacji oraz do jak najmniejszych obciążeń administracyjnych.¹⁶

3. Wytyczne horyzontalne

Oprócz powyższych zasad oraz działań przedstawionych w poszczególnych rozdziałach, należy rozważyć następujące wytyczne horyzontalne, przy czym priorytetowo należy potraktować dwie pierwsze kwestie.

- **Po opracowaniu danego(-ych) rozwiązania(-ń) technicznego(-ych) dążyć do rozwiązań interoperacyjnych, obejmujących pojedynczy interfejs, lecz niekoniecznie ograniczających się tylko do niego.** Warunkiem wstępnym takiego działania jest pełne wzięcie pod uwagę i umożliwienie stosowania wymogów w zakresie ochrony danych i przepisów dotyczących wzajemnej pomocy prawnej oraz skrupulatnego wdrażania zasady odnoszącej się do właściciela danych. Takie rozwiązania mogą zapewnić wzrost wydajności w zakresie dostarczania oraz przeszukiwania informacji i zwracania się o nie, lecz jednocześnie powinny one zapewniać, by właściwe agencje UE mogły wypełniać swój mandat i wspierać państwa członkowskie.¹⁷ Należy zaproponować rozwiązania w zakresie jednego wyszukiwania, opierając się na istniejących już dobrych praktykach dostępnych na poziomie krajowym i międzynarodowym. Jeśli chodzi o wdrożenie, zastosowanie ma działanie 4 w rozdziale 2.

¹⁵ Dok. 16637/09 + COR 1.

¹⁶ W dziedzinie współpracy policyjnej: pojedynczy punkt kontaktowy (Single Point of Contact – SPOC) w każdym państwie członkowskim, jako działający non stop punkt kompleksowej obsługi w dziedzinie międzynarodowej współpracy policyjnej.

¹⁷ Przykłady technologii: w przypadku Sieci Jednostek Analityki Finansowej – zastosowanie technologii MA3TCH, a w przypadku obecnej listy działań w ramach strategii zarządzania informacjami – projekt dotyczący automatyzacji wymiany danych (ADEP).

- **Zbadać wartość dodaną i wymogi, jeśli chodzi o funkcję kojarzenia danych biometrycznych wspólną dla wszystkich odnośnych systemów informacyjnych.**¹⁸ Interoperacyjność identyfikatorów biometrycznych umożliwia stosowanie funkcji kojarzenia danych biometrycznych wspólnej dla kilku systemów informacyjnych i zwiększy zdolność organów do dokładnego sprawdzenia tożsamości danej osoby. Taka funkcja powinna być zgodna z zasadami ochrony danych osobowych. Grupa ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, która zostanie powołana przez Komisję, jest proszona o zbadanie tej kwestii i poinformowanie Rady o swoich ustaleniach.
- **Na wyraźny wniosek Rady zbadać skutki prawne, techniczne, operacyjne i finansowe:**
 - a) **połączeń międzysystemowych, dzięki którym systemy mogą nawzajem przeszukiwać swoją zawartość, w stosownych przypadkach i z zastrzeżeniem zasady, zgodnie z którą właściciel danych zachowuje kontrolę nad dostarczaniem przez siebie danymi;**
 - b) **wspólnego repozytorium danych (rozwiązań dotyczących architektury na szczeblu zdecentralizowanym lub scentralizowanym – do określenia).** Repozytorium umożliwiłoby rozpoznanie powiązań i uzyskanie całościowego obrazu poprzez połączenie poszczególnych elementów danych przechowywanych w różnych zdecentralizowanych systemach informacyjnych, a tym samym uzupełnienie luk informacyjnych.

Na wyraźny wniosek Rady grupa ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, powołana przez Komisję, jest proszona o podjęcie działań służących określeniu skutków i o poinformowanie Rady o swoich ustaleniach.
- **Zapewnić synergie zarządzania ryzykiem przez organy celne¹⁹ z informacjami będącymi w posiadaniu agencji WSiSW.** Przyczyni się to do intensywniejszej współpracy międzyagencyjnej i zwiększonej wymiany danych między organami celnymi a organami WSiSW na szczeblu państw członkowskich i na szczeblu unijnym w powiązanych z handlem przypadkach dotyczących zwalczania terroryzmu oraz poważnej i zorganizowanej przestępczości. W strategii zarządzania ryzykiem w ramach unii celnej zawiera się wymiana informacji, analiza tendencji w zakresie nadużyć finansowych oraz wiedza fachowa w dziedzinie współpracy organów celnych z policją i strażą graniczną. To warunki wstępne efektywnego wnoszenia przez urzędy celne wkładu w obszar bezpieczeństwa.

¹⁸ Dok. 7665/16 JAI 258 ASIM 50 RELEX 239.

¹⁹ Strategia UE i plan działania w zakresie zarządzania ryzykiem celnym, COM(2014) 527.

W planie działania towarzyszącym strategii zarządzania ryzykiem celnym przewidziano konkretne działanie obejmujące: opracowanie ustaleń dotyczących współpracy międzysektorowej, usprawnienie wymiany informacji (o ryzyku) i poprawę dostępności takich informacji oraz zaangażowanie organów celnych w oceny ryzyka i zagrożeń. Organy WSiSW i organy celne muszą współpracować, by zapewnić osiągnięcie rezultatów tego działania w określonym terminie.

- **Rozpocząć długoterminową inicjatywę – przede wszystkim poprzez ocenę potrzeb państw członkowskich i agencji UE – służącą opracowaniu spójnego podejścia do wymiany informacji z państwami trzecimi i organizacjami**, przy pełnym uwzględnieniu praw podstawowych oraz przepisów ogólnego unijnego ustawodawstwa dotyczącego ochrony danych, a także określonych systemów ochrony danych stosowanych w agencjach UE. Zbieranie, wymiana i łączenie informacji przekracza zdolności UE; należy zapewnić wzmocnienie tych działań wspólnie z państwami trzecimi i organizacjami międzynarodowymi, zważywszy na wyzwania w dziedzinie WSiSW.

Szefowie unijnych agencji WSiSW są proszeni o zastanowienie się wspólnie z organami zarządzającymi macierzystych agencji, w których to organach uczestniczą państwa członkowskie i Komisja, nad elementami, które mogą posłużyć za podstawę dla rozpoczęcia tej inicjatywy i o poinformowanie COSI o wnioskach. Następnie COSI powinien kontynuować inicjatywę, przy uwzględnieniu kompetencji państw członkowskich.

4. Dalsze działania

Plan działania i towarzyszące mu działania będą na poziomie centralnym i strategicznym monitorowane przez Stały Komitet Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego (COSI). Poszczególne działania będą monitorowane przez odnośne wyspecjalizowane organy Rady (np. SCIFA, Grupę Roboczą ds. Terroryzmu, Grupę Roboczą ds. Wymiany Informacji i Ochrony Danych, Grupę Roboczą ds. Granic, Grupę Roboczą ds. SIS i Sirene, Grupę Roboczą ds. Współpracy w Sprawach Karnych i Grupę Roboczą ds. Współpracy Celnej), organy Komisji, a także organy zarządzające agencji UE, zgodnie z tym, co określono w planach tych działań; organy te będą regularnie składać sprawozdania COSI. Monitorowanie będzie w pełni uwzględniać kompetencje i zakres odpowiedzialności Komisji w kwestii monitorowania i działań następczych w odniesieniu do wdrażania unijnego prawodawstwa.

Grupa ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, która zostanie powołana przez Komisję, jest proszona o zaproponowanie wymogów prawnych, technicznych, finansowych i operacyjnych na rzecz interoperacyjności systemów informacyjnych. Posiłkując się wnioskami grupy ekspertów, Komisja przedstawi Radzie i Parlamentowi Europejskiemu dalsze szczegółowe pomysły dotyczące dalszych działań, które obejmowałyby również działania wspierające wdrażanie, a także przegląd i dostosowanie przedmiotowego planu.

Co roku COSI w sposób kompleksowy określi postępy w realizacji planu działania i towarzyszących mu szczegółowych planów działań, wskaże główne przeszkody oraz zaproponuje dalsze działania, a w stosownych przypadkach zwróci się do Rady o wskazówki polityczne. Działania te zostaną podjęte przez inne organy, które będą przekazywać informacje COSI, tak by mógł on wypełnić swoją rolę w zakresie monitorowania.

ROZDZIAŁ 2: ZARZĄDZANIE INFORMACJAMI I WYMIANA INFORMACJI W OBSZARZE EGZEKWOWANIA PRAWA, W TYM WSPÓŁPRACY WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH

Temat 1 Ukierunkowane na informacje podejście do egzekwowania prawa

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
1	Określić przeszkody operacyjne i prawne, by poprawić dostępność informacji i dalsze działania	Podjąć analizę luk i potrzeb wśród organów ścigania w państwach członkowskich, m.in. prokuratur, unijnych agencji ds. wymiaru sprawiedliwości i spraw wewnętrznych oraz organów celnych, z punktu widzenia prawnego, operacyjnego, behawioralnego i informatycznego/technicznego, pod kątem dostępności informacji w istniejących i tworzonych instrumentach informacyjnych UE, by określić, co jest zbędne i nieuwzględniane. Analiza ta powinna obejmować dogłębną ocenę faktycznych przeszkód operacyjnych i prawnych (także sposobu, w jaki stosuje się zasady) oraz wyzwań, by ulepszyć działania w następstwie wymiany informacji w systemach egzekwowania prawa i wymiaru sprawiedliwości w sprawach karnych oraz by poszukiwać ewentualnych połączeń z systemami zarządzania granicami. <i>Nie są wymagane zmiany prawa (ewentualnie przy dalszych działaniach)</i>	Komisja (grupa ekspertów wysokiego szczebla) państwa członkowskie	Europol Eurojust Frontex eu-LISA FRA	2017	COSI	budżet Komisji (nie w ramach unijnych programów finansowania)

Dodatkowe uwagi: Złożony charakter bieżących problemów z zakresu egzekwowania prawa i, co za tym idzie, wielu zmieniających się zadań dla praktyków, ma wpływ na potrzebę pozyskiwania i analizowania/sprawdzania informacji. W rezultacie może to spowodować zaistnienie potrzeby szerszego dostępu do danych w dziedzinie migracji lub zwiększenia efektywności procesu wymiany informacji między dziedzinami migracji i egzekwowania prawa. Oprócz tego rozszerzenie praw dostępu na dany system może ograniczyć potrzebę przechowywania informacji w innych systemach, co z kolei może zlikwidować nadmiar informacji i w rezultacie stworzyć korzyści dla ochrony danych. Niedawno na różnych szczeblach Rady rozpoznano i podkreślono pewną liczbę przeszkód. Podjęcie takiego działania byłoby próbą uzupełnienia obrazu, zapewniając uwzględnienie wszystkich ewentualnych luk.

Zob. konkluzje Rady w następstwie komunikatu Komisji na temat europejskiego modelu wymiany informacji (EIXM) z dnia 6 i 7 czerwca 2013 r. (9811/13).

Zbieranie, sprawdzanie i łączenie informacji powinno prowadzić do dalszych działań operacyjnych, takich jak działania po uzyskaniu trafienia, kroki dochodzeniowe, działania kontrolne, identyfikacja osób lub przepływów finansowych i inne działania. Etapów tych nie można łatwo rozróżnić. Jednak podstawową przesłanką wszystkich tych etapów są dostateczne, wyraźnie określone informacje (w tym informacje uzupełniające), dzięki którym można ustalić, jakie podjąć działanie. Jest to niezwykle ważne, by zapewnić właściwe wykorzystywanie ograniczonych zasobów i nie dopuszczać do niewłaściwie ukierunkowanych lub nieskutecznych działań. Niedawno na różnych forach Rady ustalono i podkreślono pewną liczbę przeszkód. Działanie to miałooby na celu uzupełnienie obrazu, zapewniając uwzględnienie wszystkich ewentualnych luk.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
2	Ulepszać jakość danych / informacji	a) W ramach odnośnego organu zarządzającego / odnośnej grupy roboczej zaproponować, omówić i uzgodnić wspólny zestaw norm (egzekwowanie prawa, organy, prokuratura) (wprowadzanie danych i zadawanie pytań) dotyczących jakości danych / informacji b) eu-LISA ma opracować centralne monitorowanie jakości danych. c) Rozpowszechniać między państwami członkowskimi normy jakości danych z pomocą wspólnych podręczników, najlepszych praktyk i wiedzy fachowej; eu-LISA ma przekazywać państwom członkowskim i innym agencjom UE z dziedziny WSiSW wiedzę fachową dotyczącą centralnego monitorowania jakości danych, przy pełnym uwzględnianiu uprawnień państw członkowskich i innych agencji UE z dziedziny WSiSW do ustalania jakości monitorowania informacji. <i>A i B: Ewentualna potrzeba zmian/kroków prawnych; C: Nie są wymagane zmiany prawa</i>	państwa członkowskie Europol, Eurojust, Frontex, eu-LISA	Komisja	A i C) 2018 B) 2018/2019 lub wcześniej, w zależności od potrzeby zmian prawnych w mandacie eu-LISA	Grupa Robocza DAPIX Grupa Robocza COPEN Grupa Robocza ds. SIS i Sirene Organy zarządzające agencji UE	A i C) ISF B) budżet eu-LISA – przez dodatkowe wsparcie z budżetu UE

Dodatkowe uwagi: Zob. rozdział 1.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
3	W pełni przestrzegać wymogów z zakresu ochrony i bezpieczeństwa danych	A) Analizować, opracowywać i propagować rozwiązania polegające na uwzględnianiu ochrony prywatności już w fazie projektowania B) Wymieniać doświadczenia, praktyki i spostrzeżenia z myślą o wdrażaniu unijnego pakietu dotyczącego ochrony danych <i>Nie są wymagane zmiany prawa</i>	państwa członkowskie Komisja eu-LISA	Europol, Eurojust, Frontex,	2017/2018 – w zakresie prawnym i 2018–2020 – w zakresie procesów operacyjnych i świadomości.	Grupa Robocza DAPIX	ISF

Dodatkowe uwagi: Warunkiem wstępnym zarządzania informacjami i ich wymiany do celów egzekwowania prawa jest pełne przestrzeganie praw podstawowych i przepisów o ochronie danych. W dniu 28 kwietnia 2016 r. unijny pakiet dotyczący ochrony danych został oficjalnie przyjęty przez współprawodawców. Teraz należy go wdrożyć i potrzebne będą środki do zapewnienia wyraźnych zasad, wskazówek i realnych rozwiązań do codziennej pracy praktyków. Międzynarodowa wymiana wiedzy fachowej, doświadczeń i praktyk będzie ułatwiać praktykom praktyczne i bardziej jednolite wsparcie przy wdrażaniu i stosowaniu wymogów z zakresu ochrony danych.

Temat 2 Ukierunkowane na praktyków podejście do zarządzania informacjami i wymiany informacji

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
4	Dążyć do uzyskania rozwiązań z zakresu interoperacyjności, tworząc rozwiązania informacyjne (lecz niekoniecznie poprzestając na nich) polegające na punktach kompleksowej obsługi na szczeblu krajowym i europejskim przez przeznaczone dla państw członkowskich pojedyncze interfejsy służące zasilaniu i przeszukiwaniu krajowych, europejskich (np. SIS), i międzynarodowych (np. Interpol) systemów	A) Zapewnić standardowe wymogi operacyjne, takie jak wymogi minimalne dla przydatnego dla użytkownika interfejsu zapewniającego standardowe struktury pozyskiwania danych oraz sprawności i korzyści operacyjnych – co umożliwi uzyskanie dostosowanych rozwiązań krajowych i poszanowanie praw dostępu; oraz zapewnić najlepsze praktyki w zakresie rozwiązań (przykład rozwiązań z zakresu dostępu do systemów Interpolu i systemów krajowych: stosowane przez Interpol metody FIND i MIND²⁰ oraz przykład przeszukiwania stosowanego przez Europol systemu EIS, indeksu plików analitycznych oraz systemów krajowych; wspierany przez Europol projekt pilotażowy QUEST). B) Zbadać najlepsze praktyki w państwach członkowskich umożliwiające praktykom mobilny dostęp w czasie rzeczywistym do niektórych źródeł informacji, generowanie sygnałów i wpisów z konkretnych lokalizacji oraz możliwości przekazywania informacji w czasie rzeczywistym, w tym przekazów audio i wideo na żywo <i>Działania podrzędne A i B nie wymagają zmian prawa. Jednak jeżeli w aktach prawnych ujęte zostaną wymogi techniczne, mogą być potrzebne poprawki.</i>	eu-LISA państwa członkowskie, Komisja	Europol Eurojust Frontex Interpol	A i B) 2018 po analizie luk działanie 1	Grupa Robocza DAPIX grupa ekspertów ds. systemów informacyjnych i interoperacyjności	ISF

²⁰ Stała baza danych sieci Interpolu (FIND) i ruchoma baza danych sieci Interpolu (MIND) mają na celu ułatwianie jednoczesnych przeszukiwań systemów Interpolu i systemów krajowych (w tym NSIS).

	informacyjnych						
--	----------------	--	--	--	--	--	--

Dodatkowe uwagi: Łatwe przekazywanie informacji i zasilanie baz danych oraz łatwy równoczesny dostęp do różnych systemów za pośrednictwem jednego interfejsu – punkt kompleksowej obsługi – jest niezbędne do zwiększania wymiany informacji i monitorowania wymienianych informacji. W związku z tym ważne jest dostrzeżenie potrzeby kompatybilności takiego interfejsu nie tylko z systemami międzynarodowymi i europejskimi, lecz także z systemami krajowymi, oraz możliwości dostosowywania go do tych systemów. Ponadto należy wziąć pod uwagę dotychczasowe inicjatywy w tym względzie, takie jak opracowanie uniwersalnego formatu przekazywania wiadomości (*Universal Messaging Format* – UMF).

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
5	Dalej rozwijać uniwersalny format przekazywania wiadomości	Dalej rozwijać uniwersalny format przekazywania wiadomości Przy dalszym rozwijaniu formatu należy brać pod uwagę struktury kont i rozwój obecnych systemów informacyjnych takich jak SIS; z kolei przy dalszym rozwijaniu tych systemów należy brać pod uwagę UMF. <i>W zależności od krajowych i europejskich ram prawnych wdrażanie UMF będzie wymagało zmian w prawie.</i>	państwa członkowskie Europol Frontex eu-LISA Interpol	Komisja	W toku (projekty pilotażowe rozpoczęły się w 2016 r. w Europolu i w kilku państwach członkowskich – projekt UMF3)	Grupa Robocza DAPIX	Projekt UMF3 finansowany jest przez ISF

Dodatkowe uwagi: Program koordynowania interoperacyjności UMF ma na celu utworzenie wspólnie uznawanej standardowej specyfikacji do wymiany informacji między krajowymi organami ścigania. Zapewni on interoperacyjność semantyczną, tym samym ulepszając jakość danych. Program ma być realizowany w trzech fazach, z których dwie już wykazały rezultaty: 1) definicja kompleksowego europejskiego modelu informacji policyjnej (EU-PIM), który zintegruje bieżące modele informacji policyjnej w europejskich państwach członkowskich i w instytucjach centralnych. 2) na podstawie EU-PIM – opracowanie specyfikacji technicznych do uniwersalnego formatu przekazywania wiadomości. Dostępna jest wspólna norma techniczna do wdrożenia do systemów informatycznych. W roku 2016 rozpoczęła się trzecia faza (UMF3); ma ona na celu przedstawienie koncepcji i propozycji organu zarządzającego i procesu zarządzania przy utrzymywaniu i rozwijaniu nowej normy. Należy zachęcać wszystkie zainteresowane strony, w tym organy ścigania, do konsekwentnego stosowania normy UMF, by ułatwiać komunikację transgraniczną.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
6	Zwiększyć zaufanie wśród praktyków na różnych szczeblach i pomiędzy różnymi szczeblami oraz ich wiedzę fachową, m.in. znajomość działań praktycznych i środowiska	A) Opracowywać (dalej) krajowe programy szkolenia i podnoszenia świadomości, skierowane do organów ścigania i prokuratur, w tym wspólne szkolenia, we współpracy z odpowiednimi agencjami UE, uwzględniając wszystkie istniejące kanały i narzędzia, wraz z ich celami, warunkami i korzyściami B) Opracować transgraniczne programy wymiany z praktykami różnych kategorii i różnego szczebla. Uwaga powinna skupiać się głównie na zintegrowanym użytkowaniu tych narzędzi, przy jednoczesnym pełnym uwzględnieniu krajowych różnic prawnych, operacyjnych i technicznych. Ważnym punktem wyjścia jest podręcznik wymiany informacji przy egzekwowaniu prawa jako narzędzie dla personelu punktów kompleksowej obsługi²¹. Podręcznik ten został przyjęty w roku 2015 i jest regularnie aktualizowany²². Praktycy, w tym personel punktów kompleksowej obsługi, centrów współpracy policyjno-celnej i inne osoby, powinni brać udział w opracowywaniu i stosowaniu wspomnianych programów. <i>A i B: Nie są wymagane zmiany prawa</i>	państwa członkowskie (Cepol) Europejska Sieć Sądowa eu-LISA biura Sirene	Europol Eurojust Komisja Interpol	W toku	Grupa Robocza DAPIX Grupa Robocza ds. Egzekwowania Prawa Grupa Robocza ds. Współpracy Celnej	A i B) centralny budżet ISF i programy krajowe Cepol i eu-LISA jako agencje UE nie korzystają z unijnych programów finansowania. Pomoc z ich strony wymaga dostatecznych środków poprzez regularne linie budżetowe przeznaczone na działalność tych agencji.

Dodatkowe uwagi: Cepol obecnie zapewnia różne kursy szkoleniowe związane z tymi sprawami, które to kursy mogą stanowić podstawę dla szkoleń na rzecz współpracy europejskich organów ścigania; niektóre elementy znajdują się w komunikacie Komisji w sprawie utworzenia europejskiego systemu szkoleń w zakresie egzekwowania prawa (COM(2013) 172). Cepol oraz Europejska Sieć Sądowa zapewniają programy wymiany, które mogą stanowić podstawę do intensywniejszych lub rozszerzonych inicjatyw lub inspirować programy dwustronnej / trójstronnej wymiany.

²¹ Zob. działanie 7.

²² Dok. 6704/16.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
7	Współpraca transgraniczna w z akresie egzekwowania prawa	A) W pełni wprowadzić pojedyncze punkty kontaktowe do transgranicznej wymiany informacji między organami ścigania we wszystkich państwach członkowskich – łącznie z dostępnością non stop w odniesieniu do art. 7 protokołu dodatkowego do Konwencji Rady Europy o zapobieganiu terroryzmowi – na podstawie wytycznych z dok. 10492/14 i zawartych w dok. 6721/14 wytycznych dla pojedynczych punktów kontaktowych dotyczących międzynarodowej wymiany informacji między organami ścigania. B) Zgodnie ze strategią zarządzania informacjami opracować programy szkolenia i wymiany dla personelu pojedynczych punktów kontaktowych. C) Zbadać przydatność tłumaczenia wspomaganego maszynowo do zmniejszenia zarówno opóźnień w wymianie informacji, jak i obciążeń dla personelu pojedynczych punktów kontaktowych. D) Opracować / wprowadzić skuteczne zarządzanie sprawami i rozwiązania pracy bieżącej konkretnie dla pojedynczych punktów kontaktowych, z myślą o współpracy w zakresie wzajemnej pomocy prawnej. Rozwiązania takie wymagają elementów specjalnie dostosowanych, by spełniały wymogi krajowe, a inicjatywa ta powinna jedynie pełnić funkcje pomocnicze. Stąd korzystanie z (konkretnych) rozwiązań nie może być obowiązkowe. E) Rozważyć utworzenie wspólnej platformy (grupy roboczej w Radzie lub grupy wspierającej grupę roboczą DAPIX), by prowadzić regularne spotkania między szefami pojedynczych punktów kontaktowych w celu omawiania bieżących kwestii. <i>A – E: nie są wymagane zmiany prawa</i>	państwa członkowskie (Cepol)	Europol Eurojust Komisja Europejska (OLAF, DG TAXUD) eu-LISA	A) w toku – zakończenie w 2018 r. B) w toku – zakończenie w 2018 r. C) 2018 D) W toku E) 2018	Grupa Robocza DAPIX Grupa Robocza COPEN Grupa Robocza ds. Egzekwowania Prawa	A. nie dotyczy B. finansowanie centralne z ISF Cepol jako agencja UE nie korzysta z unijnych programów finansowania C. finansowanie ze środków UE D. finansowanie ze środków UE E. nie dotyczy

Dodatkowe uwagi: W konkluzjach z dnia 6 i 7 czerwca 2013 r. przyjętych po wydaniu przez Komisję komunikatu na temat europejskiego modelu wymiany informacji (dok. 9811/13) Rada potwierdziła potrzebę utworzenia pojedynczych punktów kontaktowych (SPOC) do transgranicznej wymiany informacji między organami ścigania we wszystkich państwach członkowskich. W tym celu opracowano wytyczne zawarte w dokumencie 10492/14. Tworzenie pojedynczych punktów kontaktowych w państwach członkowskich należy kontynuować zgodnie ze wspomnianymi wytycznymi, mając na uwadze różnice prawne, operacyjne, proceduralne i inne między państwami członkowskimi. Tym samym można zapewnić szybkość, większą spójność i nadzór przy wymianie informacji do celów wzajemnej pomocy prawnej. Działanie to będzie wspomagane przez wdrażanie skutecznych rozwiązań z zakresu zarządzania sprawami i pracą. Rozwiązania takie wymagają elementów specjalnie dostosowanych, by spełniały krajowe wymogi, a inicjatywa ta powinna jedynie pełnić funkcje pomocnicze. Stąd korzystanie z (konkretnych) rozwiązań nie może być obowiązkowe.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
8	Zwiększyć dwustronną wymianę informacji z zakresu egzekwowania prawa	Wzmacniać centra współpracy policyjno-celnej i ich współpracę ze SPOC, jednocześnie zapewniając scentralizowany (na szczeblu krajowym lub co najmniej państwowym) nadzór i monitorowanie transgranicznej wymiany informacji. <i>Nie są wymagane zmiany prawa</i>	państwa członkowskie	Europol Frontex	W toku	Grupa Robocza DAPIX Grupa Robocza ds. Współpracy Celnej	Projekt finansowany z ISF

Uwagi dodatkowe: w UE istnieje ponad 40 centrów współpracy policyjno-celnej. Są one ważnymi instrumentami dochodzeń w sprawach karnych i prewencji w regionach przygranicznych, a ich głównym celem jest szybka i łatwa transgraniczna wymiana informacji. Należy je wzmocnić, by były one dobrze wyposażone i zdolne sprostać zadaniom, biorąc pod uwagę szybko zmieniające się zagrożenia dla bezpieczeństwa.

Temat 3 Optymalne wykorzystywanie europejskich systemów informacyjnych

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
9	Poprawić potencjał informacyjny agencji UE	W miarę potrzeby zwiększyć dostarczanie danych do Europolu i Eurojustu, a także systematyczną wymianę spraw <i>Nie są wymagane zmiany prawa</i>	państwa członkowskie	Europol Eurojust	W toku	zarząd Europolu Kolegium Eurojustu	nie dotyczy

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
10	Europol ma w pełni korzystać z baz SIS, VIS i Eurodac	A) Europol ma w pełni korzystać ze swojego bieżącego zezwolenia, by uzyskiwać dostęp do baz SIS, VIS i Eurodac, także tworząc technicznie skuteczne połączenia; oraz B) Po podjęciu tych kroków określających ewentualne przeszkody dla zbiorowych trafień w tych systemach – ma prowadzić statystyki oraz zapewniać analizę użytkowania wyżej wspomnianych baz danych w podobny sposób, jak muszą to robić państwa członkowskie <i>A i B: Nie są wymagane zmiany prawa</i>	Europol Komisja eu-LISA	państwa członkowskie	W toku – zakończenie działania A w 2017 r.	zarząd Europolu zarząd eu-LISA grupa robocza ds. systemów informacyjnych i interoperacyjności	budżet Europolu

Dodatkowe uwagi: UE przyznała Europolowi dostęp do głównych centralnych baz danych, ale agencja ta nie wykorzystwała jeszcze w pełni tej możliwości. Europol ma prawo dostępu do danych wprowadzonych do SIS oraz bezpośredniego przeszukiwania tych danych dotyczących aresztowań, kontroli niejawnych i kontroli szczególnych oraz przedmiotów przeznaczonych do zajęcia. Dotychczas Europol wykonał jedynie stosunkowo ograniczoną liczbę przeszukiwań w SIS, ale stara się wdrożyć rozwiązanie polegające na przeszukiwaniu zbiorczym, by dokonywać krzyżowego sprawdzania w szczególności danych otrzymanych od stron trzecich w bazach danych Europolu w obecnych ramach prawnych; potrzebny jest dialog ze wspólnym organem nadzorczym na temat ochrony danych. Europol ma prawną możliwość dostępu do bazy VIS do celów konsultacji od września 2013 r. Od lipca 2015 r. podstawa prawna systemu Eurodac dopuszcza dostęp ze strony Europolu. Agencja powinna przyspieszyć prace nad utworzeniem połączenia z systemami VIS i Eurodac.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
11	Zwiększyć skuteczność wykorzystywania systemu informacyjnego Schengen (SIS)	A) Organy ścigania, straż graniczna i służby imigracyjne wprowadzają do wpisów identyfikatory (gdy są one dostępne) (należy brać pod uwagę kopie paszportu, zdjęcie cyfrowe, dane biometryczne, profile DNA) na podstawie istniejących przepisów prawa; umożliwiają przeszukanie baz odcisków palców i przekazywanie wizerunków w przypadku trafienia. Należy ocenić obciążenie pracą biur Sirene i innych praktyków przy prowadzeniu tego działania, także z uwzględnieniem rozwiązań umożliwiających łatwą interpretację informacji. B) Wprowadzić do SIS – w systemie centralnym oraz krajowym, z myślą o jego pełnym wykorzystywaniu – funkcję automatycznego systemu identyfikacji daktyloskopijnej (AFIS). C) Znaleźć rozwiązanie krótkoterminowe, by umożliwić wzajemną wymianę informacji między państwami należącymi do strefy Schengen, państwami nienależącymi do niej i państwami częściowo korzystającymi z instrumentów połączonych z dorobkiem Schengen, do czasu uzyskania stałego rozwiązania tej kwestii w kategoriach udostępniania baz danych UE. <i>A – C: nie są wymagane zmiany prawa</i>	państwa członkowskie Komisja eu-LISA	Europol Eurojust Frontex biura Sirene	A) stopniowy, bieżący proces, zależny od krajowej dostępności i możliwości B) 2017 (na szczeblu centralnym) / począwszy od 2018 (na szczeblu krajowym) C) 2017/2018	A) Grupa Robocza ds. SIS i Sirene B) zarząd eu-LISA Komitet SIS/VIS C) Grupa Robocza ds. SIS i Sirene Komitet SIS/VIS	A) nie dotyczy B) wprowadzenie do systemu centralnego – budżet UE; wprowadzenie na szczeblu krajowym – budżet krajowy (z ewentualnym finansowaniem z Funduszu Bezpieczeństwa Wewnętrznego po roku 2017) C) do ustalenia

Uwagi dodatkowe: skuteczniejsza identyfikacja osób w przypadku trafienia będzie możliwa przez wprowadzanie dodatkowych informacji wraz z wpisem, gdy są one dostępne. Mogą one obejmować różne wskaźniki takie jak dane biometryczne, znaczniki ostrzegawcze lub zdjęcia (cyfrowe). Wyszukiwane odcisków palców za pomocą AFIS (automatycznego systemu identyfikacji daktyloskopijnej), które ma zostać wprowadzone do SIS, także przyspieszy identyfikację i uczyni ją bardziej wiarygodną. Identyfikatory te, jeśli są dostępne, powinny być dodawane do wpisów. Brak identyfikatorów nie powinien jednak uniemożliwiać wprowadzania wpisów. Państwa członkowskie poprawiają procesy krajowe, by egzekwować dodawanie takich identyfikatorów do wpisów.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
12	Zwiększyć skuteczność wykorzystywania systemu informacyjnego Schengen (SIS)	Zmienić postawę prawną systemu informacyjnego Schengen, biorąc pod uwagę ocenę dokonaną przez Komisję (w tym nowe funkcje, rozszerzenie dostępu dla agencji UE przy pełnym uwzględnianiu zasady odnoszącej się do właściciela informacji oraz podstaw prawnych działania tych agencji, ułatwianie dostępu do informacji o trafieniach). Zmiana powinna obejmować zapewnienie długoterminowego rozwiązania umożliwiającego wzajemną wymianę informacji między państwami należącym do strefy Schengen, państwami spoza tej strefy i państwami częściowo wykorzystującymi instrumenty połączone z systemem Schengen Dalej zbadać i stwierdzić, czy zarządzenia powrotu ze strony państw członkowskich można i należy wpisywać do SIS. <i>Nie są wymagane zmiany prawa</i>	Komisja Rada Parlament Europejski	eu-LISA Europol Eurojust Frontex	W toku: Wniosek do końca 2016 r. Przyjęcie przez Współprawodawców w 2017 r.	Skład Grupy Roboczej ds. Schengen (SIS/Sirene)	finansowanie przez UE z myślą o wdrożeniu

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
13	Pełne wykorzystywanie możliwości sieci Prüm do wymiany odcisków palców, danych DNA i danych rejestracyjnych pojazdów	A) Podjąć unijne projekty pilotażowe i w razie potrzeby, dalsze kroki, by egzekwować przyłączenie państw członkowskich do sieci Prüm B) określić główne przeszkody dla: i: przyłączenia do sieci Prüm ii: pełnego korzystania z możliwości sieci Prüm iii: rozwiązania problemów C) Zbadać możliwość zostania przez Europol partnerem w sieci Prüm, by umożliwiać krzyżowe zestawianie danych DNA, odcisków palców i danych rejestracyjnych pojazdów z danymi w posiadaniu państw trzecich, z którymi Europol zawarł umowę operacyjną, przy pełnym uwzględnianiu zasady odnoszącej się do właściciela informacji. <i>A i B: nie są wymagane zmiany prawa; C: zmiany prawa są wymagane</i>	A) Komisja B) państwa członkowskie, Komisja C) Komisja	Europol Eurojust Frontex	A) W toku B) W toku C) 2018	Komisja Grupa Robocza DAPIX	A i B (i oraz ii) nie dotyczy B) (iii): finansowanie programów krajowych z ISF C) nie dotyczy

Dodatkowe uwagi: DNA, odciski palców i dane rejestracyjne pojazdów są głównymi identyfikatorami w dochodzeniach karnych i mogą stanowić dowody w postępowaniu karnym. Z racji stale rosnącego międzynarodowego wymiaru przestępczości zorganizowanej, terroryzmu i innych zagrożeń dla bezpieczeństwa, istotne jest, aby wszystkie państwa członkowskie jak najszybciej zostały w pełni przyłączone do automatycznej wymiany danych w ramach Prüm. Ponadto państwa członkowskie powinny priorytetowo traktować operacyjne połączenia z innymi państwami członkowskimi. Przeszkody dla wdrożenia należy usunąć jak najszybciej.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
14	Poprawić wymianę informacji z rejestrów skazanych, zwłaszcza odnoszących się do wyroków skazujących za terroryzm	A) Ułatwiać dostęp wszystkim odnośnym organów do ECRIS i zwiększyć użytkowanie tego systemu B) Oprócz tego rozważyć rozwiązania (inne niż system ECRIS) umożliwiające proaktywną wymianę danych o wyrokach skazujących, zwłaszcza odnoszących się do terroryzmu; oraz, w miarę potrzeby, ocenić prawną i praktyczną wykonalność rozwiązania polegającego na udostępnianiu niektórych danych o wyrokach skazujących właściwym organom. <i>A: Nie są wymagane zmiany prawa; B: Nie są wymagane zmiany prawa</i>	państwa członkowskie Eurojust Komisja	Europol Frontex OLAF eu-LISA	A) W toku B) 2019	Grupa Robocza COPEN	A) nie dotyczy B) do ustalenia

Dodatkowe uwagi: Państwa członkowskie powinny inwestować w ułatwianie dostępu do bazy ECRIS na szczeblu krajowym w celu zapewnienia powszechniejszego korzystania z tej bazy. W nagłych przypadkach państwa członkowskie powinny zwrócić się do Eurojustu o ułatwienie uzyskiwania informacji z rejestrów karnych. Jeżeli dostęp nie został jeszcze utworzony, państwa członkowskie powinny wymieniać informacje na podstawie decyzji ramowej 2009/315/WSiSW. Po przyjęciu wniosku ustawodawczego dotyczącego uzupełnienia ECRIS o system odnośników w celu umożliwienia organom krajowym ustalenia, które państwo członkowskie posiada rejestr karny zawierający dane obywatela kraju trzeciego, państwa członkowskie zachęca się do pełnego wykorzystywania tej możliwości.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
15	Zwiększyć zdolności członków Eurojustu w zakresie koordynacji i monitorowania	Umożliwić ustanawianie i przyłączanie członków krajowego systemu koordynacyjnego Eurojustu do należącego do Eurojustu zautomatyzowanego systemu zarządzania sprawami (CMS) <i>Nie są wymagane zmiany prawa</i>	państwa członkowskie Eurojust	Europol Frontex OLAF	w toku, z myślą o zakończeniu w 2017/2018	Kolegium Eurojustu	finansowanie ze środków UE

Dodatkowe uwagi: System zarządzania sprawami (CMS) jest przeznaczony do gromadzenia i przetwarzania danych dotyczących spraw, w przypadku których zwrócono się do Eurojustu o pomoc. W celu poprawy funkcjonalności i wydajności operacyjnej, w 2015 r. udostępniono dwie uaktualnione wersje CMS w celu wsparcia realizacji przyłączenia członków krajowego systemu koordynacyjnego Eurojustu z każdego państwa członkowskiego do CMS, zgodnie z art. 12 decyzji Rady ustanawiającej Eurojust. Utworzono bezpieczne połączenia sieciowe z kilkoma państwami członkowskimi, co zapewnia bezpieczną wymianę informacji między Eurojustem a państwami członkowskimi. Wartość dodana dobrze funkcjonujących krajowych systemów koordynacyjnych Eurojustu jest szczególnie widoczna w dziedzinie zwalczania terroryzmu.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
16	Usprawnić i przyspieszyć międzynarodową wymianę informacji poprzez automatyzację procedur ręcznych	Rozwinąć projekt dotyczący automatyzacji wymiany danych (ADEP) Projekt ten musi zapewnić komplementarność z istniejącymi rozwiązaniami z dziedziny zarządzania informacjami, zwłaszcza względem Europolu (EIS), a także dążyć do tego, by zapewnione rozwiązanie było tanie, prawnie pewne i przydatne dla użytkownika. <i>Zmiany prawa mogą być wymagane, zwłaszcza przy wdrażaniu</i>	państwa członkowskie	Europol	w toku, zgodnie z obecnym projektem w ramach strategii zarządzania informacjami	Grupa Robocza DAPIX	projekt finansowany z ISF

Dodatkowe uwagi: Szybka i skuteczna wymiana informacji jest niezbędna, aby zapewnić szybkie działania następcze w prowadzeniu dochodzeń, działań kontrolnych i innych działań. Dlatego ważne jest szybkie określenie miejsca, w którym znajdują się najważniejsze informacje, i zwrócenie się do odpowiedniej strony. Projekt dotyczący automatyzacji wymiany danych (ADEP) ma na celu zaspokojenie tej potrzeby i zapewnienie wkładu w realizację celów decyzji ramowej Rady 2006/960/WSiSW („szwedzkiej decyzji ramowej”). Rozwój techniczny ADEP uwzględnia treść załącznika A do decyzji 2009/316/WSiSW (ECRIS) dotyczącego kategorii przestępstw.

ROZDZIAŁ 3: USPRAWNIANIE ZBIERANIA, WERYFIKOWANIA I ŁĄCZENIA INFORMACJI W CELU WYKRYWANIA OSÓB ZAANGAŻOWANYCH W DZIAŁALNOŚĆ TERRORYSTYCZNĄ I ZWIĄZANĄ Z TERRORYZMEM ORAZ ICH PODRÓŻY

Temat 1 Usprawnianie istniejących instrumentów – liczba, jakość i terminowość

SIS

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
17	Wypracować wspólne rozumienie odnośnie do tego, kiedy dana osoba powinna zostać wpisana do SIS w związku z działalnością terrorystyczną i związaną z terroryzmem	Uzgodnić orientacyjne kryteria odnoszące się do wprowadzania do SIS wpisów dotyczących terroryzmu	państwa członkowskie, Grupa Robocza ds. Terroryzmu, Komitet SIS–VIS	państwa członkowskie (biuro Sirene) eu-LISA	2016, w toku	COSI	nie dotyczy

Dodatkowe uwagi: SIS już teraz jest cennym narzędziem, a wspólne kryteria pozwalające określić, czy dana osoba jest zaangażowana w działalność terrorystyczną lub związaną z terroryzmem, będą stanowić wartość dodaną. Wpłynie to pozytywnie na wprowadzanie wpisów do SIS oraz na działania użytkowników końcowych w związku z uzyskanym trafieniem. Różnice pomiędzy krajowymi procedurami dotyczącymi dodawania informacji o „działalności związanej z terroryzmem” – jako rodzaju przestępstwa – sprawiają, że trudno ustanowić jasną typologię tych osób. Definicja terroryzmu zawarta w zmienionej decyzji ramowej Rady 2002/475/WSiSW stanowi wytyczną dla dalszych wysiłków na rzecz doprowadzenia do jej bardziej zharmonizowanego stosowania. W celu zapewnienia jasnych wymagań co do działań, które należy podjąć, oraz w celu zapewnienia niezbędnej reakcji w związku z wpisami w SIS i przekazywanymi informacjami, ustanawia się orientacyjne kryteria dotyczące wymiany i przekazywania informacji o osobach, które są zainteresowane udaniem się na obszary objęte konfliktem, by brać udział w walkach lub by wspierać ugrupowania terrorystyczne. Działanie to jest powiązane z działaniem 20.

Grupa najbardziej dotkniętych państw członkowskich uzgodniła już wykaz kryteriów, które zostały ujęte w załączniku do konkluzji z Mediolanu z dnia 7 lipca 2014 r. (zob. załącznik).²³ Orientacyjne kryteria zostaną uzgodnione na podstawie tego wykazu oraz zaktualizowanych informacji i innych wskaźników, np. wspólnych wskaźników ryzyka na potrzeby przeprowadzania kontroli granicznej (opracowanych przez Frontex i Grupę Roboczą Dumas).

Kryteria te mogą być również uwzględniane w przypadku przekazywania informacji Europolowi, na przykład na potrzeby systemu informacyjnego Europolu i punktu kontaktowego „Travellers”. Działanie to jest ściśle powiązane z działaniem 24 dotyczącym (jakości) informacji przekazywanych wraz z wpisem przy użyciu formularza M.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
18	Zapewnić biurom Sirene i użytkownikom końcowym SIS informacje strukturalne dotyczące osób zaangażowanych w działalność terrorystyczną lub związaną z terroryzmem	Państwa członkowskie będą tworzyć wpisy, gdy spełnione zostaną kryteria (chyba że nie będzie to wskazane ze względów operacyjnych)	państwa członkowskie	biura Sirene	2016, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Wpisy dotyczące osób są tworzone są na podstawie orientacyjnych kryteriów opracowanych w ramach działania 1. Państwa członkowskie muszą stosować te kryteria w celu stwierdzenia, czy należy wprowadzić wpis. Chociaż kryteria ujęte w wykazie nie są prawnie wiążące ani ograniczające, spełnienie już jednego z nich powinno prowadzić do sporządzenia wpisu, chyba że państwo członkowskie stwierdzi, że należy zrobić wyjątek. Oczywiście wszelkie przekazywanie i wymiana informacji dotyczących osób, o których mowa, nadal podlega gwarancjom przewidzianym w prawie krajowym i europejskim. Państwa członkowskie zadbają o należytą rozagę w sytuacjach, gdy pomimo spełnienia kryteriów wpis nie zostaje sporządzony. W celu zwiększenia wzajemnego zrozumienia i usprawnienia ewentualnych dobrych praktyk państwa członkowskie będą sobie nawzajem przekazywać spostrzeżenia dotyczące interpretowania standardów prawnych lub krajowe rozwiązania operacyjne. Działanie to jest powiązane z działaniem 17.

²³ Oprócz konkluzji z Mediolanu zob. również rezolucję ONZ nr 2178, decyzję ramową Rady 2002/475/WSiSW, decyzję ramową Rady 2008/919/WSiSW oraz tabele kodów SIS (ST 028 – działalność związana z terroryzmem).

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
19	Zapewniać biuram Sirene i użytkownikom końcowym SIS elementy wyraźnie wskazujące, że dany wpis dotyczy osoby zaangażowanej w działalność terrorystyczną lub związaną z terroryzmem	Wykorzystywać w stosownych przypadkach znacznik „działalność związana z terroryzmem”	państwa członkowskie	Komitet SIS–VIS, biura Sirene eu-LISA	2016, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Znacznik „działalność związana z terroryzmem” jest dodawany do wpisu sporządzanego dla osób, do których znacznik ten ma zastosowanie. Ustawienie domyślne będzie takie, że jeśli na mocy art. 36 decyzji w sprawie SIS II sporządzany będzie wpis na temat kontroli niejawnej lub kontroli szczególnej wobec osoby zaangażowanej w działalność terrorystyczną lub związaną z terroryzmem, znacznik „działalność związana z terroryzmem” będzie do wpisu dodawany zawsze, gdy wymagane będzie podjęcie natychmiastowego działania. Przy domyślnym zastosowaniu znacznika można będzie w praktyce zapewnić jasność i spójność. Niezależnie od korzyści, jakie przyniesie wprowadzanie wpisu dotyczącego osoby w oparciu o ustalone kryteria, stosowanie znacznika sprawi, że biuro Sirene i użytkownicy końcowi będą dysponować jeszcze dokładniejszymi informacjami i będą mieć większą pewność co do tego, jakie rezultaty mają przynieść działania podejmowane na podstawie danego wpisu. Państwa członkowskie zadbają o należytą rozagę (pod względem operacyjnym) w sytuacjach, gdy znacznik ten nie jest dodawany do wpisu. Oczywiście wszelkie przekazywanie i wymiana informacji dotyczących osób, o których mowa, nadal podlega gwarancjom przewidzianym w prawie krajowym i europejskim.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
20	Zapewnić wystarczającą jakość danych w SIS, tak żeby można było podjąć uzasadnione działania następcze	Państwa członkowskie powinny respektować minimalne standardy jakości danych wymagane dla SIS	państwa członkowskie, SIS/Sirene, Komisja Europejska, Komitet SIS–VIS	eu-LISA biura Sirene	2017, w toku	COSI, eu-LISA	nie dotyczy

Dodatkowe uwagi: Organy państw członkowskich muszą się orientować, jaka jest ważność/wiarygodność przekazywanych informacji, tak aby mogły podjąć skuteczne działania po uzyskaniu trafienia. Brak wspólnych standardów dla wszystkich państw członkowskich ogranicza efekty przekazywania informacji i działań następczych. Dotyczy to informacji wprowadzanych do systemu informacyjnego Schengen (SIS) oraz systemu informacyjnego Europolu (EIS), jak również informacji przekazywanych punktom kontaktowym „Travellers” i „Hydra” w Europolu. Państwa członkowskie same zobowiązują się do przestrzegania wspólnie uzgodnionych wymogów operacyjnych i technicznych dotyczących jakości danych. Prowadzone będą regularne dyskusje, w trakcie których szczegółowo omawiane będą na przykład znaczenie i dokładny cel przekazywanych i otrzymywanych danych oraz przekazywania danych we wspólnie ustalonym języku; dyskusje te umożliwią również ustalenie priorytetów, jeśli chodzi o działania do podjęcia. Eu-LISA bada i wdraża w SIS rozwiązania techniczne służące wspieraniu spójności z myślą o regularnym przekazywaniu państwom członkowskim informacji zwrotnych na temat jakości danych. Komisja będzie otrzymywać syntetyczne sprawozdania strategiczne wysokiego szczebla. Konieczne będzie opracowanie specjalnego formularza Sirene służącego do wymiany dodatkowych informacji i zawierającego również pola z opcjami wielokrotnego wyboru (*multiple choice*). Do tego czasu państwa członkowskie powinny przedstawiać w formularzu M przynajmniej w minimalnym zakresie informacje na temat przyczyn i okoliczności, w związku z którymi dane informacje są przekazywane. Wysyłanie prawie pustego formularza nie odpowiada potrzebom operacyjnym. Będą one uzupełnieniem już istniejących pól z opcjami wielokrotnego wyboru oraz pól przeznaczonych na wpisanie tekstu; ich wypełnienie będzie potrzebne do finalizowania formularza M. Jeśli chodzi o systemy w obszarze kompetencji eu-LISA, działania te są objęte planem działania w sprawie zarządzania informacjami i wymiany informacji w obszarze egzekwowania prawa.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowani e	Wsparcie finansowe na wniosek Rady
21	Zapewnić biurom Sirene i użytkownikom końcowym SIS dodatkowe informacje pochodzące z rejestrów karnych	Wraz z wpisem wprowadzać dodatkowe informacje w oparciu o rejestry karne (krajowe bazy danych i ECRIS)	państwa członkowskie, Komitet SIS–VIS	Eurojust, biura Sirene, Komisja Europejska	2016, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Pochodzące z rejestrów karnych informacje na temat osoby, w odniesieniu do której w systemie SIS sporządza się odpowiedni wpis, są wprowadzane wraz z tym wpisem (jeśli są dostępne i adekwatne). Wykorzystanie – przy sporządzaniu wpisów do SIS, w szczególności również w przypadku „działalności związanej z terroryzmem” – informacji pochodzących z ECRIS może zapewnić biurom Sirene i użytkownikom końcowym cenne informacje uzupełniające.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
22	Wypracować wspólne rozumienie odnośnie do natychmiastowego zgłaszania uzyskania trafienia w SIS	Wspólnie określić, kiedy wymagane jest „natychmiastowe zgłoszenie” uzyskania trafienia i jakie należy podjąć działania	Grupa Robocza ds. Terroryzmu, Grupa Robocza ds. SIS i Sirene	biura Sirene Komisja, eu-LISA	2016, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Ze względu na charakter niektórych artykułów, takich jak art. 24 rozporządzenia w sprawie SIS II oraz art. 36 i 38 decyzji w sprawie SIS II, możliwe są różne interpretacje co do działań, jakie należy podjąć w wyniku uzyskania trafienia. Na przykład osoby, wobec których w danym państwie wydano zakaz podróżowania, być może nie zostaną zatrzymane z tytułu wpisu na mocy art. 36, nawet jeśli naruszają one taki zakaz podróżowania. Konfiskata dokumentów z tytułu wpisów dotyczących zajęcia (na mocy art. 38 decyzji w sprawie SIS II) nie zawsze jest automatyczna, lecz może zależeć od przepisów krajowych.

Ponadto procedury krajowe dotyczące dodawania wymogu natychmiastowego zgłoszenia w odpowiedzi na wpis są bardzo zróżnicowane. Czas ma podstawowe znaczenie; dlatego też organy muszą mieć jasność co do tego, dlaczego wymaga się natychmiastowego zgłoszenia, i jak mają wyglądać pożądane działania. W celu zapewnienia jednolitego stosowania i rozumienia zharmonizowane zostaną kryteria wykorzystywania nowej możliwości odnośnie do „natychmiastowego zgłoszenia”; wyjaśnione zostanie, w jakich przypadkach taka możliwość powinna być wykorzystywana. W związku z tym Komisja (lub eu-LISA) powinny przeprowadzić badanie dotyczące rezultatów osiąganych w przypadkach „natychmiastowego zgłaszania”. Formularz M powinien zawierać dodatkowe informacje, które będzie można natychmiast przekazać funkcjonariuszowi w terenie. Należy bezzwłocznie – na przykład telefonicznie – kontaktować się z właściwymi biurami Sirene. W celu przedstawienia wspólnie uzgodnionych pożądanych działań oraz sprzyjania przestrzeganiu ustaleń zmieniony zostanie podręcznik Sirene. Aby zapewnić odpowiednie działania, niezbędne jest przeszkolenie użytkowników końcowych. W stosownych przypadkach w stosunku do konkretnych artykułów przyjęte zostaną dalsze specyfikacje w celu usprawnienia praktyk odnośnie do tych artykułów.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
23	Sprawić, by we wpisach w SIS można było domagać się wstępnego i tymczasowego zatrzymania lub aresztowania, jeżeli istnieją ku temu wystarczające podstawy prawne w przepisach krajowych	Stworzyć nowy rodzaj działania	Komisja Europejska, Grupa Robocza ds. SIS i Sirene	państwa członkowskie	2017–2018, w toku (aktualizacja rozporządzenia i decyzji w sprawie SIS II)	COSI	nie dotyczy

Dodatkowe uwagi: Obecne możliwości działania w następstwie uzyskania trafienia w związku z wpisami na mocy artykułów rozporządzenia i decyzji w sprawie SIS II nie zaspokajają w pełni potrzeb operacyjnych. Na przykład charakter art. 36 decyzji w sprawie SIS II nie pozwala na podjęcie innego działania niż kontrola niejawna lub kontrola szczególna. Często wobec osoby będącej przedmiotem wpisu na mocy art. 36 decyzji w sprawie SIS II odnoszącego się do „działalności związanej z terroryzmem” nie został jeszcze wydany europejski nakaz aresztowania; po uzyskaniu trafienia mogą być jednak potrzebne inne działania niż tylko prowadzenie kontroli niejawnej lub kontroli szczególnej. Może to dotyczyć na przykład osób podlegających zakazowi podróży wydanemu w danym kraju. W związku z tym – z zachowaniem możliwości, jakie dają istniejące wpisy na mocy ram prawnych dotyczących SIS – nowy rodzaj działania powinien przewidywać możliwość wstępnego i tymczasowego zatrzymania lub aresztowania, jeżeli istnieją ku temu wystarczające podstawy prawne w przepisach krajowych.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
24	Zapewnić, by użytkownicy końcowi byli przygotowani do przeprowadzania kontroli niejawnej i (jeżeli istnieją ku temu podstawy prawne w przepisach krajowych) kontroli szczególnej	Wzmocnić skuteczną kontrolę niejawną i kontrolę szczególną, w tym poprzez szkolenie szkoleniowców	Komisja Europejska, państwa członkowskie, Ceuł, eu-LISA	biura Sirene	2016 (początek), w toku	COSI	nie dotyczy

Dodatkowe uwagi: Kwestiami istotnymi dla przeprowadzania kontroli niejawnej jest również zapewnienie właściwych informacji i odpowiedniego szkolenia, np. szkolenia szkoleniowców. Dotyczy to w szczególności sytuacji, gdy wpis opatrzony jest znacznikiem „działalność związana z terroryzmem”. Aby zapewnić lepsze wsparcie użytkowników końcowych, w formularzu M muszą być podawane konkretne informacje, takie jak znaczniki ostrzegawcze. Szkolenia dla użytkowników końcowych, także ze wsparciem ze strony Ceułu, oraz wsparciem technicznym, powinny ułatwić państwom członkowskim prowadzenie kontroli niejawnych i kontroli szczególnych.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
25	Przekazywać systematyczne informacje zwrotne na temat uzyskanych trafień lub wniosków o natychmiastowe działanie krajowym biur Sirene i wprowadzającym wpisy	Umożliwić systematyczne zgłaszanie uzyskanych trafień w systemie SIS do krajowego biura Sirene państwa członkowskiego, w którym to trafienie wystąpiło, oraz do biura Sirene państwa członkowskiego, które wprowadziło wpis	Komitet SIS–VIS, Komisja Europejska, Europol, państwa członkowskie	biura Sirene	2017, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Powiadamanie biur Sirene w czasie rzeczywistym o przeglądaniu wpisu związanego z terroryzmem nie zawsze ma miejsce; powiadamanie jest szczególnie potrzebne w przypadku wpisów, przy których wymaga się natychmiastowego zgłoszenia, oraz wpisów dotyczących „działalności związanej z terroryzmem”. Ma to również zastosowanie do wszelkich dodatkowych informacji otrzymanych w drodze wymiany informacji.

Przekazywanie informacji do innych państw członkowskich ma kluczowe znaczenie zwłaszcza po poważnych incydentach. Wystąpienie trafienia powinno zatem być niezwłocznie i automatycznie zgłaszane krajowym biur Sirene, które wprowadziły wpis.

Należy zbadać – jako rozwiązanie w przypadku tego działania – stosowane w państwach członkowskich dobre praktyki i wsparcie techniczne, które umożliwiają bezpośrednie udostępnianie informacji użytkownikowi końcowemu i biuru Sirene. Państwa członkowskie rozważą możliwość systematycznego przekazywania uzyskanych trafień – oraz informacji dodatkowych – Europolowi, na przykład do punktu kontaktowego „Travellers” lub punktu kontaktowego „Hydra”. Systematyczne przekazywanie Europolowi informacji związanych z uzyskanym trafieniem może wymagać zmian w prawie, a zatem potrzebna będzie analiza prawna.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
26	Zapewnić, by państwa członkowskie wymieniały między sobą informacje dotyczące ekstremistycznych agitatorów, którzy stanowią zagrożenie dla porządku publicznego	Optymalnie wykorzystywać SIS – przede wszystkim poprzez art. 24.3 oraz zgodnie z prawodawstwem krajowym – a w stosownych przypadkach sporządzać wpisy dotyczące obywateli państw trzecich, którzy nie przebywają na terytorium państw członkowskich	Komisja Europejska, współprawodawcy, państwa członkowskie podejmujące działania następcze	państwa członkowskie (tj. biura Sirene)	2017, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Państwa członkowskie postanawiają oflagowywać w SIS, na mocy odpowiedniego artykułu, wszystkich agitatorów ekstremistycznych – niezależnie od tego, czy dotyczy ich obowiązek wizowy czy nie – których uznaje się za osoby stanowiące zagrożenie dla porządku publicznego i którzy zamierzają wjechać do UE. Pozwala to państwom członkowskim na zwrócenie uwagi na agitatorów ekstremistycznych wskazanych przez inne państwa członkowskie i na podjęcie niezbędnych środków. Wpis w systemie SIS jest niezbędny do zapewnienia, by odpowiednia ocena była przeprowadzana za każdym razem, gdy agitator ekstremistyczny, którego państwo członkowskie uznaje za osobę stanowiącą zagrożenie dla porządku publicznego, zamierza wjechać do UE. Państwa członkowskie będą oflagowywać agitatorów ekstremistycznych na okres maksymalnie dwóch lat; wpisy zostaną następnie usunięte lub będą nadal utrzymywane, jeśli państwa członkowskie w oparciu o stałą ocenę uznają to za konieczne. Państwa członkowskie mogą rozważyć możliwość dostosowania prawodawstwa krajowego, tak aby uwzględnić ten cel.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
27	Zapewnić, by zarówno organy ścigania, jak i służby bezpieczeństwa mogły szybko wprowadzać wpisy do SIS	W stosownych przypadkach – zmienić krajowe praktyki, aby zapewnić zarówno organom ścigania, jak i służbom bezpieczeństwa możliwość bezpośredniego wprowadzania wpisów do SIS bez ingerencji organów sądowych	państwa członkowskie	biura Sirene państw członkowskich Grupa Robocza ds. Terroryzmu, SIS i Sirene	2016, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Państwa członkowskie zapewnią, by organy ścigania i służby bezpieczeństwa (wpisy na mocy art. 36) miały możliwość wprowadzania wpisów do SIS bez ingerencji organów sądowych. Rozpowszechniane będą informacje na temat dobrych praktyk ułatwiających angażowanie organów ścigania i służb bezpieczeństwa w używanie SIS (w tym poprzez oddelegowanie do biura Sirene) i ułatwiających usuwanie przeszkód prawnych/administracyjnych na szczeblu krajowym.

Baza zawierająca dane skradzionych lub utraconych dokumentów podróży

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
28	Umożliwić sprawdzanie odnośnie do dokumentów podróży, które nie zostały jeszcze zgłoszone jako skradzione, utracone lub unieważnione	Wprowadzać do bazy danych TDAWN w Interpolu dokumenty związane z wpisami dotyczącymi osób, w razie stwierdzenia takiej potrzeby	państwa członkowskie, państwa trzecie Interpol	eu-LISA	2016, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Państwa członkowskie mają pewne problemy z wprowadzaniem wpisów dotyczących dokumentów podróży do SIS lub bazy SLTD, jeśli takie dokumenty nie zostały jeszcze zgłoszone jako skradzione, utracone lub unieważnione na potrzeby podróży. Dlatego też powinna być dostępna baza danych TDAWN, w połączeniu z dyfuzjami w ramach Interpolu. Państwa członkowskie rozważą wprowadzanie do TDAWN dokumentów podróży związanych z osobami, które zaznaczyły w SIS, a także dyfuzje w ramach Interpolu, w razie stwierdzenia takiej potrzeby (pod warunkiem, że Interpol będzie w stanie uszanować ograniczony charakter dyfuzji przy wykorzystywaniu TDAWN). Dodatkowe wsparcie dla tych działań można będzie znaleźć w planie działania, który przedstawi Komisja i który ma dotyczyć zapobiegania przestępstwom przeciwko wiarygodności dokumentów i wykrywania takich przestępstw w odniesieniu do unijnych i pozaunijnych paszportów i dokumentów podróży.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
29	Pełne połączenie z bazą danych SLTD na zewnętrznych przejściach granicznych	Sprawić, by baza danych SLTD była dostępna w kraju na potrzeby automatycznych i systematycznych sprawdzeń	państwa członkowskie	Interpol	2017, w toku	COSI	

Dodatkowe uwagi: Państwa członkowskie powinny ustanowić elektroniczne połączenia z SLTD podczas kontroli – zwłaszcza na swoich zewnętrznych przejściach granicznych oraz w konsulatach wydających wizy; takie połączenia elektroniczne należy ustanowić dla wszystkich użytkowników końcowych. Dodatkowe wsparcie dla tych działań można będzie znaleźć w planie działania, który przedstawi Komisja i który ma dotyczyć zapobiegania przestępstwom przeciwko wiarygodności dokumentów i wykrywania takich przestępstw w odniesieniu do unijnych i pozaunijnych paszportów i dokumentów podróży.

Europol

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wniosek Rady
30	Zapewnić, by informacje o zagranicznych bojownikach terrorystycznych (FTF) były konsekwentnie i systematycznie przekazywane do europejskich systemów i platform, a także w miarę możliwości synchronizowane	Wdrożyć spójne trzystopniowe podejście do przekazywania informacji dotyczących FTF poprzez optymalne i spójne wykorzystywanie SIS, systemu informacyjnego Europolu (EIS) oraz właściwych punktów kontaktowych w Europolu	państwa członkowskie, Europol	biura Sirene eu-LISA	2017, w toku	COSI	nie dotyczy

Dodatkowe uwagi: Państwa członkowskie powinny konsekwentnie i systematycznie przekazywać informacje o zagranicznych bojownikach terrorystycznych do europejskich systemów i platform. Choć takie przekazywanie informacji podlega oczywiście nadal gwarancjom przewidzianym w prawie krajowym i europejskim, państwa członkowskie zadbają o należyłą rozagę w sytuacjach, gdy z przyczyn operacyjnych informacje nie są przekazywane do któregoś z tych systemów.

System EIS jest wykorzystywany jako baza danych do systematycznego gromadzenia informacji na temat zagranicznych bojowników terrorystycznych oraz innych dodatkowych informacji, których nie można uzyskać w SIS. W celu zapewnienia jednolitej jakości danych należy w miarę możliwości zsynchronizować informacje dotyczące terroryzmu zawarte w SIS i w EIS. Ponieważ nie jest to proces automatyczny, odpowiedzialność spoczywa na właścicielu danych. Państwa członkowskie powinny rozważyć przekazywanie poprzez EIS, zgodnie z „trzystopniowym podejściem”, odpowiednich trafień dotyczących zagranicznych bojowników, które uzyskano w SIS. W tym przypadku EIS przyczyniałby się (jako „pamięć o trafieniu”) do uzupełnienia luk wywiadowczych. Kilka państw członkowskich wdrożyło już to podejście w praktyce, np. zaznaczając w EIS, że w oparciu o trafienie uzyskane w SIS osoba A podlegająca kontroli niejawnej przekroczyła granicę między państwem członkowskim A a państwem B w dniu 10.4.2016 r., w pojeździe o numerze rejestracyjnym XXXXX, zarejestrowanym w państwie członkowskim C, i że w pojeździe tym znajdowała się również osoba B. Można by rozważyć wprowadzenie na poziomie europejskim technicznego (automatycznego) rozwiązania mającego wesprzeć ten proces.

EIS powinien być dostępny dla wszystkich właściwych organów państw członkowskich i UE zajmujących się zwalczaniem terroryzmu i powinien być przez nie w pełni wykorzystywany; bardzo przydatny byłby moduł ładowania danych (*data loader*). Istnieje jeszcze inny sposób wprowadzania dużej ilości danych: można ładować całe partie plików (*batch upload*). W stosownych przypadkach przy wprowadzaniu danych do EIS należy zamieścić odniesienie do wpisów w SIS II.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
31	Zapewnić lepsze wykorzystanie istniejących bezpiecznych kanałów wymiany informacji dotyczących terroryzmu i działalności związanej z terroryzmem	A) Lepiej wykorzystywać aplikację SIENA jako bezpieczny kanał wymiany – między organami ścigania – informacji dotyczących działalności terrorystycznej i związanej z terroryzmem B) Rozważyć wprowadzenie 24-godzinnego trybu pracy przez 7 dni w tygodniu w celu usprawnienia skuteczności kanałów	państwa członkowskie, Europol	Grupa Robocza ds. Terroryzmu	A: 2016 B: 2017 (dyskusje) i później (wdrożenie w kraju)	COSI	nie dotyczy

Dodatkowe uwagi: Europol kontynuuje wspieranie dalszego wprowadzania aplikacji SIENA na potrzeby organów ścigania w państwach członkowskich. Pod koniec 2015 r. Europol stworzył możliwość dwustronnego porozumiewania się poprzez aplikację SIENA pomiędzy komórkami antyterrorystycznymi. Obecnie Europol pracuje nad nowszą wersją aplikacji SIENA przystosowaną do informacji CONFIDENTIAL UE/EU CONFIDENTIAL – ta funkcja ma być dostępna jeszcze w 2016 r. W roku 2016 i 2017 w ramach aplikacji SIENA zostanie rozszerzona funkcja usługi sieciowej; będzie ona oferowała lepsze możliwości integracji z systemami krajowymi.

Eurojust

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady nie dotyczy
32	Dopilnować, by państwa członkowskie były informowane o wszystkich postępowaniach karnych i wyrokach skazujących dotyczących przestępstw terrorystycznych w UE	Przekazywać Eurojustowi informacje o wszystkich postępowaniach karnych i wyrokach skazujących dotyczących przestępstw terrorystycznych	państwa członkowskie, Eurojust	Grupa Robocza ds. Terroryzmu	2016, w toku	COSI	

Dodatkowe uwagi: Zgodnie z wymogami decyzji Rady 2005/671/WSiSW państwa członkowskie powinny przekazywać Eurojustowi informacje o wszystkich toczących się postępowaniach karnych i wydanych wyrokach skazujących w odniesieniu do przestępstw terrorystycznych oraz informacje na temat szczególnych okoliczności popełnienia tych przestępstw, związków z innymi odnośnymi sprawami, wniosków o wzajemną pomoc prawną i informacje na temat realizowania takich wniosków. Pozwala to państwom członkowskim korzystać ze zdolności Eurojustu w zakresie wykrywania powiązań między sprawami, a także ze stałych wysiłków Eurojustu na rzecz traktowania w sposób scentralizowany oraz analizowania wyzwań i najlepszych praktyk związanych z postępowaniami karnymi w sprawie przestępstw terrorystycznych, które to analizy i najlepsze praktyki są udostępniane państwom członkowskim, w szczególności poprzez regularnie ukazującą się publikację Eurojustu – *Terrorism Convictions Monitor* (Monitor dotyczący wyroków w sprawach o terroryzm), sprawozdania Eurojustu dotyczące zagranicznych bojowników terrorystycznych oraz poprzez wkład Eurojustu w roczne sprawozdanie dotyczące sytuacji i tendencji w dziedzinie terroryzmu w UE. W związku z tym wzywa się również państwa członkowskie, by wymieniały z Eurojustem informacje o sprawach dotyczących nielegalnego handlu bronią palną, przemytu narkotyków, przemytu nielegalnych imigrantów, cyberprzestępczości oraz innych poważnych przestępstw. Pozwoli to Eurojustowi na systematyczne kojarzenie krzyżowe istniejących informacji i ustalanie ewentualnych powiązań między terroryzmem a innymi poważnymi przestępstwami.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady nie dotyczy
33	Zapewnić przyłączenie Eurojustu do działającego w Europolu punktu kontaktowego „Hydra”	Przyłączyć Eurojust do działającego w Europolu punktu kontaktowego „Hydra”	Eurojust, Europol	państwa członkowskie	2016, 2017	COSI	

Dodatkowe uwagi: Eurojust został już skutecznie przyłączony do punktu kontaktowego „Travellers”. Państwa członkowskie wspomogą i ułatwią przystąpienie Eurojustu do punktu kontaktowego „Hydra”, tak by agencja ta mogła zapewniać terminowe i skuteczne wsparcie na rzecz dochodzeń i postępowań karnych prowadzonych w państwach członkowskich.

Temat 2 Organizuj, aby chronić: łączenie struktur i wiedzy fachowej

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
34	Zapewnić na szczeblu krajowym łączność między ekspertami ds. zwalczania terroryzmu a innymi służbami biorącymi udział w wykrywaniu podróży osób zaangażowanych w działalność terrorystyczną i związaną z terroryzmem	Na szczeblu krajowym należałoby stworzyć – jeśli nie istnieją – multidyscyplinarne platformy ds. wykrywania podróży osób zaangażowanych w działalność terrorystyczną i związaną z terroryzmem	państwa członkowskie		2016	COSI	nie dotyczy

Dodatkowe uwagi: W państwach członkowskich w wykrywaniu podróży osób zaangażowanych w działalność terrorystyczną i związaną z terroryzmem bierze udział wiele podmiotów. Należy zapewnić łączność między tymi podmiotami, na przykład za pośrednictwem multidyscyplinarnych platform służących wymianie fachowej wiedzy i dyskusjom na temat usprawnienia procedur krajowych.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
35	Zapewnić, by dobre praktyki krajowe dotyczące współpracy z państwami trzecimi w dziedzinie zwalczania terroryzmu były rozpowszechniane wśród państw członkowskich	Rozpowszechniać wśród państw członkowskich i partnerów z państw trzecich dobre praktyki dotyczące współpracy z państwami trzecimi w dziedzinie zwalczania terroryzmu	państwa członkowskie, Grupa Robocza ds. Terroryzmu	Komisja Europejska	2017	COSI	

Dodatkowe uwagi: Dokładne poznanie obecnie prowadzonej wymiany informacji o terrorystach między państwami członkowskimi UE a państwami trzecimi miałyby pozytywny wpływ na praktyki operacyjne. Mogłoby to obejmować: sposoby wprowadzania do SIS, na żądanie, informacji otrzymanych z państw trzecich, wykorzystanie dyfuzji w ramach Interpolu oraz rozpowszechnianie list zagrożeń, wspólne wskaźniki ryzyka, także z wykorzystaniem porozumień zawieranych przez Europol z partnerami z państw trzecich.

	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
36	Zapewnić wspólne rozumienie przez użytkowników końcowych wykrywania podróży osób zaangażowanych w działalność terrorystyczną i związaną z terroryzmem	Stworzyć wspólne i wielodyscyplinarne szkolenia dla ekspertów ds. zwalczania terroryzmu, ekspertów ds. granic i ekspertów ds. egzekwowania prawa we współpracy z istniejącymi grupami ekspertów, takimi jak SIS/Sirene, które to szkolenia dotyczyłyby wykrywania podróży osób zaangażowanych w działalność terrorystyczną i związaną z terroryzmem	państwa członkowskie, Ceuol, Frontex	SIS/Sirene, Grupa Robocza ds. Terroryzmu, Komitet SIS–VIS	2017	COSI	

Dodatkowe uwagi: Wspólne rozumienie przez ekspertów ds. zwalczania terroryzmu, ekspertów ds. granic i ekspertów ds. egzekwowania prawa różnych ról i praktyk jest niezbędnym warunkiem zapewnienia poprawy wymiany informacji, zwłaszcza pod względem jakości informacji. Należy zatem opracować wspólne i wielodyscyplinarne szkolenia.

Temat 3 Krajowe zdolności w zakresie wykrywania zapewniane przez jednostki do spraw informacji o pasażerach (PIU)

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
37	Zapewnić jednolite wdrażanie dyrektywy w sprawie danych PNR w poszczególnych państwach członkowskich	Zainicjowanie nieformalnej operacyjnej grupy roboczej ds. danych PNR	prezydencja, państwa członkowskie i Komisja	jednostki do spraw informacji o pasażerach w państwach członkowskich, Europol	2016	nie dotyczy	państwa członkowskie

Dodatkowe uwagi: W celu zapewnienia spójności wdrażania dyrektywy w sprawie danych PNR oraz kompatybilności krajowych jednostek do spraw informacji o pasażerach (PIU), zachęca się państwa członkowskie do udziału w nieformalnej operacyjnej grupie roboczej ds. danych PNR, zainicjowanej przez obecną prezydencję. W skład tej grupy muszą wchodzić szefowie krajowych jednostek do spraw informacji o pasażerach oraz eksperci. Grupa ta będzie omawiać, w ramach UE i wraz z Europolem i państwami trzecimi, kwestie rozwoju (przyszłych) operacyjnych praktyk jednostek do spraw informacji o pasażerach. Wspólne zasady wymiany informacji będą stanowić wsparcie zharmonizowanej i optymalnej współpracy operacyjnej między tymi jednostkami. Grupa ta mogłaby pośredniczyć przy wsparciu operacyjnym i technicznym oraz w udostępnianiu dobrych praktyk.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wnioski Rady
38	Przy tworzeniu nowych jednostek do spraw informacji o pasażerach wykorzystywać krajową praktykę państw członkowskich	Oferować pomoc techniczną przy tworzeniu jednostek do spraw informacji o pasażerach	państwa członkowskie		2016	nie dotyczy	państwa członkowskie

Dodatkowe informacje: W ramach nieformalnej operacyjnej grupy roboczej ds. danych PNR państwa członkowskie, które zapewniły już krajowe urządzenia techniczne na potrzeby jednostek do spraw informacji o pasażerach, będą, w stosownych przypadkach, udostępniać technologię, doświadczenia i wiedzę fachową w celu wsparcia państw członkowskich, które jeszcze tego nie uczyniły. Państwa członkowskie, które jeszcze nie ustanowiły jednostek do spraw informacji o pasażerach, proszone są o uruchomienie w tym celu swojej krajowej części Funduszu Bezpieczeństwa Wewnętrznego (ISF).

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
39	Porozumienie dotyczące sposobu, w jaki będzie prowadzona wymiana informacji pomiędzy jednostkami do spraw informacji o pasażerach oraz, o ile to możliwe, z państwami trzecimi	Zapewnić interoperacyjność i wymieniać informacje na temat osób podejrzanych i nietypowych schematów podróży oraz przepisów ukierunkowanych na tę kwestię	państwa członkowskie, Komisja / Europol		2018	nie dotyczy	nie dotyczy

Dodatkowe uwagi: Jednostki do spraw informacji o pasażerach działające w państwach członkowskich uzgodnią sposób wymiany informacji na temat osób podejrzanych i nietypowych schematów podróży oraz przepisów ukierunkowanych na tę kwestię, pomiędzy tymi jednostkami oraz, o ile to możliwe, z państwami trzecimi. Interoperacyjność jednostek do spraw informacji o pasażerach oraz wymiana informacji między nimi mają zasadnicze znaczenie, by zapewnić skuteczne wykorzystywanie danych PNR. Przyszłe jednostki do spraw informacji o pasażerach muszą być interoperacyjne. Przy tworzeniu infrastruktury wymiany informacji i opracowywaniu praktyk w zakresie wymiany informacji na potrzeby przyszłych PIU należy wykorzystać doświadczenia płynące z projektów, takich jak wbudowywanie Sieci Jednostek Analityki Finansowej (FIU.NET) z myślą o zapewnieniu, by wspólna wizja była uwzględniana od samego początku. Zachęca się państwa członkowskie, by w maksymalnym zakresie uczestniczyły w projektach Komisji realizowanych w ramach ISF i dotyczących interoperacyjności oraz w innych wielostronnych i międzynarodowych inicjatywach odnoszących się do tej ważnej kwestii. Europol mógłby zapewnić wsparcie w dyskusjach prowadzonych na szczeflu UE na temat ukierunkowanych przepisów stosowanych na poziomie krajowym oraz w opracowywaniu takich ukierunkowanych przepisów o zasięgu ponadnarodowym.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Monitorowanie	Wsparcie finansowe na wniosek Rady
40	W pełni wykorzystywać bazy danych Europolu w celu wsparcia jednostek do spraw informacji o pasażerach	Określić wsparcie Europolu na rzecz praktyk, współpracy i działań jednostek do spraw informacji o pasażerach	państwa członkowskie, Europol	Komisja Europejska	2017	nie dotyczy	nie dotyczy

Dodatkowe uwagi: W myśl art. 10 dyrektywy w sprawie danych PNR Europol odgrywa rolę we wspieraniu krajowych jednostek do spraw informacji o pasażerach. Bazy danych Europolu mogą zapewnić tym jednostkom wartość dodaną, będąc źródłem dodatkowych danych wywiadowczych (do celów weryfikacji, kontroli krzyżowej i zagwarantowania, by podejmowano uzasadnione decyzje). Za ogólną zasadę należy uznać, że współpraca operacyjna i kojarzenie informacji o podróżach z innymi źródłami danych wywiadowczych (*layering*) przynoszą korzyści, jeśli chodzi o identyfikowanie nowych/dodatkowych powiązań/podejrzanych/wątków śledztwa. Europol mógłby ułatwić zapewnienie ponadnarodowej perspektywy, jeśli chodzi o schematy podróży oraz ukierunkowane przepisy.

ROZDZIAŁ 4: ZARZĄDZANIE GRANICAMI I MIGRACJA

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
41	Rejestrowanie na granicach zewnętrznych UE wjazdu i wyjazdu osób korzystających z prawa do swobodnego przemieszczania się	Zbadać, czy istnieje potrzeba i wartość dodana rejestrowania podróży osób korzystających z prawa do swobodnego przemieszczania się, w tym ocenić skutki, koszty i proporcjonalność różnych możliwych rozwiązań (w tym rozszerzenia zakresu systemu wjazdu/wyjazdu – EES)	Komisja, grupa ekspertów wysokiego szczebla	Komisja, państwa członkowskie, eu-LISA, EIOD, Frontex	koniec 2016	SCIFA / COSI / Grupa Robocza ds. Granic	ISF

Dodatkowe uwagi: Konieczne jest – zwłaszcza w odpowiedzi na wyzwania związane z bezpieczeństwem, które zostały jeszcze raz uwypuklone na skutek zamachów w Paryżu i Brukseli – wyposażenie UE w odznaczające się szybką skutecznością i bezpieczne narzędzia w celu usprawnienia kontroli naszych granic zewnętrznych. Konieczne jest przeprowadzenie oceny, czy istnieje wartość dodana rejestrowania wjazdu i wyjazdu osób korzystających z prawa do swobodnego przemieszczania się, w tym osób, którym przysługuje prawo swobodnego przepływu – z wykorzystaniem nowoczesnych technologii zapewniających sprawne przepływy. Taka ocena powinna również obejmować oszacowanie finansowej i technicznej wykonalności tego projektu. Należy również ocenić możliwość ustanowienia modułu w ramach systemu wjazdu/wyjazdu lub rozszerzenia tego systemu. Ocena ta nie powinna opóźniać bieżących negocjacji w sprawie systemu wjazdu/wyjazdu odnośnie do obywateli państw trzecich. Zob. działania 42 i 44.

24

²⁴ Jest to odpowiedź na decyzję podjętą przez Radę ds. WSiSW w dniu 25 lutego 2016 r.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
42	Rejestrowanie na granicach zewnętrznych UE wjazdu i wyjazdu osób, które otrzymały zgodę na krótki pobyt, oraz odmów wjazdu udzielonych obywatelom państw trzecich, także przyczyniające się do powrotów	Negocjacje w sprawie wniosków ustawodawczych dotyczących „inteligentnych granic”, unijnego systemu wjazdu/wyjazdu oraz zmiany kodeksu granicznego Schengen w ramach Grupy Roboczej ds. Granic	państwa członkowskie, Komisja i PE	eu-LISA	grudzień 2016	SCIFA / COSI / Grupa Robocza ds. Granic	ISF, budżet Komisji

Dodatkowe uwagi: Obok istniejących systemów ICT, Komisja zaproponowała 6 kwietnia 2016 r. ustanowienie kolejnego scentralizowanego systemu informatycznego – systemu wjazdu/wyjazdu (EES) – który ma poprawić zarządzanie granicą zewnętrzną w celu zmniejszenia nieuregulowanej imigracji poprzez zajęcie się zjawiskiem przekraczania dozwolonego okresu pobytu oraz ma przyczynić się do zwalczania terroryzmu i poważnej przestępczości, a tym samym do zapewnienia wysokiego poziomu bezpieczeństwa wewnętrznego. System ten powinien zostać wdrożony do 2020 r. (Wnioski ustawodawcze dotyczące „inteligentnych granic” [dok. 7675/16 i dok. 7676/16]). Zob. działania 41 i 44; w tym kontekście adekwatne jest również działanie 50.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
43	Usunięcie luki informacyjnej odnośnie do pozyskiwanych przed podróżą danych tych pasażerów, dla których nie są generowane dane API, PNR czy dane wizowe	Studium wykonalności i studium strategiczne unijnego systemu informacji i zezwoleń dotyczących podróży	Komisja	Komisja, państwa członkowskie, eu-LISA, EIOD, Frontex	październik 2016	SCIFA / Grupa Robocza ds. Granic i Grupa Robocza ds. Wiz	ISF, budżet Komisji

Dodatkowe uwagi: Podczas gdy organy ścigania mogą uzyskać z systemu VIS (wstępne) informacje dotyczące posiadaczy wiz, jeśli takie informacje są niezbędne do zwalczanie poważnej przestępczości i terroryzmu, porównywalne dane dotyczące osób zwolnionych z obowiązku wizowego w ogóle nie są dostępne. Trwające procesy liberalizacji reżimu wizowego mogą doprowadzić w niedalekiej przyszłości do znacznego wzrostu liczby podróżnych zwolnionych z obowiązku wizowego. W tym kontekście należy dokładniej zbadać możliwości w zakresie unijnego elektronicznego systemu zezwoleń na podróż odnoszącego się do obywateli państw trzecich zwolnionych z obowiązku wizowego. Dzięki takiemu systemowi wszyscy obywatele państw trzecich zamierzający wjechać na terytorium UE – nie tylko ci, którzy podlegają obowiązkowi wizowemu – mogliby zostać objęci pewną formą wstępnej kontroli przed podróżą i mogliby uzyskiwać wstępne zezwolenie przed przybyciem na przejście graniczne znajdujące się na granicy zewnętrznej. System ten umożliwiłby zbieranie i sprawdzanie informacji o obywatelach państw trzecich zamierzających podróżować do Europy na zasadzie indywidualnej, po to by udzielić im zezwolenia na podróż do granic zewnętrznych UE. Podobne systemy zostały już utworzone w Australii i USA. W oparciu o doświadczenia tych państw oraz z uwzględnieniem systemów obejmujących informacje zbierane przed podróżą (morski pojedynczy punkt kontaktowy, dane PNR i API), elektroniczny system zezwoleń na podróż można zdefiniować jako system:

- do zbierania wniosków o zezwolenie na podróż do ich terytorium składanych przez cudzoziemców bezpośrednio oraz drogą elektroniczną na potrzeby krótkoterminowych pobytów turystycznych lub służbowych;
- do określenia kwalifikowalności cudzoziemców do podróży do ich terytorium na potrzeby krótkoterminowych pobytów bez konieczności przechodzenia pełnej procedury ubiegania się o wizę;
- do określenia, czy taka podróż stanowi zagrożenie z punktu widzenia egzekwowania prawa bądź bezpieczeństwa;
- umożliwiający zapobieżenie podróży cudzoziemca do ich terytorium, jeżeli taka podróż stanowi zagrożenie z punktu widzenia egzekwowania prawa bądź bezpieczeństwa, przy jednoczesnym zachowaniu możliwości wydania odmowy zgody na wjazd na granicy, nawet w przypadku podróżnych, którzy uzyskali zezwolenie na podróż. Aby umożliwić formalne dyskusje na temat wartości dodanej takiego systemu, w studium wykonalności należy zbadać wszystkie opcje, mając na względzie konieczność stworzenia i proporcjonalność ETIAS.

(Komunikat „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”)

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
44	Usprawnienie weryfikacji danych w hotspotach	W celu skrócenia czasu i usprawnienia każdej weryfikacji danych, w standardowych procedurach operacyjnych w ramach procesów działań hotspotów i relokacji należy jasno opisać każdy krok. Należy zapewnić dostęp do odpowiednich baz danych, tj. SIS, VIS, Eurodac, baz danych Interpolu oraz baz danych Europolu, zwłaszcza w celu ułatwienia wymiany informacji o zastrzeżeniach w zakresie bezpieczeństwa w przypadkach relokacji, w tym wymiany odcisków palców przez relokacją. Jeśli chodzi o relokację, należy sporządzić kwestionariusz, aby ustalić, kiedy dossier dotyczące relokacji spełnia odpowiednie normy. W przypadku gdy dossier dotyczące relokacji zostaje odrzucone z powodu zastrzeżeń w związku z bezpieczeństwem, informację o tym należy przekazać wszystkim państwom członkowskim.	agencje UE i przyjmujące państwa członkowskie (EL i IT)	państwa członkowskie, Komisja	natychmiast	SCIFA / COSI / Grupa Robocza ds. Azylu	ISF, AMF

Dodatkowe uwagi: Prezydencja sformułowała zalecenia w sprawie weryfikacji danych w hotspotach i podczas procesu relokacji, które zostały omówione i poparte przez dużą liczbę państw członkowskich podczas posiedzenia COSI i SCIFA 18 kwietnia 2016 r. Proces działań w hotspotach rozpoczyna się w momencie przybycia/zatrzymania i trwa do momentu opuszczenia centrum rejestracji lub otwartego bądź zamkniętego ośrodka recepcyjnego. Zarówno proces działań w hotspotach, jak i proces relokacji muszą być zaprojektowane w taki sposób, by obejmowały weryfikację danych odbywającą się systematycznie, bez powodowania nowych utrudnień. Taka weryfikacja służy nie tylko wydaniu decyzji o azylu, relokacji lub powrocie, lecz także upewnieniu się, że dana osoba nie stanowi zagrożenia dla bezpieczeństwa wewnętrznego/unijnego. Należy zorganizować bezzwłocznie dostęp do odpowiednich baz danych, tj. SIS, VIS, Eurodac oraz baz danych Interpolu i Europolu, w celu przeprowadzania odpowiednich weryfikacji danych. Aby jeszcze bardziej przyspieszyć proces relokacji, Komisja sporządzi kwestionariusz, na podstawie którego państwa członkowskie mogłyby określić, co należy rozumieć pod pojęciem „dobrej jakości” dossier dotyczącego relokacji, w tym także pod pojęciem „wystarczających” informacji dotyczących aspektów bezpieczeństwa. Dzięki ustanowieniu bardziej przejrzystych norm, jeśli chodzi o to, jakie informacje powinny być zawarte w dossier dotyczącym relokacji, państwo członkowskie będzie miało mniej powodów, by żądać dodatkowej weryfikacji prowadzącej do przedłużania się procesu. W przypadku odrzucenia dossier państwo członkowskie relokacji powinno uzasadnić decyzję o odrzuceniu wniosku o relokację w oparciu o podstawy przewidziane w decyzji Rady 2015/1601 z dnia 22 września 2015 r. oraz decyzji Rady 2015/1523 z dnia 14 września 2015 r. Jeżeli odrzucenie wiąże się z zastrzeżeniami w zakresie bezpieczeństwa w sprawach dotyczących relokacji, taką informację, o ile pozwala na to ustawodawstwo krajowe, należy przekazać jak najszybciej państwom członkowskim będącym beneficjentami.

(Konkluzja Rady UE z grudnia 2015 r.)

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe
45	Usprawnić – poprzez działania prowadzone przez państwa członkowskie UE w hotspotach – ich współpracę operacyjną dotyczącą zwalczania przemytu migrantów	Wszystkie agencje muszą nadal udostępniać niezbędne zasoby, m.in. w zakresie tłumaczeń ustnych i pisemnych	Frontex, Europol, Eurojust i EASO	państwa członkowskie	natychmiast	SCIFA / COSI	nie dotyczy

Wszystkie agencje (Frontex, Europol, Eurojust i EASO) muszą nadal udostępniać niezbędne zasoby, m.in. w zakresie tłumaczeń ustnych i pisemnych, w celu usprawnienia – poprzez działania prowadzone przez państwa członkowskie UE w hotspotach – ich współpracy operacyjnej dotyczącej zwalczania przemytu migrantów. W miarę możliwości należałoby prowadzić również transport do miejsca rejestracji ze scentralizowanych punktów zejścia na ląd na wyspach lub na kontynencie, także z myślą o jak najszybszym przekazaniu migrantom informacji o relokacji, azylu i (dobrowolnym) powrocie oraz o zagrożeniach związanych z dalszymi nieuregulowanymi ruchami migracyjnymi. Koordynowanie w ten sposób napływu migrantów sprzyja większej kontroli nad procesem działań w hotspotach i nad procesem relokacji oraz zapobiega działalności przemytniczej.

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
46	Zwiększyć wykorzystanie danych API do celów zarządzania granicami	Zapewnić systematyczne kontrolowanie krzyżowe danych API z danymi zawartymi w SIS i w prowadzonej przez Interpol bazie danych SLTD	państwa członkowskie	Komisja, eu-LISA, Frontex i inne właściwe agencje	koniec 2017	COSI	ISF

Dodatkowe uwagi: Postęp technologiczny zasadniczo umożliwia dokonanie sprawdzenia w odpowiedniej bazie danych bez opóźniania procedury przekraczania granicy, ponieważ kontrole dokumentów i osób mogą być prowadzone równolegle. Wykorzystywanie informacji o pasażerach, które to informacje uzyskiwane są zgodnie z dyrektywą Rady 2004/82/WE, może również przyczynić się do przyspieszenia niezbędnych kontroli w trakcie procedury przekraczania granicy. W tym kontekście należy zapewnić systematyczne kontrolowanie krzyżowe danych API z danymi zawartymi w SIS i w prowadzonej przez Interpol bazie danych SLTD.

(Komunikat „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” oraz przeprowadzona przez Komisję ocena dyrektywy dotyczącej danych API)

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
47	Umocnienie z perspektywy informacji pozycji państw członkowskich UE w zakresie zarządzania granicami (oraz zwalczania terroryzmu i przestępczości zorganizowanej)	Sprawdzenie, czy potrzebna jest zmiana podstawy prawnej przetwarzania danych API	Komisja	państwa członkowskie, Frontex	2017	SCIFA / Grupa Robocza ds. Granic	nie dotyczy

Dodatkowe uwagi: Aby zapewnić powszechniejsze wdrożenie i nałożyć na państwa członkowskie obowiązek żądania danych API i wykorzystywania ich w odniesieniu do wszystkich lotów wychodzących i przychodzących, niezbędne jest dokonanie oceny obowiązującego ustawodawstwa dotyczącego danych API. Ma to szczególne znaczenie w kontekście wdrażania dyrektywy w sprawie danych PNR, ponieważ łączne użycie danych PNR i API zwiększa skuteczność wykorzystania danych PNR w walce z terroryzmem i poważną przestępczością.

(Komunikat „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” oraz przeprowadzona przez Komisję ocena dyrektywy dotyczącej danych API)

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
48	Poprawa funkcji wizowego systemu informacyjnego (VIS)	Zbadanie dalszych ulepszeń w VIS, a jednocześnie rozważenie ewentualnej konieczności zmiany podstawy prawnej	Komisja	eu-LISA, państwa członkowskie, Europol	przed końcem 2016	SCIFA / Grupa Robocza ds. Wiz	nie dotyczy

Dodatkowe uwagi: Dalej poprawiać jakość danych wprowadzanych do VIS, w tym udoskonalić jakość obrazu twarzy, aby umożliwić porównywanie danych biometrycznych. Ułatwić sprawdzanie danych w bazie SLTD podczas procedury ubiegania się danej osoby o wizę oraz zapewnić interoperacyjność z systemem SIS, aby móc wyszukiwać odciski palców osób ubiegających się o wizę – w ramach przyszłego automatycznego systemu identyfikacji daktyloskopijnej, który ma zostać opracowany na potrzeby SIS – np. po to by umożliwić wyszukiwanie na podstawie dokumentu podróży, jak zaproponowano w europejskim systemie wjazdu/wyjazdu (EES).

(Komunikat „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”)

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
49	Przegląd rozporządzenia Eurodac	Negocjacje w sprawie wniosku ustawodawczego dotyczącego Eurodac	państwa członkowskie, Komisja i PE	eu-LISA	koniec 2017	SCIFA / Grupa Robocza ds. Azylu	nie dotyczy

Odniesienia do innych działań ujętych w planie działania: działania dotyczące hostpotów oraz działania dotyczące zorganizowania łatwiejszego dostępu organów ścigania – w ramach ich obowiązków – do systemów informatycznych w dziedzinie migracji. (Wniosek ustawodawczy dotyczący Eurodac z 4 maja 2016 r.).

Nr	Cel	Działanie	Podmiot(y) prowadzący(-e)	Uczestnicy	Termin	Mechanizm monitorowania	Wsparcie finansowe na wniosek Rady
50	Wyeliminować istniejącą lukę informacyjną w odniesieniu do dokumentów (podróży) obywateli państw trzecich	Ocena zapotrzebowania na centralne repozytorium dokumentów pobytowych: czy takie nowe unijne narzędzie jest niezbędne, wykonalne i proporcjonalne w celu wyeliminowania istniejącej luki informacyjnej w odniesieniu do tych kategorii obywateli państw trzecich	Komisja	państwa członkowskie, eu-LISA, Frontex	pierwsza połowa 2017 r.	SCIFA / COSI / Grupa Robocza ds. Granic	ISF, eu-LISA

Dodatkowe uwagi: Repozytorium dokumentów pobytowych. Wydawanie dokumentów pobytowych, kart pobytu i wiz długoterminowych należy do kompetencji państw członkowskich. Zdecentralizowane zarządzanie tymi dokumentami powoduje jednak trudności w zakresie kontroli granicznych, w momencie gdy posiadacze tych dokumentów pobytowych, kart pobytu lub wiz długoterminowych przekraczają granice zewnętrzne strefy Schengen. Osoby posiadające dokumenty podróży wydane przez państwa trzecie muszą zostać skontrolowane na granicy w określony sposób, na podstawie dokumentów, których ważności ani autentyczności nie można zweryfikować w oparciu o wspólną bazę danych. Mimo że w drodze weryfikacji biometrycznej można ustalić, że podróżny jest prawowitym właścicielem danego dokumentu pobytowego, nie jest to możliwe w przypadku kart pobytu oraz wiz długoterminowych, gdyż nie istnieje dla nich wspólny format. Taka sytuacja stanowi zagrożenie dla bezpieczeństwa, które należy wyeliminować.

Oprócz względów bezpieczeństwa znaczenie ma też aspekt związany z ułatwieniem przekroczenia granicy: obywatele państw trzecich, którzy są zwolnieni ze spełnienia warunków uprawniających do krótkoterminowego pobytu, nie zostaną objęci zakresem EES (zgodnie z obecnym wnioskiem). Wprowadzenie EES da obywatelowi państwa trzeciego korzystającemu z krótkoterminowego pobytu możliwość skorzystania z rozwiązań w zakresie automatycznego przekraczania granicy, takich jak eGates, lecz takiej możliwości nie będą mieli obywatele państw trzecich korzystający z prawa do pobytu długoterminowego. Aby wyeliminować to niedociągnięcie, korzystne byłoby ustanowienie systemu na granicach umożliwiającego upewnienie się, czy obywatel państwa trzeciego posiada ważną kartę pobytu, ważny dokument pobytowy lub ważną wizę długoterminową, i, w razie konieczności, pozwalającego państwom członkowskim na przyznanie tej osobie dostępu do strefy Schengen na takich samych warunkach jak te przysługujące obywatelom UE (poprzez zastosowanie bramek eGate). Należy zbadać, czy możliwe jest stworzenie takiego systemu.

Poza kwestią zarządzania granicami możliwe jest trzecie uzasadnienie ustanowienia centralnego systemu informacyjnego dotyczącego obywateli państw trzecich będących posiadaczami dokumentów pobytowych. Beneficjenci europejskiego zezwolenia na pobyt muszą spełnić pewne warunki. Mogą one obejmować ograniczenia co do czasu, jaki osoby te mogą spędzać poza państwem członkowskim, które wydało to zezwolenie, bez groźby utraty prawo pobytu i prawa dostępu do określonych praw i usług socjalnych. Niektóre państwa członkowskie wyraziły chęć monitorowania również podróży osób będących posiadaczami dokumentów pobytowych, aby ocenić przestrzeganie przez nich tych ograniczeń.

W świetle powyższego należy rozważyć ustanowienie centralnego repozytorium dokumentów pobytowych, kart pobytu i wiz długoterminowych wydawanych przez państwa członkowskie, po to by przechowywać informacje o tych dokumentach (w tym informacje o dacie ważności i ewentualnym cofnięciu). Komisja powinna ocenić, czy takie nowe unijne narzędzie jest niezbędne, wykonalne i proporcjonalne w celu wyeliminowania istniejącej luki informacyjnej w odniesieniu do tych kategorii obywateli państw trzecich lub czy można podjąć inne kroki, by rozwiązać ten problem.

Odniesienie do innych działań ujętych w planie działania: działania 41 i 42.
