ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/817

z dnia 20 maja 2019 r.

w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726, (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

po konsultacji z Komitetem Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

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

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

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

(4) W swoich konkluzjach z dnia 15 grudnia 2016 r. Rada Europejska zaapelowała o kontynuowanie prac nad osiągnięciem interoperacyjności systemów informacyjnych i baz danych UE.

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

([1]) Dz.U. C 283 z 10.8.2018, s. 48.
([2]) Stanowisko Parlamentu Europejskiego z dnia 16 kwietnia 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 14 maja 2019 r.
([3]) Dz.U. C 101 z 16.3.2018, s. 116.

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

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

(8) W swoich konkluzjach z dnia 23 czerwca 2017 r. Rada Europejska podkreśliła potrzebę poprawy interoperacyjności baz danych i zachęciła Komisję do jak najszybszego sporządzenia projektu przepisów w oparciu o propozycje grupy ekspertów wysokiego szczebla ds. systemów informatycznych i interoperacyjności.

(9) Aby poprawić skuteczność i wydajność kontroli na granicach zewnętrznych, przyczynić się do zapobiegania nielegalnej imigracji i jej zwalczania oraz wnieść wkład w zapewnienie wysokiego poziomu bezpieczeństwa w ramach unijnej przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w tym utrzymanie bezpieczeństwa publicznego i polityki publicznej, oraz aby chronić bezpieczeństwo na terytoriach państw członkowskich, poprawić wdrażanie wspólnej polityki wizowej, ułatwić rozpatrywanie wniosków o udzielenie ochrony międzynarodowej, przyczynić się do zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie postępowań przygotowawczych, ułatwić identyfikację osób nieznanych w przypadku klęski żywiołowej, wypadku lub zamachu terrorystycznego, aby utrzymać zaufanie społeczeństwa do unijnego systemu migracji i azylu, unijnych środków bezpieczeństwa i zdolności Unii do zarządzania granicami zewnętrznymi, należy ustanowić interoperacyjność systemów informacyjnych UE — a mianowicie systemu wjazdu/wyjazdu (EES), wizowego systemu informacyjnego (VIS), europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS), systemu Eurodac, Systemu Informacyjnego Schengen (SIS) oraz europejskiego systemu przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN), aby te systemy informacyjne UE i zawarte w nich dane mogły się wzajemnie uzupełniać przy jednoczesnym poszanowaniu praw podstawowych obywateli, zwłaszcza prawa do ochrony danych osobowych. W tym celu jako elementy interoperacyjności należy ustanowić europejski portal wyszukiwania, wspólny system porównywania danych biometrycznych, wspólne repozytorium danych umożliwiających identyfikację i detektor wielokrotnych tożsamości.

(10) Interoperacyjność systemów informacyjnych UE powinna umożliwiać tym systemom wzajemne uzupełnianie się i ułatwić w ten sposób poprawną identyfikację osób, w tym osób nieznanych, które nie są w stanie potwierdzić swojej tożsamości, lub niezidentyfikowanych szczątków ludzkich, przyczynić się do zwalczania oszustw dotyczących tożsamości, poprawić i zharmonizować wymagania dotyczące jakości danych w odpowiednich unijnych systemach informacyjnych, ułatwić wdrożenie systemów informacyjnych UE przez państwa członkowskie od strony technicznej i operacyjnej, wzmocnić gwarancje bezpieczeństwa danych i ochrony danych regulujące odpowiednie systemy informacyjne UE, usprawnić dostęp do systemów EES, VIS, ETIAS i Eurodac do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych oraz wspierać realizację celów systemów EES, VIS, ETIAS, Eurodac, SIS i ECRIS-TCN.

(11) Elementy interoperacyjności powinny obejmować systemy EES, VIS, ETIAS, Eurodac, SIS i system ECRIS-TCN. Powinny one obejmować również dane Europolu, ale jedynie w zakresie umożliwiającym przeszukiwanie danych Europolu jednocześnie z tymi systemami informacyjnymi UE.

(12) Elementy interoperacyjności powinny przetwarzać dane osobowe osób, których dane osobowe są przetwarzane w poszczególnych systemach informacyjnych UE i przez Europol.

(13) Należy ustanowić europejski portal wyszukiwania, aby technicznie umożliwić szybki, sprawny, wydajny, systematyczny i kontrolowany dostęp organów państw członkowskich i agencji unijnych do systemów informacyjnych UE, danych Europolu i baz danych Międzynarodowej Organizacji Policji Kryminalnej (Interpolu) w zakresie, w jakim jest to konieczne do wykonywania przez nie ich funkcji w oparciu o ich własne prawa dostępu.

Europejski portal wyszukiwania powinien też wspierać osiąganie celów systemów EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN i danych Europolu. Poprzez umożliwienie równoległego przeszukiwania wszystkich istotnych systemów informacyjnych UE, danych Europolu i baz danych Interpolu, europejski portal wyszukiwania powinien działać jako pojedynczy punkt kontaktowy lub „pośrednik komunikatów" oraz służyć sprawnemu przeszukiwaniu różnych systemów centralnych i uzyskiwaniu koniecznych informacji, przy pełnym poszanowaniu zasad kontroli dostępu i wymogów dotyczących ochrony danych regulujących systemy podstawowe.

(14) Struktura europejskiego portalu wyszukiwania powinna gwarantować, że podczas przeszukiwania baz danych Interpolu dane użyte przez użytkownika europejskiego portalu wyszukiwania w celu dokonania zapytania nie będą przekazywane właścicielom danych Interpolu. Struktura europejskiego portalu wyszukiwania powinna też gwarantować, że bazy danych Interpolu będą przeszukiwane wyłącznie zgodnie z obowiązującym prawem unijnym i krajowym.

(15) Baza Interpolu zawierająca dane skradzionych lub utraconych dokumentów podróży (zwana dalej „bazą danych SLTD") umożliwia uprawnionym podmiotom odpowiedzialnym za zapobieganie przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywanie lub prowadzenie w ich sprawie postępowań przygotowawczych w państwach członkowskich, w tym organom imigracyjnym i organom kontroli granicznej, ustalenie, czy dany dokument podróży jest ważny. System ETIAS przeszukuje bazę danych SLTD i bazę danych dokumentów podróży powiązanych z notami Interpolu (zwaną dalej „bazą danych TDAWN") w kontekście oceny, czy istnieje ryzyko, że osoba ubiegająca się o zezwolenie na podróż migruje nielegalnie lub może stwarzać zagrożenie dla bezpieczeństwa. Scentralizowany europejski portal wyszukiwania powinien umożliwiać przeszukiwanie baz danych SLTD i TDAWN za pomocą danych dotyczących tożsamości danej osoby lub danych dokumentu podróży. W przypadku przekazywania danych osobowych z Unii do Interpolu za pośrednictwem europejskiego portalu wyszukiwania obowiązują przepisy w sprawie międzynarodowego przekazywania danych określone w rozdziale V rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]) lub przepisy krajowe dokonujące transpozycji rozdziału V dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([5]). Powinno to pozostawać bez uszczerbku dla przepisów szczegółowych określonych we wspólnym stanowisku Rady 2005/69/WSiSW ([6]) oraz w decyzji Rady 2007/533/WSiSW ([7]).

(16) Europejski portal wyszukiwania powinien zostać opracowany i skonfigurowany tak, aby umożliwiał jedynie dokonanie tego typu zapytań z wykorzystaniem danych związanych z osobami lub dokumentami podróży przechowywanych w systemach informacyjnych UE, danych Europolu lub bazie danych Interpolu.

(17) Aby umożliwić systematyczne wykorzystywanie właściwych systemów informacyjnych UE, należy korzystać z europejskiego portalu wyszukiwania w celu dokonywania zapytań we wspólnym repozytorium danych umożliwiających identyfikację oraz systemów EES, VIS, ETIAS, Eurodac i ECRIS-TCN. Należy jednak pozostawić krajowe połączenie z różnymi systemami informacyjnymi UE, aby zapewnić techniczną opcję awaryjną. Agencje unijne powinny też korzystać z europejskiego portalu wyszukiwania, aby przeszukiwać system centralny SIS zgodnie z posiadanymi prawami dostępu w celu pełnienia swoich funkcji. Europejski portal wyszukiwania powinien stanowić dodatkowy środek konsultacji systemu centralnego SIS, danych Europolu i baz danych Interpolu, uzupełniając istniejące interfejsy dedykowane.

(18) Dane biometryczne, takie jak odciski palców i wizerunki twarzy, są unikalne, a zatem znacznie bardziej niezawodne do celów identyfikacji osób, niż dane alfanumeryczne. Wspólny system porównywania danych biometrycznych powinien stanowić narzędzie techniczne służące wzmacnianiu i ułatwianiu prac odpowiednich systemów informacyjnych UE i pozostałych elementów interoperacyjności. Głównym celem wspólnego systemu porównywania danych biometrycznych powinno być ułatwienie identyfikacji osób, które mogą być zarejestrowane w kilku bazach danych, poprzez użycie pojedynczego komponentu technologicznego, zamiast wielu, w celu skojarzenia danych biometrycznych tych osób w różnych systemach. Wspólny system porównywania danych biometrycznych powinien przyczynić się do poprawy bezpieczeństwa oraz przynieść korzyści finansowe i związane z jego utrzymaniem i zarządzaniem nim. Wszystkie zautomatyzowane systemy identyfikacji daktyloskopijnej, w tym te obecnie wykorzystywane na potrzeby systemów Eurodac, VIS i SIS, korzystają z wzorców biometrycznych składających się z danych uzyskanych w wyniku ekstrakcji cech z rzeczywistych próbek biometrycznych. Wspólny system porównywania danych biometrycznych powinien przegrupować i gromadzić wszystkie te wzorce biometryczne – logicznie oddzielone w zależności od systemu informacyjnego, z którego pochodzą – w jednej lokalizacji, ułatwiając w ten sposób porównania międzysystemowe wykorzystujące wzorce biometryczne i umożliwiając korzyści skali w zakresie rozwoju i utrzymywania systemów centralnych UE.

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

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

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

([7]) Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 205 z 7.8.2007, s. 63).

(19) Wzorce biometryczne przechowywane we wspólnym systemie porównywania danych biometrycznych powinny składać się z danych uzyskanych w wyniku ekstrakcji cech z rzeczywistych próbek biometrycznych i powinno uzyskiwać się je w sposób uniemożliwiający odwrócenie procesu ekstrakcji. Wzorce biometryczne powinno się uzyskiwać z danych biometrycznych, ale nie powinno być możliwe uzyskanie tych samych danych biometrycznych z wzorców biometrycznych. Ponieważ dane dotyczące odcisków dłoni i profile DNA są przechowywane wyłącznie w SIS i nie można ich wykorzystać do kontroli krzyżowej z danymi zawartymi w innych systemach informacyjnych zgodnie z zasadami konieczności i proporcjonalności, we wspólnym systemie porównywania danych biometrycznych nie powinno się przechowywać profili DNA ani wzorów biometrycznych uzyskanych z danych dotyczących odcisków dłoni.

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

(21) Systemy EES, VIS, ETIAS, Eurodac i ECRIS-TCN wymagają poprawnej identyfikacji osób, których dane osobowe są w nich przechowywane. Wspólne repozytorium danych umożliwiających identyfikację powinno zatem ułatwiać poprawną identyfikację osób zarejestrowanych w tych systemach.

(22) Dane osobowe przechowywane w tych systemach informacyjnych UE mogą dotyczyć tych samych osób, zidentyfikowanych jednak za pomocą różnych lub niekompletnych tożsamości. Państwa członkowskie dysponują skutecznymi sposobami identyfikacji swoich obywateli lub zarejestrowanych stałych mieszkańców na swoim terytorium. Interoperacyjność systemów informacyjnych UE powinna przyczyniać się do poprawnej identyfikacji osób obecnych w tych systemach. We wspólnym repozytorium danych umożliwiających identyfikację powinno się przechowywać dane osobowe konieczne do dokładniejszej identyfikacji osób, których dane są przechowywane w tych systemach, w tym ich dane dotyczące tożsamości, dane dokumentu podróży i dane biometryczne, bez względu na system, do którego zostały pierwotnie pobrane. W repozytorium przechowywane są jedynie dane osobowe ściśle konieczne do przeprowadzenia dokładnej kontroli tożsamości. Zarejestrowane w nim dane osobowe powinny być przechowywane nie dłużej niż jest to absolutnie konieczne na potrzeby systemów podstawowych i automatycznie usuwane wraz z usunięciem tych danych z systemów podstawowych, zgodnie z logicznym rozdzieleniem danych.

(23) Nowa operacja przetwarzania danych polegająca na przechowywaniu takich danych we wspólnym repozytorium danych umożliwiających identyfikację zamiast w każdym z odrębnych systemów jest konieczna w celu umożliwienia zwiększenia dokładności identyfikacji poprzez automatyczne porównywanie i dopasowywanie danych. Fakt, że dane dotyczące tożsamości, dane dokumentu podróży i dane biometryczne są przechowywane w repozytorium nie powinien w żaden sposób utrudniać przetwarzania danych na potrzeby systemów EES, VIS, ETIAS, Eurodac czy ECRIS-TCN, ponieważ repozytorium będzie stanowić nowy wspólny komponent tych systemów podstawowych.

(24) W związku z tym konieczne jest stworzenie we wspólnym repozytorium danych umożliwiających identyfikację akt osobowych dla każdej osoby zarejestrowanej w systemach EES, VIS, ETIAS, Eurodac lub ECRIS-TCN do osiągnięcia celu poprawnej identyfikacji osób w granicach strefy Schengen oraz wspierania detektora wielokrotnych tożsamości, w podwójnym celu ułatwienia kontroli tożsamości osób podróżujących w dobrej wierze i zwalczania oszustw dotyczących tożsamości. Akta osobowe powinny gromadzić wszystkie informacje dotyczące tożsamości powiązane z daną osobą w jednej lokalizacji i umożliwiać dostęp do nich właściwie uprawnionym użytkownikom końcowym.

(25) Wspólne repozytorium danych umożliwiających identyfikację powinno zatem ułatwiać i usprawniać dostęp organów odpowiedzialnych za zapobieganie przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywanie lub prowadzenie w ich sprawie postępowań przygotowawczych do tych systemów informacyjnych UE, które nie powstały wyłącznie w celach zapobiegania poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych.

(26) Wspólne repozytorium danych umożliwiających identyfikację powinno stanowić wspólny zbiór danych dotyczących tożsamości, danych dokumentu podróży i danych biometrycznych osób zarejestrowanych w systemach EES, VIS, ETIAS, Eurodac i ECRIS-TCN. Powinno ono stanowić element struktury technicznej tych systemów i pełnić funkcję wspólnego komponentu łączącego je w celu przechowywania i przeszukiwania przetwarzanych przez nie danych dotyczących tożsamości, danych dokumentu podróży i danych biometrycznych.

(27) Wszystkie wpisy we wspólnym repozytorium danych umożliwiających identyfikację powinny być logicznie oddzielone poprzez automatyczne oznakowanie każdego wpisu ze wskazaniem systemu podstawowego, do którego on należy. Oznaczenia te powinny być wykorzystywane w celu ustalenia czy powinno się umożliwić dostęp do repozytorium.

(28) Jeżeli organ policji państwa członkowskiego nie jest w stanie zidentyfikować osoby z powodu braku dokumentu podróży lub innego wiarygodnego dokumentu potwierdzającego jej tożsamość, bądź jeżeli istnieją wątpliwości co do danych dotyczących tożsamości podawanych przez tę osobę lub autentyczności dokumentu podróży, lub

tożsamości jego posiadacza, bądź też osoba ta jest niezdolna do współpracy lub odmawia jej, organ policji powinien móc przeszukać wspólne repozytorium danych umożliwiających identyfikację, aby zidentyfikować tę osobę. W tym celu organy policji powinny pobrać odciski palców przy użyciu metod pobierania odcisków palców na żywo, o ile przeszukanie systemu nastąpiło w obecności tej osoby. Dokonywanie takich zapytań we wspólnym repozytorium danych umożliwiających identyfikację nie powinno być dozwolone w odniesieniu do osób małoletnich, które nie ukończyły 12. roku życia, chyba że jest to w interesie dziecka.

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

(30) Państwa członkowskie powinny przyjąć krajowe środki ustawodawcze wyznaczające właściwe organy odpowiedzialne za przeprowadzanie kontroli tożsamości za pomocą wspólnego repozytorium danych umożliwiających identyfikację oraz określające procedury, warunki i kryteria, jakim podlegają takie kontrole, zgodnie z zasadą proporcjonalności. W szczególności prawo krajowe powinno określać uprawnienia do pobierania danych biometrycznych podczas kontroli tożsamości danej osoby przez członków personelu tych organów.

(31) Niniejsze rozporządzenie powinno także wprowadzić nową możliwość usprawnienia dostępu do danych wykraczających poza dane dotyczące tożsamości lub dane dokumentu podróży zawarte w systemach EES, VIS, ETIAS lub Eurodac przez wyznaczone przez państwa członkowskie organy odpowiedzialne za zapobieganie przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywanie ich lub prowadzenie w ich sprawie postępowań przygotowawczych i Europol. Takie dane mogą być konieczne do zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych w konkretnych sprawach, jeśli istnieją uzasadnione podstawy, by uważać, że dokonanie sprawdzeń przyczyni się do zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych, w szczególności w przypadku podejrzenia, że osoba podejrzana, sprawca lub ofiara przestępstwa terrorystycznego lub innego poważnego przestępstwa jest osobą, której dane są przechowywane w systemie EES, VIS, ETIAS lub Eurodac.

(32) Pełen dostęp do danych zawartych w systemach EES, VIS, ETIAS lub Eurodac konieczny do zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych, wykraczający poza dostęp do danych dotyczących tożsamości lub danych dokumentu podróży przechowywanych we wspólnym repozytorium danych umożliwiających identyfikację, powinien nadal podlegać przepisom mających zastosowanie aktów prawnych. Wyznaczone organy odpowiedzialne za zapobieganie przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywanie lub prowadzenie w ich sprawie postępowań przygotowawczych i Europol nie wiedzą z góry, który system informacyjny UE zawiera dane osób będących przedmiotem zapytania. Prowadzi to do opóźnień i osłabienia skuteczności. Użytkownik końcowy uprawniony przez wyznaczony organ powinien móc zatem widzieć, w którym z tych systemów informacyjnych UE zarejestrowano dane odpowiadające wynikowi jego zapytania. Dany system zostałby zatem odpowiednio oznaczony w wyniku automatycznej weryfikacji obecności dopasowania w danym systemie (tzw. funkcja „dopasowanie/brak dopasowania").

(33) W tym kontekście odpowiedź ze wspólnego repozytorium danych umożliwiających identyfikację nie powinna być interpretowana lub wykorzystywana jako powód czy podstawa do wyciągania wniosków lub podejmowania działań wobec danej osoby, lecz powinna być wykorzystywana wyłącznie w celu złożenia wniosku o dostęp do podstawowych systemów informacyjnych UE, z zastrzeżeniem warunków i procedur określonych w odpowiednich aktach prawnych regulujących taki dostęp. Taki wniosek o dostęp powinien podlegać rozdziałowi VII niniejszego rozporządzenia oraz, w stosownych przypadkach, rozporządzeniu (UE) 2016/679, dyrektywie 2016/680 lub rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1725 ([8]).

(34) Zasadniczo, jeżeli znacznik dopasowania wskazuje na to, że dane są zapisane w systemach EES, ETIAS, VIS lub Eurodac, wyznaczone organy lub Europol powinny zwrócić się o pełny dostęp do co najmniej jednego z odpowiednich systemów informacyjnych UE. Jeżeli wyjątkowo nie złożono wniosku o taki pełny dostęp, na przykład ze względu na to, że wyznaczone organy lub Europol już uzyskały dane w inny sposób, lub uzyskanie tych danych nie jest już dozwolone na mocy prawa krajowego, należy odnotować uzasadnienie niewystąpienia o dostęp.

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

(35) Rejestry wyszukiwań we wspólnym repozytorium danych umożliwiających identyfikację powinny podawać cel wyszukiwania. Jeśli wyszukiwania dokonano w ramach dwuetapowego podejścia do sprawdzania danych, rejestry powinny zawierać odniesienie do akt krajowych związanych z danym postępowaniem przygotowawczym lub sprawą, wskazując w ten sposób, że danego zapytania dokonano w celach zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych.

(36) Dokonanie przez wyznaczone organy i Europol wyszukiwania we wspólnym repozytorium danych umożliwiających identyfikację w celu uzyskania odpowiedzi typu „dopasowanie/brak dopasowania" wskazującej, czy dane zostały zarejestrowane w systemach EES, VIS, ETIAS lub Eurodac, wymaga automatycznego przetwarzania danych osobowych. Dopasowanie nie powinno wiązać się z ujawnianiem danych osobowych osoby, której dotyczy wyszukiwanie, innych niż wskazanie, że pewne jej dane znajdują się w jednym z systemów. Uprawniony użytkownik nie ma prawa podejmować nieprzychylnej decyzji w stosunku do osoby, której dotyczy wyszukiwanie, jedynie na podstawie samego wystąpienia dopasowania. Dostęp użytkownika do dopasowania będzie stanowić zatem jedynie bardzo ograniczoną ingerencję w prawo do ochrony danych osobowych osoby, której dotyczy wyszukiwanie, umożliwiając zarazem wyznaczonym organom i Europolowi złożenie wniosku o dostęp do danych osobowych w bardziej efektywny sposób.

(37) Należy ustanowić detektor wielokrotnych tożsamości, aby wspierać funkcjonowanie wspólnego repozytorium danych umożliwiających identyfikację oraz osiągnięcie celów systemów EES, VIS, ETIAS, Eurodac, SIS i ECRIS-TCN. Aby skutecznie osiągnąć ich cele, wszystkie te systemy informacyjne UE wymagają dokładnej identyfikacji osób, których dane są w nich przechowywane.

(38) Aby lepiej osiągnąć cele systemów informacyjnych UE, organy korzystające z tych systemów powinny mieć możliwość przeprowadzania wystarczająco rzetelnej weryfikacji tożsamości osób, których dane są przechowywane w różnych systemach. Zestaw danych dotyczących tożsamości lub danych dokumentu podróży przechowywanych w danym systemie może być niepoprawny, niepełny lub fałszywy, a obecnie nie ma sposobu na wykrywanie takich niepoprawnych, niepełnych lub fałszywych danych dotyczących tożsamości lub danych dokumentu podróży poprzez porównywanie ich z danymi przechowywanymi w innym systemie. Aby zaradzić tej sytuacji, konieczne jest dysponowanie instrumentem technicznym na szczeblu Unii, który umożliwiałby dokładną identyfikację osób w tych celach.

(39) Detektor wielokrotnych tożsamości powinien stworzyć i przechowywać powiązania między danymi w różnych systemach informacyjnych UE, aby wykrywać wielokrotne tożsamości, w podwójnym celu ułatwienia kontroli tożsamości osób podróżujących w dobrej wierze i zwalczania oszustw dotyczących tożsamości. Detektor wielokrotnych tożsamości powinien zawierać jedynie powiązania między danymi dotyczącymi osób obecnych w więcej niż jednym systemie informacyjnym UE. Powiązane ze sobą dane powinny być ściśle ograniczone do danych potrzebnych do weryfikacji, czy dana osoba została w sposób uzasadniony lub nieuzasadniony zarejestrowana pod różnymi tożsamościami w różnych systemach, lub wyjaśnienia sytuacji, w których dwie osoby o zbliżonych danych w zakresie tożsamości mogą nie być tą samą osobą. Przetwarzanie danych za pośrednictwem europejskiego portalu wyszukiwania i wspólnego systemu porównywania danych biometrycznych w celu powiązania zestawów danych osobowych w różnych systemach należy sprowadzić do absolutnego minimum i przez to powinno ono ograniczać się do wykrywania wielokrotnych tożsamości, które ma zostać przeprowadzone w chwili dodawania nowych danych do jednego z systemów obejmującego dane przechowywane we wspólnym repozytorium danych umożliwiających identyfikację lub w chwili dodawania do SIS. Detektor wielokrotnych tożsamości powinien zawierać zabezpieczenia przed potencjalną dyskryminacją i nieprzychylnymi decyzjami wobec osób posługujących się różnymi tożsamościami w sposób zgodny z prawem.

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

(41) Europejski portal wyszukiwania i wspólny system porównywania danych biometrycznych powinny porównywać dane dotyczące osób we wspólnym repozytorium danych umożliwiających identyfikację i w SIS przy tworzeniu lub przekazywaniu nowych wpisów przez organ krajowy lub agencję unijną. Takie porównywanie powinno odbywać się automatycznie. Wspólne repozytorium danych umożliwiających identyfikację i SIS powinny korzystać ze wspólnego systemu porównywania danych biometrycznych, aby wykrywać możliwe powiązania na podstawie danych biometrycznych. Wspólne repozytorium danych umożliwiających identyfikację i SIS powinny korzystać z europejskiego portalu wyszukiwania, aby wykrywać możliwe powiązania na podstawie danych alfanumerycznych. Wspólne repozytorium danych umożliwiających identyfikację i SIS powinny móc identyfikować tożsame lub zbliżone dane dotyczące osoby przechowywane w różnych systemach. W takich przypadkach należy ustanowić powiązanie wskazujące, że jest to ta sama osoba. Wspólne repozytorium danych umożliwiających identyfikację i SIS powinny być tak skonfigurowane, aby wykrywały drobne błędy transliteracji lub zapisu w sposób, który nie przysparzałby danej osobie nieuzasadnionych trudności.

(42) Organ krajowy lub agencja unijna, które zarejestrowały dane w odpowiednim systemie informacyjnym UE, powinny potwierdzić te powiązania lub wprowadzić w nich zmiany. Ten organ krajowy lub ta agencja unijna powinny mieć dostęp do danych przechowywanych we wspólnym repozytorium danych umożliwiających identyfikację lub w SIS oraz w detektorze wielokrotnych tożsamości w celu ręcznej weryfikacji różniących się tożsamości.

(43) Organ odpowiedzialny za tworzenie lub aktualizację danych, które spowodowały dopasowanie prowadzące do ustanowienia powiązania z danymi przechowywanymi w innym systemie informacyjnym UE, zapewnia przeprowadzenie ręcznej weryfikacji różniących się tożsamości. Organ odpowiedzialny za ręczną weryfikację różniących się tożsamości powinien ocenić, czy istnieją różne tożsamości odnoszące się do tej samej osoby w sposób uzasadniony lub nieuzasadniony. Takiej oceny w miarę możliwości należy dokonać w obecności danej osoby, w stosownych przypadkach zwracając się o dodatkowe wyjaśnienia lub informacje. Oceny należy dokonać niezwłocznie, zgodnie z wymogami prawnymi dotyczącymi dokładności informacji na mocy prawa Unii i prawa krajowego. Zwłaszcza na granicach przemieszczanie się danej osoby będzie ograniczone w czasie dokonywania weryfikacji, która z tego względu nie powinna trwać przez czas nieokreślony. Istnienie powiązania żółtego w detektorze wielokrotnych tożsamości nie powinno stanowić podstawy do odmowy wjazdu, a decyzje dotyczące zezwolenia na wjazd lub odmowy wjazdu powinny być podejmowane wyłącznie na podstawie obowiązujących przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 ([9]).

(44) W odniesieniu do powiązań uzyskanych w związku z SIS dotyczących wpisów związanych z osobami poszukiwanymi w celu aresztowania i wydania lub ekstradycji, osobami zaginionymi lub narażonymi na zagrożenia, osobami, których obecność jest wymagana do celów postępowania sądowego lub osobami poddawanymi kontrolom niejawnym, rozpytaniom kontrolnym lub kontrolom szczególnym, organem odpowiedzialnym za ręczną weryfikację różniących się tożsamości powinno być biuro SIRENE państwa członkowskiego, które dokonało wpisu. Te kategorie wpisów w SIS mają charakter wrażliwy i nie muszą być przekazywane organom tworzącym lub aktualizującym dane powiązane z nimi w jednym z pozostałych systemów informacyjnych UE. Utworzenie powiązania do danych SIS nie powinno wpływać na działania podejmowane zgodnie z rozporządzeniami Parlamentu Europejskiego i Rady (UE) 2018/1860 ([10]), (UE) 2018/1861 ([11]) i (UE) 2018/1862 ([12]).

(45) Tworzenie takich powiązań wymaga przejrzystości wobec osób, których one dotyczą. Aby ułatwić wprowadzenie niezbędnych zabezpieczeń zgodnych z mającymi zastosowanie unijnymi przepisami o ochronie danych, osoby, które są objęte powiązaniem czerwonym lub powiązaniem białym po ręcznej weryfikacji różniących się tożsamości, powinny być informowane na piśmie, z zastrzeżeniem ograniczeń dotyczących ochrony bezpieczeństwa i porządku publicznego, zapobiegania przestępczości i zagwarantowania, że nie są zagrożone krajowe postępowania przygotowawcze. Osoby te powinny otrzymać pojedynczy numer identyfikacyjny umożliwiający im zidentyfikowanie organu, do którego powinny się zwrócić w celu skorzystania z przysługujących im praw.

(46) W przypadku utworzenia powiązania żółtego, organ odpowiedzialny za ręczną weryfikację różniących się tożsamości powinien mieć dostęp do detektora wielokrotnych tożsamości. W przypadku istnienia powiązania czerwonego do detektora wielokrotnych tożsamości powinny mieć dostęp organy państwa członkowskiego i agencje unijne mające dostęp do co najmniej jednego systemu informacyjnego UE włączonego do wspólnego repozytorium danych umożliwiających identyfikację lub do SIS. Powiązanie czerwone powinno wskazywać, że dana osoba posługuje się różnymi tożsamościami w sposób nieuzasadniony lub posługuje się tożsamością innej osoby.

(47) W przypadku gdy istnieje białe lub zielone powiązanie między danymi z dwóch systemów informacyjnych UE, dostęp do detektora wielokrotnych tożsamości powinny mieć organy państw członkowskich i agencje unijne, gdy dany organ lub agencja mają dostęp do obydwu systemów informacyjnych. Taki dostęp powinno się przyznawać wyłącznie w celu umożliwienia temu organowi lub agencji wykrycia potencjalnych przypadków, w których dane były powiązane nieprawidłowo lub przetwarzane w detektorze wielokrotnych tożsamości, wspólnym repozytorium danych umożliwiających identyfikację i SIS z naruszeniem niniejszego rozporządzenia, i podjęcia działań w celu naprawy sytuacji i uaktualnienia lub usunięcia połączenia.

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

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz.U. L 312 z 7.12.2018, s. 1).

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006 (Dz.U. L 312 z 7.12.2018, s. 14).

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz.U. L 312 z 7.12.2018, s. 56).

(48) Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) powinna ustanowić mechanizmy automatycznej kontroli jakości danych i wspólne wskaźniki jakości danych. eu-LISA powinna odpowiadać za stworzenie możliwości scentralizowanego monitorowania jakości danych oraz sporządzać regularne sprawozdania z analizy danych, aby poprawić kontrolę wdrażania systemów informacyjnych UE przez państwa członkowskie. Wspólne wskaźniki jakości danych powinny obejmować minimalne normy jakości w zakresie przechowywania danych w systemach informacyjnych UE lub elementach interoperacyjności. Celem takich norm kontroli jakości danych powinna być automatyczna identyfikacja wprowadzonych danych wyglądających na nieprawidłowe lub niespójne przez systemy informacyjne UE i elementy interoperacyjności, tak aby państwo członkowskie, z którego te dane pochodzą, mogło je sprawdzić i podjąć konieczne środki naprawcze.

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

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

(51) Można rozważyć wdrożenie standardu UMF w przypadku systemów VIS, SIS oraz innych dotychczasowych lub nowych modeli transgranicznej wymiany informacji i systemów informacyjnych w dziedzinie wymiaru sprawiedliwości i bezpieczeństwa opracowywanych przez państwa członkowskie.

(52) Należy ustanowić centralne repozytorium sprawozdawczo-statystyczne, aby generować międzysystemowe dane statystyczne i sprawozdania analityczne na potrzeby strategii politycznych, działań operacyjnych i zapewniania jakości danych zgodnie z mającymi zastosowanie aktami prawnymi. eu-LISA powinna ustanowić, wdrożyć i obsługiwać to repozytorium w swoich centrach technicznych. Powinno ono zawierać zanonimizowane dane statystyczne z systemów informacyjnych UE, wspólnego repozytorium danych umożliwiających identyfikację, detektora wielokrotnych tożsamości i wspólnego systemu porównywania danych biometrycznych. Dane zawarte w centralnym repozytorium sprawozdawczo-statystycznym nie powinny umożliwiać identyfikacji osób fizycznych eu-LISA powinna anonimizować dane w sposób zautomatyzowany i gromadzić takie zanonimizowane dane w tym repozytorium. Proces anonimizacji danych powinien przebiegać automatycznie, a pracownicy eu-LISA nie powinni otrzymywać bezpośredniego dostępu do żadnych danych osobowych przechowywanych w systemach informacyjnych UE lub w elementach interoperacyjności.

(53) Do przetwarzania danych osobowych przez krajowe organy na potrzeby interoperacyjności na mocy niniejszego rozporządzenia ma zastosowanie rozporządzenie (UE) 2016/679, z wyjątkiem sytuacji, gdy takiego przetwarzania dokonują wyznaczone organy lub centralne punkty dostępu państw członkowskich w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie postępowań przygotowawczych.

(54) Jeśli przetwarzania danych osobowych przez państwa członkowskie na potrzeby interoperacyjności na mocy niniejszego rozporządzenia dokonują właściwe organy do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych, zastosowanie ma dyrektywa (UE) nr 2016/680.

(55) Rozporządzenie (UE) 2016/679, rozporządzenie (UE) 2018/1725 lub w stosownych przypadkach dyrektywa (UE) 2016/680 mają zastosowanie do przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na mocy niniejszego rozporządzenia. Bez uszczerbku dla podstaw do przekazania danych na mocy rozdziału V rozporządzenia (UE) 2016/679 lub w stosownych przypadkach dyrektywy (UE) 2016/680 orzeczenia sądu oraz decyzje organu administracyjnego państwa trzeciego wymagające od administratora lub podmiotu przetwarzającego dane przekazania lub ujawnienia danych osobowych powinny być uznawane lub egzekwowalne wyłącznie w oparciu o międzynarodowe porozumienie obowiązujące między wnioskującym państwem trzecim a Unią lub państwem członkowskim.

(56) Szczegółowe przepisy dotyczące ochrony danych zawarte w rozporządzeniach Parlamentu Europejskiego i Rady (UE) 2017/2226 ([13]), (WE) nr 767/2008 ([14]), (UE) 2018/1240 ([15]) i (UE) 2018/1861 mają zastosowanie w stosunku do przetwarzania danych osobowych przez systemy podlegające tym rozporządzeniom.

(57) W stosunku do przetwarzania danych osobowych przez eu-LISA oraz pozostałe instytucje i organy Unii przy wykonywaniu ich obowiązków na mocy niniejszego rozporządzenia ma zastosowanie rozporządzenie (UE) 2018/1725, bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 ([16]), które ma zastosowanie do przetwarzania danych osobowych przez Europol.

(58) Organy nadzoru, o których mowa w rozporządzeniu (UE) 2016/679 lub dyrektywie (UE) 2016/680, powinny monitorować zgodność z prawem przetwarzania danych osobowych przez państwa członkowskie. Europejski Inspektor Ochrony Danych powinien monitorować działalność instytucji i organów Unii w odniesieniu do przetwarzania danych osobowych. Europejski Inspektor Ochrony Danych i organy nadzorcze powinny współpracować ze sobą w zakresie monitorowania przetwarzania danych osobowych przez elementy interoperacyjności. Aby Europejski Inspektor Ochrony Danych wypełniał zadania powierzone mu na mocy niniejszego rozporządzenia, potrzebuje on wystarczających zasobów, zarówno kadrowych, jak i finansowych.

(59) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([17]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 16 kwietnia 2018 r. ([18])

(60) Grupa Robocza Art. 29 przedstawiła opinię w dniu 11 kwietnia 2018 r.

(61) Zarówno państwa członkowskie, jak i eu-LISA powinny utrzymywać plany ochrony, aby ułatwić wdrożenie obowiązków w zakresie bezpieczeństwa oraz współpracować ze sobą w celu rozwiązywania problemów związanych z bezpieczeństwem. eu-LISA powinna też zapewniać stałe wprowadzanie najnowszych rozwiązań technologicznych, aby zapewnić integralność danych w ramach rozwoju i projektowania elementów interoperacyjności oraz zarządzania nimi. Obowiązki eu-LISA w tym względzie powinny obejmować przyjmowanie środków niezbędnych do zapobiegania dostępowi osób nieuprawnionych, takich jak pracownicy zewnętrznych dostawców usług, do danych osobowych przetwarzanych za pośrednictwem elementów interoperacyjności. Udzielając zamówień na świadczenie usług, państwa członkowskie i eu-LISA powinny uwzględnić wszystkie środki niezbędne do zapewnienia zgodności z przepisami ustawowymi lub wykonawczymi dotyczącymi ochrony danych osobowych oraz ochrony prywatności osób lub zabezpieczyć podstawowe interesy w zakresie bezpieczeństwa zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 ([19]) oraz stosownymi konwencjami międzynarodowymi. eu-LISA powinna stosować zasady ochrony prywatności w fazie projektowania i domyślnej ochrony prywatności w całym cyklu opracowywania elementów interoperacyjności.

(62) Wdrożenie elementów interoperacyjności, o których mowa w niniejszym rozporządzeniu, będzie mieć wpływ na sposób przeprowadzania kontroli na przejściach granicznych. Wpływ ten będzie wynikiem łącznego stosowania obowiązujących przepisów rozporządzenia (UE) nr 2016/399 oraz przepisów dotyczących interoperacyjności zawartych w niniejszym rozporządzeniu.

(63) W wyniku takiego łącznego stosowania przepisów to europejski portal wyszukiwania powinien stanowić główny punkt dostępu służący przeprowadzaniu obowiązkowego i systematycznego sprawdzania baz danych w stosunku do osób na przejściach granicznych, o którym mowa w rozporządzeniu (UE) 2016/399. Dodatkowo dane

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

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

([15]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226 (Dz.U. L 236 z 19.9.2018, s. 1).

([16]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).

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

([18]) Dz.U. C 233 z 4.7.2018, s. 12.

([19]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1).

dotyczące tożsamości lub dane dokumentu podróży, które doprowadziły do klasyfikacji powiązania w detektorze wielokrotnych tożsamości jako powiązania czerwonego, powinny być brane pod uwagę przez funkcjonariuszy straży granicznej przy ocenie, czy dana osoba spełnia warunki wjazdu określone w rozporządzeniu (UE) 2016/399. Obecność powiązania czerwonego sama w sobie nie powinna jednak stanowić przyczyny odmowy wjazdu, a obowiązujący wykaz warunków odmowy wjazdu zawarty w rozporządzeniu (UE) 2016/399 nie powinien zatem ulec zmianie.

(64) Należałoby zaktualizować Praktyczny podręcznik dla straży granicznej, aby doprecyzować powyższe wyjaśnienia.

(65) Jeśli zapytanie w detektorze wielokrotnych tożsamości za pośrednictwem europejskiego portalu wyszukiwania wykaże obecność powiązania żółtego lub czerwonego, funkcjonariusz straży granicznej powinien dokonywać sprawdzeń wspólnego repozytorium danych umożliwiających identyfikację lub SIS lub do ich obu, aby uzyskać dostęp do informacji o kontrolowanej osobie, ręcznie zweryfikować dane dotyczące jej tożsamości i w razie potrzeby odpowiednio dostosować kolor powiązania.

(66) Na potrzeby statystyk i sprawozdawczości konieczne jest przyznanie dostępu uprawnionemu personelowi właściwych organów oraz instytucji Unii i agencji unijnych, o których mowa w niniejszym rozporządzeniu, aby mogły sprawdzać niektóre dane związane z pewnymi elementami interoperacyjności bez umożliwiania im identyfikacji osób fizycznych.

(67) Aby umożliwić organom państw członkowskich i agencjom unijnym dostosowanie się do nowych wymogów w zakresie korzystania z europejskiego portalu wyszukiwania, konieczne jest wprowadzenie okresu przejściowego. Podobnie aby umożliwić spójne i optymalne funkcjonowanie detektora wielokrotnych tożsamości należy, na początku jego działania, ustanowić środki przejściowe.

(68) Ponieważ celu niniejszego rozporządzenia, mianowicie stworzenia ram interoperacyjności unijnych systemów informacyjnych, nie mogą w wystarczający sposób osiągnąć państwa członkowskie, natomiast z uwagi na zakres i skutki działań można je lepiej osiągnąć na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej (TUE). Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(69) Pozostała kwota przeznaczona w budżecie na inteligentne granice zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 515/2014 ([20]) powinna zostać przydzielona na potrzeby niniejszego rozporządzenia zgodnie z art. 5 ust. 5 lit. b) rozporządzenia (UE) nr 515/2014 w celu pokrycia kosztów opracowania elementów interoperacyjności.

(70) Aby uzupełnić pewne szczegółowe aspekty techniczne niniejszego rozporządzenia, należy przyznać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) w zakresie:

— wydłużenia okresu przejściowego użytkowania europejskiego portalu wyszukiwania,

— wydłużenia okresu przejściowego dotyczącego wykrywania wielokrotnych tożsamości przez jednostkę centralną ETIAS,

— procedur określania przypadków, w których dane dotyczące tożsamości można uznać za tożsame lub zbliżone,

— zasad funkcjonowania centralnego repozytorium sprawozdawczo-statystycznego, w tym szczególnych gwarancji dotyczących przetwarzania danych osobowych oraz zasad bezpieczeństwa mających zastosowanie do repozytorium, oraz

— szczegółowych zasad funkcjonowania portalu internetowego.

Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r. ([21]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(71) Aby zapewnić jednolite warunki wykonania niniejszego rozporządzenia, należy przyznać Komisji uprawnienia wykonawcze obejmujące określanie terminów, w których europejski portal wyszukiwania, wspólny system porównywania danych biometrycznych, wspólne repozytorium danych umożliwiających identyfikację, detektor wielokrotnych tożsamości oraz centralne repozytorium sprawozdawczo-statystyczne zaczną funkcjonować.

([20]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 515/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego w zakresie granic zewnętrznychi wiz oraz uchylające decyzję nr 574/2007/WE (Dz.U. L 150 z 20.5.2014, s. 143).

([21]) Dz.U. L 123 z 12.5.2016, s. 1.

(72) Należy również przyznać Komisji uprawnienia wykonawcze dotyczące przyjmowania szczegółowych przepisów w zakresie: informacji technicznych dotyczących profili użytkowników europejskiego portalu wyszukiwania; specyfikacji rozwiązania technicznego umożliwiającego przeszukiwanie systemów informacyjnych UE, baz danych Europolu i Interpolu za pomocą europejskiego portalu wyszukiwania i formatu odpowiedzi uzyskiwanych w europejskim portalu wyszukiwania; przepisów technicznych służących do tworzenia powiązań w ramach detektora wielokrotnych tożsamości między danymi z różnych systemów informacyjnych UE; treści i formatu formularza, który ma być stosowany do powiadamiania osoby, której dane dotyczą, w przypadku powstania powiązania czerwonego; wymogów dotyczących wyników i monitorowania funkcjonowania wspólnego systemu porównywania danych biometrycznych; mechanizmów, procedur i wskaźników związanych z automatyczną kontrolą jakości danych; rozwijania standardu uniwersalnego formatu wiadomości (UMF); procedury współpracy, która ma być stosowana w przypadku incydentów bezpieczeństwa; oraz specyfikacji technicznego rozwiązania mającego służyć zarządzaniu przez państwa członkowskie wnioskami użytkowników o dostęp. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([22]).

(73) Ponieważ elementy interoperacyjności będą obejmować przetwarzanie znaczących ilości wrażliwych danych osobowych, ważne jest, aby osoby, których dane są przetwarzane za pośrednictwem tych elementów, mogły skutecznie korzystać z praw przysługujących osobom, których dane dotyczą, zgodnie z wymogami rozporządzenia (UE) 2016/679, dyrektywy (UE) 2016/2016 oraz rozporządzenia (WE) nr 2018/1725. Osobom, których dane dotyczą, należy zapewnić portal internetowy ułatwiający wykonywanie przysługujących im praw w zakresie dostępu do danych, ich korekty, usuwania i ograniczania przetwarzania ich danych osobowych. eu-LISA powinna stworzyć taki portal internetowy i zarządzać nim.

(74) Jedną z podstawowych zasad ochrony danych jest minimalizacja danych: zgodnie z art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679 przetwarzanie danych osobowych musi być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Z tego względu elementy interoperacyjności nie powinny przewidywać przechowywania nowych danych osobowych, z wyjątkiem powiązań, które będą przechowywane w detektorze wielokrotnych tożsamości i które stanowią minimum niezbędne do celów niniejszego rozporządzenia.

(75) Niniejsze rozporządzenie powinno zawierać jasne przepisy dotyczące odpowiedzialności i prawa do odszkodowania za niezgodne z prawem przetwarzanie danych osobowych oraz za inne działanie niezgodne z przepisami niniejszego rozporządzenia. Takie przepisy pozostają bez uszczerbku dla prawa do odszkodowania od administratora lub podmiotu przetwarzającego i odpowiedzialności tych podmiotów zgodnie z rozporządzeniem (UE) 2016/679, dyrektywą (UE) 2016/680 i rozporządzeniem (WE) 2018/1725. eu-LISA powinna być odpowiedzialna za szkodę spowodowaną przez siebie jako podmiotu przetwarzającego dane w przypadku gdy nie wypełniła ona szczególnych obowiązków nałożonych na nią w niniejszym rozporządzeniu lub gdy działała ona bez zgodnych z prawem zaleceń państwa członkowskiego będącego administratorem danych albo wbrew tym zaleceniom.

(76) Niniejsze rozporządzenie pozostaje bez uszczerbku dla dyrektywy Parlamentu Europejskiego i Rady 2004/38/WE ([23]).

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

(78) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Zjednoczonego Królestwa, zgodnie z decyzją Rady 2000/365/WE ([24]); Zjednoczone Królestwo nie uczestniczy zatem w przyjęciu niniejszego rozporządzenia, nie jest nim związane ani go nie stosuje.

(79) Niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Irlandii zgodnie z decyzją Rady 2002/192/WE ([25]); Irlandia nie uczestniczy w związku z tym w przyjęciu niniejszego rozporządzenia, nie jest nim związana ani go nie stosuje.

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

([23]) Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium Państw Członkowskich, zmieniająca rozporządzenie (EWG) nr 1612/68 i uchylająca dyrektywy 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG i 93/96/EWG (Dz.U. L 158 z 30.4.2004, s. 77).

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

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

(80) W odniesieniu do Islandii i Norwegii niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, w rozumieniu umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii, dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([26]), który należy do dziedziny, o której mowa w art. 1 pkt A, B i G decyzji Rady 1999/437/WE ([27]).

(81) W odniesieniu do Szwajcarii niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([28]), które wchodzą w zakres obszaru, o którym mowa w art. 1 pkt A, B i G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2008/146/WE ([29]).

(82) W odniesieniu do Liechtensteinu niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu o przystąpieniu Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([30]), które wchodzą w zakres obszaru, o którym mowa w art. 1 pkt A, B, C i G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2011/350/UE ([31]).

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

(84) Aby niniejsze rozporządzenie było spójne z obowiązującymi ramami prawnymi, rozporządzenia (WE) nr 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE ([32]) i 2008/633/WSiSW ([33]) powinny zostać odpowiednio zmienione,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot

1. Niniejsze rozporządzenie, wraz z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/818 ([34]), ustanawia ramy zapewniające interoperacyjność systemu wjazdu/wyjazdu (EES), wizowego systemu informacyjnego (VIS), europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS), systemu Eurodac, Systemu Informacyjnego Schengen (SIS) oraz europejskiego systemu przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN).

([26]) Dz.U. L 176 z 10.7.1999, s. 36.
([27]) Decyzja Rady 1999/437/WE z dnia 17 maja 1999 r. w sprawie niektórych warunków stosowania Układu zawartego przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącego włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 176 z 10.7.1999, s. 31).
([28]) Dz.U. L 53 z 27.2.2008, s. 52.
([29]) Decyzja Rady 2008/146/WE z dnia 28 stycznia 2008 r. w sprawie zawarcia w imieniu Wspólnoty Europejskiej Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia tego państwa we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 53 z 27.2.2008, s. 1).
([30]) Dz.U. L 160 z 18.6.2011, s. 21.
([31]) Decyzja Rady 2011/350/UE z dnia 7 marca 2011 r. w sprawie zawarcia w imieniu Unii Europejskiej Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, odnoszącego się do zniesienia kontroli na granicach wewnętrznych i do przemieszczania się osób (Dz.U. L 160 z 18.6.2011, s. 19).
([32]) Decyzja Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (Dz.U. L 213 z 15.6.2004, s. 5).
([33]) Decyzja Rady (WE) nr 2008/633/WSiSW z dnia 23 czerwca 2008 r. w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania (Dz.U. L 218 z 13.8.2008, s. 129).
([34]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/818 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze współpracy policyjnej i sądowej, azylu i migracji oraz zmieniające rozporządzenia (UE) 2018/1726, (UE) 2018/1862 i (UE) 2019/816 (zob. s. 85 niniejszego Dziennika Urzędowego).

2. Ramy te obejmują następujące elementy interoperacyjności:

a) europejski portal wyszukiwania;

b) wspólny system porównywania danych biometrycznych;

c) wspólne repozytorium danych umożliwiających identyfikację;

d) detektor wielokrotnych tożsamości.

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

4. Rozporządzenie dostosowuje także procedury i warunki dostępu wyznaczonych organów i Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) do EES, VIS, ETIAS oraz systemu Eurodac na potrzeby zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom oraz ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych.

5. Rozporządzenie określa też ramy weryfikacji tożsamości i identyfikacji osób.

Artykuł 2

Cele

1. Poprzez zapewnienie interoperacyjności niniejsze rozporządzenie służy następującym celom:

a) poprawie skuteczności i wydajności kontroli granicznych na granicach zewnętrznych;

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

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

d) poprawie wdrażania wspólnej polityki wizowej;

e) pomocy w rozpatrywaniu wniosków o udzielenie ochrony międzynarodowej;

f) przyczynianiu się do zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie postępowań przygotowawczych;

g) ułatwianiu w identyfikacji nieznanych osób, które nie są w stanie potwierdzić swojej tożsamości, lub niezidentyfikowanych szczątków ludzkich w przypadku klęski żywiołowej, wypadku lub zamachu terrorystycznego.

2. Cele, o których mowa w ust. 1, są osiągane przez:

a) zapewnienie poprawnej identyfikacji osób;

b) wspieranie walki z oszustwami dotyczącymi tożsamości;

c) poprawę jakości danych i harmonizację wymogów jakościowych w odniesieniu do danych przechowywanych w systemach informacyjnych UE przy jednoczesnym poszanowaniu wymogów dotyczących przetwarzania danych zawartych w aktach prawnych regulujących poszczególne systemy, a także norm i zasad ochrony danych;

d) ułatwianie i wspieranie technicznego i operacyjnego wdrożenia przez państwa członkowskie systemów informacyjnych UE;

e) wzmocnienie, uproszczenie i ujednolicenie warunków bezpieczeństwa danych i ochrony danych regulujących odpowiednie systemy informacyjne UE, bez wpływu na specjalną ochronę i gwarancje zapewnione dla pewnych kategorii danych;

f) usprawnienie warunków dostępu wyznaczonych organów do systemów EES, VIS, ETIAS i Eurodac przy zapewnieniu niezbędnych i proporcjonalnych warunków tego dostępu;

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

Artykuł 3

Zakres

1. Niniejsze rozporządzenie stosuje się do EES, VIS, ETIAS i SIS.

2. Niniejsze rozporządzenie obowiązuje w stosunku do osób, których dane osobowe mogą być przetwarzane za pomocą systemów informacyjnych UE, o których mowa w ust. 1 niniejszego artykułu i których dane są gromadzone do celów określonych w art. 1 i 2 rozporządzenia (WE) nr 767/2008, art. 1 rozporządzenia (UE) 2017/2226, art. 4 rozporządzenia (UE) 2018/1240, art. 1 rozporządzenia (UE) 2018/1860 oraz art. 1 rozporządzenia (UE) 2018/1861.

Artykuł 4

Definicje

Na potrzeby niniejszego rozporządzenia stosuje się następujące definicje:

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

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

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

4) „organy nadzorcze" oznaczają organ nadzorczy, o którym mowa w art. 51 ust. 1 rozporządzenia (UE) 2016/679, oraz organ nadzorczy, o którym mowa w art. 41 ust. 1 dyrektywy (UE) 2016/680;

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

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

7) „dane alfanumeryczne" oznaczają dane wyrażone literami, cyframi, znakami specjalnymi, odstępami i znakami przestankowymi;

8) „dane dotyczące tożsamości" oznaczają dane, o których mowa w art. 27 ust. 3, lit. a)–e);

9) „dane daktyloskopijne" oznaczają odwzorowania odcisków palców i śladów palców, które ze względu na ich niepowtarzalny charakter i układ cech szczególnych linii papilarnych umożliwiają dokładne i jednoznaczne ustalenie tożsamości danej osoby;

10) „wizerunek twarzy" oznacza cyfrowe wizerunki twarzy osoby;

11) „dane biometryczne" oznaczają dane daktyloskopijne lub wizerunki twarzy lub oba te elementy;

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

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

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

15) „systemy informacyjne UE" oznaczają EES, VIS, ETIAS, Eurodac, SIS i ECRIS-TCN;

16) „dane Europolu" oznaczają dane osobowe przetwarzane przez Europol do celów, o których mowa w art. 18 ust. 2 lit. a), b) i c) rozporządzenia (UE) 2016/794;

17) „bazy danych Interpolu" oznaczają bazę Interpolu zawierającą dane skradzionych lub utraconych dokumentów podróży (zwaną dalej „bazą danych SLTD") i bazę danych dokumentów podróży powiązanych z notami Interpolu (zwaną dalej „bazą danych TDAWN");

18) „dopasowanie" oznacza istnienie zgodności ustalone w wyniku automatycznego porównania danych osobowych zarejestrowanych lub będących w trakcie rejestrowania w systemie informacyjnym lub bazie danych;

19) „organ policji" oznacza właściwy organ zgodnie z definicją zawartą w art. 3 pkt 7 dyrektywy (UE) 2016/680;

20) „wyznaczone organy" oznaczają wyznaczone przez państwo członkowskie organy zdefiniowane w art. 3 ust. 1 pkt 26 rozporządzenia (UE) 2017/2226, art. 2 ust. 1 lit. e) decyzji 2008/633/WSiSW i art. 3 ust. 1 pkt 21 rozporządzenia (UE) 2018/1240;

21) „przestępstwo terrorystyczne" oznacza określone w prawie krajowym przestępstwo odpowiadające lub równoważne jednemu z przestępstw, o których mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/541 ([35]);

22) „poważne przestępstwo" oznacza przestępstwo odpowiadające lub równoważne jednemu z przestępstw, o których mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW ([36]), jeżeli zgodnie z prawem krajowym podlega ono karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat;

23) „system wjazdu/wyjazdu" lub „EES" oznacza system wjazdu/wyjazdu ustanowiony w rozporządzeniu (UE) 2017/2226;

24) „wizowy system informacyjny" lub „VIS" oznacza wizowy system informacyjny ustanowiony w rozporządzeniu (WE) nr 767/2008;

25) „europejski system informacji o podróży oraz zezwoleń na podróż" lub „ETIAS" oznacza europejski system informacji o podróży oraz zezwoleń na podróż ustanowiony w rozporządzeniu (UE) 2018/1240;

26) „Eurodac" oznacza system Eurodac ustanowiony w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 603/2013 ([37]);

27) „System Informacyjny Schengen" lub „SIS" oznacza system informacyjny Schengen ustanowiony w rozporządzeniach (UE) 2018/1860, (UE) 2018/1861 i (UE) 2018/1862;

28) „ECRIS-TCN" oznacza scentralizowany system identyfikacji państw członkowskich posiadających informacje o wyrokach skazujących w odniesieniu do obywateli państw trzecich i bezpaństwowców ustanowiony w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/816 ([38]).

Artykuł 5

Zakaz dyskryminacji i prawa podstawowe

Przetwarzanie danych osobowych do celów niniejszego rozporządzenia nie może prowadzić do dyskryminacji ze względów takich jak płeć, rasa, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religia lub przekonania, poglądy polityczne lub jakiekolwiek inne, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek czy orientacja seksualna. Odbywa się ono z pełnym poszanowaniem godności ludzkiej i integralności osoby oraz praw podstawowych, w tym prawa do poszanowania życia prywatnego i do ochrony danych osobowych. Szczególną uwagę poświęca się dzieciom, osobom starszym, niepełnosprawnym, a także osobom wymagającym ochrony międzynarodowej. Dobro dziecka ma wagę nadrzędną.

ROZDZIAŁ II

Europejski portal wyszukiwania

Artykuł 6

Europejski portal wyszukiwania

1. Europejski portal wyszukiwania ustanawia się, aby ułatwić organom państw członkowskich i agencjom unijnym uzyskiwanie szybkiego, sprawnego, wydajnego, systematycznego i kontrolowanego dostępu do systemów informacyjnych UE, danych Europolu i baz danych Interpolu w celu pełnienia przez nie ich funkcji oraz zgodnie z przysługującymi im prawami dostępu, a także celami i zamierzeniami systemów EES, VIS, ETIAS, Eurodac, SIS oraz ECRIS-TCN.

([35]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

([36]) Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).

([37]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.U. L 180 z 29.6.2013, s. 1).

([38]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (zob. s. 1 niniejszego Dziennika Urzędowego).

2. Europejski portal wyszukiwania składa się z:

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

b) bezpiecznego kanału komunikacji między europejskim portalem wyszukiwania a państwami członkowskimi i agencjami unijnymi uprawnionymi do korzystania z europejskiego portalu wyszukiwania;

c) bezpiecznej infrastruktury łączności między europejskim portalem wyszukiwania a systemami EES, VIS, ETIAS, Eurodac, systemem centralnym SIS, systemem ECRIS-TCN, danymi Europolu i bazami danych Interpolu, a także między europejskim portalem wyszukiwania a infrastrukturą centralną wspólnego repozytorium danych umożliwiających identyfikację i detektorem wielokrotnych tożsamości.

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

Artykuł 7

Korzystanie z europejskiego portalu wyszukiwania

1. Korzystanie z europejskiego portalu wyszukiwania jest zarezerwowane dla organów państw członkowskich i agencji unijnych mających dostęp do przynajmniej jednego z systemów informacyjnych UE, zgodnie z instrumentami prawnymi regulującymi funkcjonowanie tych systemów, do wspólnego repozytorium danych umożliwiających identyfikację i detektora wielokrotnych tożsamości zgodnie z niniejszym rozporządzeniem, do danych Europolu zgodnie z rozporządzeniem (UE) 2016/794 lub do baz danych Interpolu zgodnie z prawem Unii lub prawem krajowym regulującym taki dostęp.

Powyższe organy państw członkowskich i agencje unijne mogą korzystać z europejskiego portalu wyszukiwania i danych przekazanych przez ten portal tylko do celów ustanowionych w aktach prawnych regulujących te systemy informacyjne UE, w rozporządzeniu (UE) 2016/794 i w niniejszym rozporządzeniu.

2. Organy państw członkowskich i agencje unijne, o których mowa w ust. 1, korzystają z europejskiego portalu wyszukiwania, aby wyszukiwać dane dotyczące osób lub ich dokumentów podróży przechowywane w systemach centralnych EES, VIS i ETIAS zgodnie z prawami dostępu, o których mowa w aktach prawnych regulujących te systemy informacyjne UE oraz w prawie krajowym. Korzystają one także z europejskiego portalu wyszukiwania, aby konsultować wspólne repozytorium danych umożliwiających identyfikację zgodnie z prawami dostępu przysługującymi im na mocy niniejszego rozporządzenia do celów, o których mowa w art. 20, 21 i 22.

3. Organy UE, o których mowa w ust. 1, mogą z niego korzystać, aby wyszukiwać dane dotyczące osób lub ich dokumentów podróży w systemie centralnym SIS, o których mowa w rozporządzeniach (UE) 2018/1860 i (UE) 2018/1861.

4. W przypadkach gdy przewiduje to prawo Unii, agencje unijne, o których mowa w ust. 1, korzystają z europejskiego portalu wyszukiwania, aby wyszukiwać dane dotyczące osób lub ich dokumentów podróży w systemie centralnym SIS.

5. Organy państw członkowskich lub agencje unijne, o których mowa w ust. 1, mogą korzystać z europejskiego portalu wyszukiwania, aby wyszukiwać dane dokumentów podróży przechowywane w bazach danych Interpolu, jeżeli jest to przewidziane i zgodnie z prawami dostępu przysługującymi im na mocy prawa Unii i prawa krajowego.

Artykuł 8

Profile użytkowników europejskiego portalu wyszukiwania

1. Aby umożliwić korzystanie z europejskiego portalu wyszukiwania, eu-LISA, we współpracy z państwami członkowskimi, opracowuje odrębny profil w oparciu o każdą kategorię użytkownika europejskiego portalu wyszukiwania i o cele zapytań, zgodnie ze szczegółowymi informacjami technicznymi i prawami dostępu, o których mowa w ust. 2. Każdy profil zgodnie z prawem Unii i prawem krajowym obejmuje następujące informacje:

a) pola danych, które mają być wykorzystywane w zapytaniach;

b) systemy informacyjne UE, dane Europolu i bazy danych Interpolu, które mają być przeglądane, które mogą być przeglądane oraz te, które powinny zapewnić udzielenie odpowiedzi użytkownikowi;

c) konkretne dane w systemach informacyjnych UE, dane Europolu i bazy danych Interpolu, które mogą być przeszukiwane;

d) kategorie danych, które mogą być przekazywane w każdej odpowiedzi.

2. Komisja przyjmuje akty wykonawcze, aby określić szczegóły techniczne profili, o których mowa w ust. 1, zgodnie z prawami dostępu przysługującymi użytkownikom europejskiego portalu wyszukiwania, na mocy aktów prawnych regulujących systemy informacyjne UE i prawa krajowego. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

3. Profile, o których mowa w ust. 1, są poddawane regularnym przeglądom przez eu-LISA we współpracy z państwami członkowskimi co najmniej raz w roku i w razie konieczności uaktualniane.

Artykuł 9

Zapytania

1. Użytkownicy europejskiego portalu wyszukiwania mogą dokonać zapytania, wprowadzając do niego dane alfanumeryczne lub biometryczne. Po dokonaniu zapytania europejski portal wyszukiwania przeszukuje równocześnie systemy EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, wspólne repozytorium danych umożliwiających identyfikację, dane Europolu i bazy danych Interpolu, za pomocą danych wprowadzonych przez użytkownika, zgodnie z jego profilem.

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

3. eu-LISA we współpracy z państwami członkowskimi wdraża dokument kontroli interfejsu oparty na uniwersalnym formacie wiadomości, o którym mowa w art. 38, w odniesieniu do europejskiego portalu wyszukiwania.

4. W przypadku dokonania zapytania przez użytkownika europejskiego portalu wyszukiwania, systemy EES, ETIAS, VIS, SIS, Eurodac, system ECRIS-TCN, wspólne repozytorium danych umożliwiających identyfikację, detektor wielokrotnych tożsamości, dane Europolu i bazy danych Interpolu dostarczają w odpowiedzi przechowywane w nich dane.

Bez uszczerbku dla art. 20 odpowiedź udzielana przez europejski portal wyszukiwania wskazuje, do którego systemu informacyjnego lub do której bazy należą dane.

W ramach europejskiego portalu wyszukiwania nie są udzielane żadne informacje dotyczące danych w systemach informacyjnych UE, danych Europolu i baz danych Interpolu, do których użytkownik nie ma dostępu na mocy mającego zastosowanie prawa Unii i prawa krajowego.

5. Przeszukiwania baz danych Interpolu dokonywane za pośrednictwem europejskiego portalu wyszukiwania są realizowane w taki sposób, by żadne informacje nie zostały ujawnione właścicielowi wpisu w bazie Interpolu.

6. Europejski portal wyszukiwania przekazuje odpowiedzi użytkownikowi niezwłocznie po udostępnieniu danych z jednego z systemów informacyjnych UE, danych Europolu lub baz danych Interpolu. Odpowiedzi te zawierają wyłącznie dane, do których użytkownik ten ma dostęp na mocy prawa Unii i prawa krajowego.

7. Komisja przyjmuje akt wykonawczy w celu szczegółowego określenia procedury technicznej dotyczącej przeszukiwania systemów informacyjnych UE, danych Europolu i baz danych Interpolu za pomocą europejskiego portalu wyszukiwania oraz formatu odpowiedzi udzielanych przez europejski portal wyszukiwania. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 10

Prowadzenie rejestrów

1. Bez uszczerbku dla art. 46 rozporządzenia (UE) 2017/2226, art. 34 rozporządzenia (WE) nr 767/2008, art. 69 rozporządzenia (UE) 2018/1240 oraz art. 12 i 18 rozporządzenia (UE) 2018/1861, eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach europejskiego portalu wyszukiwania. Rejestry te obejmują:

a) państwo członkowskie lub agencję Unii dokonujące zapytania i zastosowany profil użytkownika europejskiego portalu wyszukiwania;

b) datę i godzinę zapytania;

c) przeszukiwane systemy informacyjne UE i bazy danych Interpolu.

2. Każde państwo członkowskie prowadzi rejestry zapytań dokonywanych przez jego organy i personel tych organów należycie upoważniony do korzystania z europejskiego portalu wyszukiwania. Każda agencja unijna prowadzi rejestry zapytań dokonywanych przez jej należycie upoważniony personel.

3. Rejestry, o których mowa w ust. 1 i 2, można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności wniosku i zgodności z prawem przetwarzania danych, oraz w celu zapewniania bezpieczeństwa i integralności danych. Rejestry są chronione za pomocą odpowiednich środków przed nieuprawnionym dostępem i usuwane jeden rok po utworzeniu. Jeżeli jednak są one konieczne do prowadzenia już rozpoczętych procedur monitorowania, są one usuwane, gdy tylko przestają być konieczne do celu tych procedur.

Artykuł 11

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

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

2. Jeśli korzystanie z europejskiego portalu wyszukiwania w celu przeszukiwania jednego lub większej liczby systemów informacyjnych UE lub wspólnego repozytorium danych umożliwiających identyfikację, nie jest technicznie możliwe z powodu awarii infrastruktury krajowej w jednym z państw członkowskich, to państwo członkowskie automatycznie powiadamia o tym fakcie eu-LISA i Komisję.

3. W przypadkach, o których mowa w ust. 1 lub 2 niniejszego artykułu, do czasu rozwiązania problemu technicznego obowiązek, o którym mowa w art. 7 ust. 2 i 4, nie obowiązuje, a państwa członkowskie mają dostęp do systemów informacyjnych UE lub do wspólnego repozytorium danych umożliwiających identyfikację, jeżeli są do tego zobowiązane na mocy prawa Unii lub prawa krajowego.

4. Jeśli korzystanie z europejskiego portalu wyszukiwania w celu przeszukiwania co najmniej jednego systemu informacyjnego UE lub wspólnego repozytorium danych umożliwiających identyfikację nie jest technicznie możliwe z powodu awarii infrastruktury agencji Unii, agencja ta automatycznie powiadamia o tym fakcie eu-LISA i Komisję.

ROZDZIAŁ III

Wspólny system porównywania danych biometrycznych

Artykuł 12

Wspólny system porównywania danych biometrycznych

1. Wspólny system porównywania danych biometrycznych gromadzący wzorce biometryczne uzyskane z danych biometrycznych, o których mowa w art. 13, przechowywane we wspólnym repozytorium danych umożliwiających identyfikację i w SIS oraz umożliwiający jednoczesne wyszukiwanie za pomocą danych biometrycznych w różnych systemach informacyjnych UE ustanawia się, aby wspierać wspólne repozytorium danych umożliwiających identyfikację i detektor wielokrotnych tożsamości oraz realizację celów systemów EES, VIS, Eurodac, SIS i systemu ECRIS-TCN.

2. Wspólny system porównywania danych biometrycznych składa się z następujących elementów:

a) infrastruktury centralnej, która zastępuje systemy centralne, odpowiednio, systemów EES, VIS, SIS, Eurodac i ECRIS-TCN w zakresie przechowywania wzorców biometrycznych i umożliwiania wyszukiwania przy użyciu danych biometrycznych;

b) bezpiecznej infrastruktury łączności między wspólnym systemem porównywania danych biometrycznych, systemem centralnym SIS i wspólnym repozytorium danych umożliwiających identyfikację.

3. Wspólny system porównywania danych biometrycznych opracowuje eu-LISA, która zarządzani nim też od strony technicznej.

Artykuł 13

Przechowywanie wzorców biometrycznych we wspólnym systemie porównywania danych biometrycznych

1. We wspólnym systemie porównywania danych biometrycznych przechowuje się wzorce biometryczne, uzyskane na podstawie następujących danych biometrycznych:

a) dane, o których mowa w art. 16 ust. 1 lit. d), art. 17 ust. 1 lit. b) i c) oraz w art. 18 ust. 2 lit. a), b) i c) rozporządzenia (UE) 2017/2226;

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

c) dane, o których mowa w art. 20 ust. 2 lit. w) i x), z wyłączeniem danych dotyczących odcisków dłoni, rozporządzenia (UE) 2018/1861;

d) dane, o których mowa w art. 4 ust. 1 lit. u) i v), z wyłączeniem danych dotyczących odcisków dłoni, rozporządzenia (UE) 2018/1860.

Wzorce biometryczne przechowywane we wspólnym systemie porównywania danych biometrycznych są logicznie oddzielone w zależności od systemu informacyjnego UE, z którego te dane pochodzą.

2. Dla każdego zestawu danych, o których mowa w ust. 1, wspólny system porównywania danych biometrycznych zawiera w każdym wzorcu biometrycznym odniesienie do systemów informacyjnych UE, w którym są przechowywane powiązane z nim dane biometryczne, oraz odniesienie do rzeczywistego zapisu w tych systemach informacyjnych UE.

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

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

5. Komisja określa w drodze aktów wykonawczych wymogi dotyczące wydajności oraz praktyczne ustalenia dotyczące monitorowania wydajności wspólnego systemu porównywania danych biometrycznych, aby zapewnić skuteczność przeszukiwania danych biometrycznych w przypadku procedur, w których czynnikiem krytycznym jest czas, takich jak odprawa graniczna i identyfikacja. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 14

Przeszukiwanie danych biometrycznych za pomocą wspólnego systemu porównywania danych biometrycznych

Aby przeszukiwać dane biometryczne zgromadzone we wspólnym repozytorium danych umożliwiających identyfikację i w SIS, wspólne repozytorium danych umożliwiających identyfikację i SIS korzystają z wzorców biometrycznych przechowywanych we wspólnym systemie porównywania danych biometrycznych. Zapytań zawierających dane biometryczne dokonuje się zgodnie z celami określonymi w niniejszym rozporządzeniu oraz w rozporządzeniach (WE) nr 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 i (UE) 2019/816.

Artykuł 15

Zatrzymywanie danych we wspólnym systemie porównywania danych biometrycznych

Dane, o których mowa w art. 13 ust. 1 i 2, są przechowywane we wspólnym systemie porównywania danych biometrycznych tak długo, jak długo odpowiadające im dane biometryczne są przechowywane we wspólnym repozytorium danych umożliwiających identyfikację lub w SIS. Dane te są automatycznie usuwane ze wspólnego systemu porównywania danych biometrycznych.

Artykuł 16

Prowadzenie rejestrów

1. Bez uszczerbku dla art. 46 rozporządzenia (UE) 2017/2226, art. 34 rozporządzenia (WE) nr 767/2008 oraz art. 12 i 18 rozporządzenia (UE) 2018/1861, eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach wspólnego systemu porównywania danych biometrycznych. Rejestry te obejmują:

a) państwo członkowskie lub agencję Unii dokonujące zapytania;

b) historię tworzenia i przechowywania wzorców biometrycznych;

c) systemy informacyjne UE przeszukiwane za pomocą wzorców biometrycznych przechowywanych we wspólnym systemie porównywania danych biometrycznych;

d) datę i godzinę zapytania;

e) rodzaj danych biometrycznych użytych przy dokonywaniu zapytania;

f) wyniki zapytania oraz datę i godzinę ich uzyskania.

2. Każde państwo członkowskie prowadzi rejestry zapytań dokonywanych przez jego organy i personel tych organów należycie upoważniony do korzystania ze wspólnego systemu porównywania danych biometrycznych. Każda agencja unijna prowadzi rejestry zapytań dokonywanych przez jej należycie upoważniony personel.

3. Rejestry, o których mowa w ust. 1 i 2, można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności wniosku i zgodności przetwarzania danych z prawem, oraz w celu zapewniania bezpieczeństwa i integralności danych. Rejestry są chronione za pomocą odpowiednich środków przed nieuprawnionym dostępem i usuwane jeden rok po utworzeniu. Jeżeli jednak są one konieczne do prowadzenia już rozpoczętych procedur monitorowania, są one usuwane, gdy tylko przestają być konieczne do celu tych procedur.

ROZDZIAŁ IV

Wspólne repozytorium danych umożliwiających identyfikację

Artykuł 17

Wspólne repozytorium danych umożliwiających identyfikację

1. Wspólne repozytorium danych umożliwiających identyfikację, tworzące indywidualne akta osobowe dla każdej osoby zarejestrowanej w systemach EES, VIS, ETIAS, Eurodac lub ECRIS-TCN, zawierające dane, o których mowa w art. 18, ustanawia się po to, aby ułatwiać i wspomagać poprawną identyfikację osób zarejestrowanych w systemach EES, VIS, ETIAS, Eurodac i ECRIS-TCN zgodnie z art. 20, wspierać funkcjonowanie detektora wielokrotnych tożsamości zgodnie z art. 21 oraz, w stosownych przypadkach, ułatwiać i usprawniać dostęp wyznaczonych organów i Europolu do systemów EES, VIC, ETIAS i Eurodac w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywania ich lub prowadzenia w ich sprawie postępowań przygotowawczych zgodnie z art. 22.

2. Wspólne repozytorium danych umożliwiających identyfikację składa się z:

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

b) bezpiecznego kanału komunikacji między wspólnym repozytorium danych umożliwiających identyfikację, państwami członkowskimi i agencjami Unii uprawnionymi do korzystania ze wspólnego repozytorium danych umożliwiających identyfikację zgodnie z prawem Unii i prawem krajowym;

c) bezpiecznej infrastruktury łączności między wspólnym repozytorium danych umożliwiających identyfikację a systemami EES, VIS, ETIAS, Eurodac i ECRIS-TCN oraz wspólną infrastrukturą europejskiego portalu wyszukiwania, wspólnego systemu porównywania danych biometrycznych i detektora wielokrotnych tożsamości.

3. Wspólne repozytorium danych umożliwiających identyfikację opracowuje eu-LISA, która zarządzani nim też od strony technicznej.

4. Jeżeli dokonanie zapytania we wspólnym repozytorium danych umożliwiających identyfikację do celów identyfikacji osoby fizycznej zgodnie z art. 20 w celu wykrywania wielokrotnych tożsamości zgodnie z art. 21 lub w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywania ich lub prowadzenia w ich sprawie postępowań przygotowawczych zgodnie z art. 22 nie jest technicznie możliwe z powodu awarii wspólnego repozytorium danych umożliwiających identyfikację, eu-LISA automatycznie powiadamia o tym fakcie użytkowników wspólnego repozytorium danych umożliwiających identyfikację.

5. eu-LISA we współpracy z państwami członkowskimi wdraża dokument kontroli interfejsu oparty na uniwersalnym formacie wiadomości, o którym mowa w art. 38, w odniesieniu do wspólnego repozytorium danych umożliwiających identyfikację.

Artykuł 18

Dane we wspólnym repozytorium danych umożliwiających identyfikację

1. We wspólnym repozytorium danych umożliwiających identyfikację przechowuje się następujące, oddzielone logicznie dane, według systemu informacyjnego, z którego dane te pierwotnie pochodzą:

a) dane, o których mowa w art. 16 ust. 1 lit. a)–d), art. 17 ust. 1 lit. a), b) i c) oraz art. 18 ust. 1 i 2 rozporządzenia (UE) 2017/2226;

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

c) dane, o których mowa w art. 17 ust. 2 lit. a)-e) rozporządzenia (EU) 2018/1240.

2. Dla każdego zestawu danych, o których mowa w ust. 1, wspólne repozytorium danych umożliwiających identyfikację zawiera odniesienie do systemów informacyjnych UE, z których dane te pochodzą.

3. Organy korzystające z dostępu do wspólnego repozytorium danych umożliwiających identyfikację czynią to zgodnie z ich prawami dostępu na mocy aktów prawnych regulujących systemy informacyjne UE i prawa krajowego oraz zgodnie z przysługującymi im prawami dostępu na mocy niniejszego rozporządzenia do celów, o których mowa w art. 20, 21 i 22.

4. Dla każdego zestawu danych, o których mowa w ust. 1, wspólne repozytorium danych umożliwiających identyfikację zawiera odniesienie do rzeczywistego zapisu w systemach informacyjnych UE, z których dane te pochodzą.

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

Artykuł 19

Dodawanie, zmiana i usuwanie danych we wspólnym repozytorium danych umożliwiających identyfikację

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

2. W razie utworzenia powiązania białego lub czerwonego przez detektor wielokrotnych tożsamości zgodnie z art. 32 lub 33 między danymi z dwóch lub większej liczby systemów informacyjnych UE składających się na wspólne repozytorium danych umożliwiających identyfikację, zamiast tworzyć nowe akta osobowe, repozytorium dodaje nowe dane do akt osobowych, z których pochodzą powiązane ze sobą dane.

Artykuł 20

Dostęp do wspólnego repozytorium danych umożliwiających identyfikację w celu identyfikacji

1. Zapytania we wspólnym repozytorium danych umożliwiających identyfikację dokonywane jest przez organ policji zgodnie z ust. 2 i 5 wyłącznie w następujących przypadkach:

a) gdy organ policji nie jest w stanie zidentyfikować osoby z powodu braku dokumentu podróży lub innego wiarygodnego dokumentu potwierdzającego tożsamość tej osoby;

b) gdy istnieją wątpliwości co do danych dotyczących tożsamości dostarczonych przez osobę;

c) gdy istnieją wątpliwości co do autentyczności dokumentu podróży lub innego wiarygodnego dokumentu przedstawionego przez osobę;

d) gdy istnieją wątpliwości co do tożsamości posiadacza dokumentu podróży lub innego wiarygodnego dokumentu; lub

e) gdy osoba nie jest w stanie współpracować lub odmawia współpracy.

Dokonywanie takich zapytań nie jest dozwolone w odniesieniu do osób małoletnich, które nie ukończyły 12. roku życia, chyba że odbywa się to dla dobra dziecka.

2. W którymkolwiek z przypadków wymienionych w ust. 1, gdy organ policji został do tego upoważniony na mocy krajowych środków ustawodawczych, o których mowa w ust. 5, może on, wyłącznie w celu identyfikacji osoby fizycznej, dokonać zapytania we wspólnym repozytorium danych umożliwiających identyfikację, posługując się danymi biometrycznymi tej osoby pobranymi bezpośrednio podczas kontroli tożsamości, pod warunkiem że procedurę tę uruchamia się w obecności tej osoby.

3. Jeśli wynik zapytania wskaże, że dane tej osoby są przechowywane we wspólnym repozytorium danych umożliwiających identyfikację, organ policji powinien mieć możliwość sprawdzania danych, o których mowa w art. 18 ust. 1.

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

4. W przypadku katastrofy, wypadku lub zamachu terrorystycznego i wyłącznie w celu identyfikacji nieznanych osób, które nie są w stanie potwierdzić swojej tożsamości, lub niezidentyfikowanych szczątków ludzkich organ policji może przeszukiwać wspólne repozytorium danych umożliwiających identyfikację za pomocą danych biometrycznych tych osób, gdy został do tego upoważniony na mocy krajowych środków ustawodawczych, o których mowa w ust. 6.

5. Państwa członkowskie, które pragną skorzystać z możliwości przewidzianej w ust. 2, przyjmują odpowiednie krajowe środki ustawodawcze. Państwa członkowskie uwzględniają przy tym potrzebę unikania dyskryminacji wobec obywateli państw trzecich. Takie środki ustawodawcze precyzują cele identyfikacji na potrzeby określone w art. 2 ust. 1 lit. b) i c). Wyznaczają one właściwe organy policji i określają procedury, warunki i kryteria takich kontroli.

6. Państwa członkowskie, które chcą skorzystać z możliwości przewidzianej w ust. 4, przyjmują krajowe środki ustawodawcze określające procedury, warunki i kryteria.

Artykuł 21

Dostęp do wspólnego repozytorium danych umożliwiających identyfikację w celu wykrywania wielokrotnych tożsamości

1. Jeśli wynikiem zapytania we wspólnym repozytorium danych umożliwiających identyfikację jest powiązanie żółte określone w art. 28 ust. 4 organ odpowiedzialny za ręczną weryfikację różniących się tożsamości zgodnie z art. 29 ma dostęp, wyłącznie w celu przeprowadzenia tej weryfikacji, do danych, o których mowa w wart. 18 ust. 1 i 2, przechowywanych we wspólnym repozytorium danych umożliwiających identyfikację i połączonych powiązaniem żółtym.

2. Jeśli wynikiem zapytania we wspólnym repozytorium danych umożliwiających identyfikację jest powiązanie czerwone określone w art. 32 organy, o których mowa w art. 26 ust. 2, mają dostęp, wyłącznie w celu zwalczania oszustw dotyczących tożsamości, do danych, o których mowa w art. 18 ust. 1 i 2, przechowywanych we wspólnym repozytorium danych umożliwiających identyfikację i połączonych powiązaniem czerwonym.

Artykuł 22

Przeszukiwanie wspólnego repozytorium danych umożliwiających identyfikację w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywania ich lub prowadzenia w ich sprawie postępowań przygotowawczych

1. Jeżeli w konkretnym przypadku istnieją uzasadnione podstawy pozwalające uważać, że dokonanie sprawdzeń w systemach informacyjnych UE przyczyni się do zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych, zwłaszcza gdy zachodzi podejrzenie, że sprawca lub ofiara przestępstwa terrorystycznego lub innego poważnego przestępstwa lub osoba podejrzana o jego popełnienie to osoba, której dane są przechowywane w EES, VIS lub ETIAS, wyznaczone organy i Europol mogą dokonać sprawdzenia we wspólnym repozytorium danych umożliwiających identyfikację, aby uzyskać informację, czy dane dotyczące konkretnej osoby znajdują się w EES, VIS lub ETIAS.

2. Jeśli odpowiedź na zapytanie we wspólnym repozytorium danych umożliwiających identyfikację wskaże, że dane dotyczące tej osoby znajdują się w EES, VIS lub ETIAS, wspólne repozytorium danych umożliwiających identyfikację udziela odpowiedzi tym wyznaczonym organom i Europolowi w postaci odniesienia, o którym mowa w art. 18 ust. 2, wskazującego, który z systemów informacyjnych UE zawiera dane odpowiadające zapytaniu. Wspólne repozytorium danych umożliwiających identyfikację udziela odpowiedzi w sposób nienaruszający bezpieczeństwa danych.

Odpowiedź wskazująca, że dane dotyczące danej osoby znajdują się w jednym z systemów informacyjnych UE, o których mowa w ust. 1, może być wykorzystywana jedynie w celu złożenia wniosku o pełny dostęp z zastrzeżeniem warunków i procedur ustanowionych w odpowiednich aktach prawnych regulujących taki dostęp.

W przypadku przynajmniej jednego dopasowania wyznaczony organ lub Europol zwraca się z wnioskiem o pełny dostęp do co najmniej jednego z systemów informacyjnych, z których uzyskano dopasowanie.

W przypadku gdy wyjątkowo nie zwrócono się z wnioskiem o pełny dostęp, wyznaczone organy rejestrują powód, dla którego nie złożono takiego wniosku, identyfikowalny w dokumentacji krajowej. Europol odnotowuje ten powód w odpowiedniej dokumentacji wewnętrznej.

3. Pełen dostęp do danych zawartych w systemach EEAS, VIS lub ETIAS w celach zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania lub prowadzenia w ich sprawie postępowań przygotowawczych nadal podlega warunkom i procedurom określonym w odpowiednich aktach prawnych regulujących taki dostęp.

Artykuł 23

Zatrzymywanie danych we wspólnym repozytorium danych umożliwiających identyfikację

1. Dane, o których mowa w art. 18 ust. 1, 2 i 4, są automatycznie usuwane ze wspólnego repozytorium danych umożliwiających identyfikację zgodnie z przepisami dotyczącymi zatrzymywania danych w, odpowiednio, rozporządzeniach (UE) 2017/2226, (WE) nr 767/2008 i (UE) 2018/1240.

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

Artykuł 24

Prowadzenie rejestrów

1. Bez uszczerbku dla art. 46 rozporządzenia (UE) 2017/2226, art. 34 rozporządzenia (WE) nr 767/2008 oraz art. 69 rozporządzenia (UE) 2018/1240, eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w ramach wspólnego repozytorium danych umożliwiających identyfikację zgodnie z ust. 2, 3 i 4 niniejszego artykułu.

2. eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych zgodnie z art. 20 w ramach wspólnego repozytorium danych umożliwiających identyfikację. Rejestry te obejmują:

a) państwo członkowskie lub agencję unijną dokonujące zapytania;

b) cel dostępu użytkownika dokonującego zapytania za pośrednictwem wspólnego repozytorium danych umożliwiających identyfikację;

c) datę i godzinę zapytania;

d) rodzaj danych użytych przy dokonywaniu zapytania;

e) wyniki zapytania.

3. eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych zgodnie z art. 21 w ramach wspólnego repozytorium danych umożliwiających identyfikację. Rejestry te obejmują:

a) państwo członkowskie lub agencję unijną dokonujące zapytania;

b) cel dostępu użytkownika dokonującego zapytania za pośrednictwem wspólnego repozytorium danych umożliwiających identyfikację;

c) datę i godzinę zapytania;

d) w razie utworzenia powiązania dane użyte w zapytaniu i wyniki zapytania wskazujący system informacyjny UE, z którego pochodzą dane.

4. eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych zgodnie z art. 22 w ramach wspólnego repozytorium danych umożliwiających identyfikację. Rejestry te obejmują:

a) datę i godzinę zapytania;

b) dane użyte przy dokonywaniu zapytania;

c) wyniki zapytania;

d) państwo członkowskie lub agencję Unii dokonujące zapytania we wspólnym repozytorium danych umożliwiających identyfikację.

Rejestry dostępu podlegają regularnej weryfikacji przez właściwy organ nadzorczy zgodnie z art. 41 dyrektywy (UE) 2016/680 lub przez Europejskiego Inspektora Ochrony Danych zgodnie z art. 43 rozporządzenia (UE) 2016/794, w odstępach czasowych nieprzekraczających sześciu miesięcy, w celu sprawdzenia, czy procedury i warunki określone w art. 22 ust. 1 i 2 niniejszego rozporządzenia zostały spełnione.

5. Każde państwo członkowskie prowadzi rejestry zapytań dokonywanych przez jego organy i personel tych organów należycie upoważniony do korzystania z europejskiego portalu wyszukiwania na mocy art. 20, 21 i 22. Każda agencja unijna prowadzi rejestr zapytań dokonywanych przez jej należycie upoważniony personel na mocy art. 21 i 22.

Ponadto w przypadku każdego dostępu do wspólnego repozytorium danych umożliwiających identyfikację na mocy art. 22 każde państwo członkowskie prowadzi następujące rejestry:

a) dane referencyjne rejestru krajowego;

b) cel dostępu;

c) zgodnie z przepisami krajowymi niepowtarzalny identyfikator użytkownika należący do urzędnika, który dokonał zapytania, i do urzędnika, który je zlecił.

6. Zgodnie z rozporządzeniem (UE) 2016/794 w przypadku dostępu do wspólnego repozytorium danych umożliwiających identyfikację zgodnie z art. 22 niniejszego rozporządzenia Europol prowadzi rejestry niepowtarzalnego identyfikatora użytkownika należącego do urzędnika, który dokonał zapytania, i do urzędnika, który je zlecił.

7. Rejestry, o których mowa w ust. 2-6, można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności zapytania i zgodności przetwarzania danych z prawem, oraz w celu zapewniania bezpieczeństwa i integralności danych. Rejestry te są chronione za pomocą odpowiednich środków przed nieuprawnionym dostępem i usuwane rok po utworzeniu. Jeżeli jednak są one konieczne do prowadzenia już rozpoczętych procedur monitorowania, są one usuwane, gdy tylko przestają być konieczne do celu tych procedur.

8. eu-LISA przechowuje rejestry dotyczące historii danych w aktach osobowych. eu-LISA automatycznie usuwa takie rejestry po usunięciu tych danych.

ROZDZIAŁ V

Detektor wielokrotnych tożsamości

Artykuł 25

Detektor wielokrotnych tożsamości

1. Detektor wielokrotnych tożsamości, tworzący i przechowujący pliki potwierdzające tożsamość, o którym mowa w art. 34, zawierające powiązania między danymi zgromadzonymi w systemach informacyjnych UE, w tym we wspólnym repozytorium danych umożliwiających identyfikację i SIS oraz umożliwiające wykrywanie wielokrotnych tożsamości, co służy podwójnemu celowi ułatwienia kontroli tożsamości i zwalczania oszustw dotyczących tożsamości, ustanawia się po to, aby wspierać funkcjonowanie wspólnego repozytorium danych umożliwiających identyfikację i realizację celów systemów EES, VIS, ETIAS, Eurodac, SIS i ECRIS-TCN.

2. Detektor wielokrotnych tożsamości składa się z:

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

b) bezpiecznej infrastruktury łączności między detektorem wielokrotnych tożsamości a SIS i infrastrukturą centralną europejskiego portalu wyszukiwania i wspólnego repozytorium danych umożliwiających identyfikację.

3. Detektor wielokrotnych tożsamości opracowuje eu-LISA, która zarządza nim też od strony technicznej.

Artykuł 26

Dostęp do detektora wielokrotnych tożsamości

1. W celu ręcznej weryfikacji różniących się tożsamości, o której mowa w art. 29, dostęp do danych określonych w art. 34 przechowywanych w detektorze wielokrotnych tożsamości mają:

a) właściwe organy wyznaczone zgodnie z art. 9 ust. 2 rozporządzenia (UE) 2017/2226, podczas tworzenia lub aktualizacji akt osobowych w EES zgodnie z art. 14 tego rozporządzenia;

b) organy wizowe, o których mowa w art. 6 ust. 1 rozporządzenia (WE) nr 767/2008, podczas tworzenia lub aktualizacji akt osobowych w systemie VIS zgodnie z art. tym rozporządzeniem;

c) jednostka centralna ETIAS i jednostki krajowe ETIAS, podczas dokonywania przetwarzania, o którym mowa w art. 22 i 26 rozporządzenia (UE) 2018/1240;

d) biuro SIRENE państwa członkowskiego, które utworzyło lub uaktualniło wpis w SIS zgodnie z rozporządzeniami (UE) 2018/1860 i (UE) 2018/1861.

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

3. Organy państw członkowskich i agencje Unii mają dostęp do powiązań białych, o których mowa w art. 33, jeżeli mają dostęp do dwóch systemów informacyjnych UE zawierających dane, między którymi zostało utworzone powiązanie białe.

4. Organy państw członkowskich i agencje Unii mają dostęp do powiązań zielonych, o których mowa w art. 31, jeżeli mają dostęp do dwóch systemów informacyjnych UE zawierających dane, między którymi zostało utworzone powiązanie zielone, a zapytanie dokonane w tych systemach informacyjnych ujawniło dopasowanie z dwoma zestawami powiązanych ze sobą danych.

Artykuł 27

Wykrywanie wielokrotnych tożsamości

1. Proces wykrywania wielokrotnych tożsamości we wspólnym repozytorium danych umożliwiających identyfikację i SIS należy uruchomić w następujących sytuacjach:

a) tworzenie lub aktualizacja akt osobowych w EES zgodnie z art. 14 rozporządzenia (UE) 2017/2226;

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

c) tworzenie lub aktualizacja pliku danych dotyczących wniosku w systemie ETIAS zgodnie z art. 19 rozporządzenia (UE) 2018/1240;

d) tworzenie lub aktualizacja wpisu dotyczącego danej osoby w SIS zgodnie z art. 3 rozporządzenia (UE) 2018/1860 i rozdziałem V rozporządzenia (UE) 2018/1861;

2. Jeśli dane zawarte w systemie informacyjnym UE, o którym mowa w ust. 1, zawierają dane biometryczne, wspólne repozytorium danych umożliwiających identyfikację i system centralny SIS korzystają ze wspólnego systemu porównywania danych biometrycznych w celu wykrycia wielokrotnych tożsamości. Wspólny system porównywania danych biometrycznych porównuje wzorce biometryczne pochodzące z nowych danych biometrycznych z wzorcami biometrycznymi już znajdującymi się we wspólnym systemie porównywania danych biometrycznych, aby sprawdzić, czy dane należące do tej samej osoby już znajdują się we wspólnym repozytorium danych umożliwiających identyfikację i w systemie centralnym SIS.

3. Obok procesu, o którym mowa w ust. 2, wspólne repozytorium danych umożliwiających identyfikację i system centralny SIS korzystają z europejskiego portalu wyszukiwania, aby przeszukiwać dane przechowywane odpowiednio w systemie centralnym SIS i we wspólnym repozytorium danych umożliwiających identyfikację, posługując się następującymi danymi:

a) nazwisko; imię lub imiona; data urodzenia; obywatelstwo lub obywatelstwa; i płeć, o których mowa w art. 16 ust. 1 lit. a), art. 17 ust. 1 i art. 18 ust. 1 rozporządzenia (UE) 2017/2226;

b) nazwisko; imię lub imiona; data urodzenia; płeć; miejsce i państwo urodzenia; obywatelstwo lub obywatelstwa, o których mowa w art. 9 pkt 4 lit. a) i aa) rozporządzenia (WE) nr 767/2008;

c) nazwisko; imię (imiona); nazwisko nadane przy urodzeniu; pseudonim (pseudonimy), data urodzenia, miejsce urodzenia, płeć i obecne obywatelstwo, o których mowa w art. 17 ust. 2 rozporządzenia (UE) 2018/1240;

d) nazwiska; imiona; imiona i nazwiska nadane przy urodzeniu, poprzednio używane imiona i nazwiska oraz pseudonimy; miejsce urodzenia; data urodzenia; płeć i posiadane obywatelstwa, o których mowa w art. 20 ust. 2 rozporządzenia (UE) 2018/1861;

e) nazwiska; imiona; imiona i nazwiska nadane przy urodzeniu, poprzednio używane imiona i nazwiska oraz pseudonimy; miejsce urodzenia; data urodzenia, płeć i posiadane obywatelstwa, o których mowa w art. 4 rozporządzenia (UE) 2018/1860.

4. Obok procesu, o którym mowa w ust. 2 i 3, wspólne repozytorium danych umożliwiających identyfikację i system centralny SIS korzystają z europejskiego portalu wyszukiwania, aby przeszukiwać dane przechowywane odpowiednio w systemie centralnym SIS i we wspólnym repozytorium danych umożliwiających identyfikację, posługując się danymi dokumentu podróży.

5. Wykrywanie wielokrotnych tożsamości należy przeprowadzić wyłącznie w celu porównania danych dostępnych w jednym systemie informacyjnym UE z danymi dostępnymi w pozostałych systemach.

Artykuł 28

Wyniki wykrywania wielokrotnych tożsamości

1. Jeśli zapytania, o których mowa w art. 27 ust. 2, 3 i 4, nie wykażą żadnego dopasowania, procedury, o których mowa w art. 27 ust. 1, są prowadzone dalej zgodnie z regulującymi je aktami prawymi.

2. Jeśli zapytanie, o którym mowa w art. 27 ust. 2, 3 i 4, wykaże jedno lub kilka dopasowań, we wspólnym repozytorium danych umożliwiających identyfikację oraz, w stosownych przypadkach, w SIS tworzone jest powiązanie między danymi użytymi w zapytaniu a danymi, które doprowadziły do wystąpienia dopasowania.

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

3. Jeśli zapytanie, o którym mowa w art. 27 ust. 2, 3 i 4, wykaże jedno lub kilka dopasowań, a dane dotyczące tożsamości zawarte w powiązanych ze sobą aktach indywidualnych są tożsame lub zbliżone, tworzone jest powiązanie białe zgodnie z art. 33.

4. Jeśli zapytanie, o którym mowa w art. 27 ust. 2, 3 i 4, wykaże jedno lub kilka dopasowań, a danych dotyczących tożsamości zawartych w powiązanych ze sobą aktach indywidualnych nie można uznać za zbliżone, tworzy się powiązanie żółte zgodnie z art. 30; obowiązuje wówczas procedura, o której mowa w art. 29.

5. Komisja przyjmuje zgodnie z art. 73 akty delegowane ustanawiające procedury ustalania przypadków, w których dane dotyczące tożsamości można uznać za tożsame lub zbliżone.

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

7. Komisja, we współpracy z eu-LISA, określa za pomocą aktów wykonawczych zasady techniczne tworzenia powiązań między danymi z różnych systemów informacyjnych UE. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 29

Ręczna weryfikacja różniących się tożsamości i odpowiedzialne organy

1. Bez uszczerbku dla ust. 2, organem odpowiedzialnym za ręczną weryfikację różniących się tożsamości jest:

a) właściwy organ wyznaczony zgodnie z art. 9 ust. 2 rozporządzenia (UE) 2017/2226, w przypadku dopasowań, które wystąpiły przy tworzeniu lub aktualizacji akt osobowych w systemie EES zgodnie z tym rozporządzeniem;

b) organy wizowe, o których mowa w art. 6 ust. 1 rozporządzenia (WE) nr 767/2008, w przypadku dopasowań, które wystąpiły podczas tworzenia lub aktualizacji pliku danych dotyczących wniosku w systemie VIS zgodnie z tym rozporządzeniem;

c) jednostka centralna ETIAS i jednostki krajowe ETIAS w przypadku dopasowań, które wystąpiły podczas tworzenia lub aktualizacji pliku danych dotyczących wniosku zgodnie z rozporządzeniem (UE) 2018/1240;

d) biuro SIRENE państwa członkowskiego, w przypadku dopasowań, które wystąpiły podczas tworzenia lub aktualizacji wpisu w SIS zgodnie z rozporządzeniami (UE) 2018/1860 i (UE) 2018/1861.

Detektor wielokrotnych tożsamości wskazuje organ odpowiedzialny za ręczną weryfikację różniących się tożsamości w pliku potwierdzającym tożsamość.

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

a) dotyczącym osób poszukiwanych w celu aresztowania i wydania lub ekstradycji, o których mowa w art. 26 rozporządzenia (UE) 2018/1862;

b) dotyczącym osób zaginionych lub narażonych na zagrożenia, o których mowa w art. 32 rozporządzenia (UE) 2018/1862;

c) dotyczącym osób, których obecność jest wymagana do celów postępowania sądowego, o których mowa w art. 34 rozporządzenia (UE) 2018/1862;

d) dotyczącym osób, wobec których prowadzone są kontrole niejawne, rozpytania kontrolne lub kontrole szczególne, o których mowa w art. 36 rozporządzenia (UE) 2018/1862.

3. Bez uszczerbku dla ust. 4 niniejszego artykułu, organ odpowiedzialny za ręczną weryfikację różniących się tożsamości ma dostęp do powiązanych ze sobą danych zawartych w odpowiednich plikach potwierdzających tożsamość i w danych dotyczących tożsamości powiązanych we wspólnym repozytorium danych umożliwiających identyfikację oraz, w stosownych przypadkach, w SIS. Ocenia on niezwłocznie różniące się tożsamości. Po dokonaniu takiej oceny aktualizuje on powiązanie zgodnie z art. 31, 32 i 33, a także niezwłocznie dodaje je do pliku potwierdzającego tożsamość.

4. Jeśli organem odpowiedzialnym za ręczną weryfikację różniących tożsamości w pliku potwierdzającym tożsamość jest właściwy organ wyznaczony zgodnie z art. 9 ust. 2 rozporządzenia (UE) 2017/2226, który tworzy lub aktualizuje akta osobowe w EES zgodnie z art. 14 tego rozporządzenia, a także w razie utworzenia powiązania żółtego, organ ten przeprowadza dodatkowe weryfikacje. Organ ten ma jedynie w tym celu dostęp do powiązanych danych dotyczących tożsamości zawartych w odpowiednim pliku potwierdzającym tożsamość. Analizuje on różne tożsamości, aktualizuje powiązanie zgodnie z art. 31, 32 i 33 niniejszego rozporządzenia i niezwłocznie dodaje je do pliku potwierdzającego tożsamość.

Taką ręczną weryfikację różniących się tożsamości rozpoczyna się w obecności zainteresowanej osoby, której zapewnia się możliwość wyjaśnienia okoliczności organowi odpowiedzialnemu, który bierze te wyjaśnienia pod uwagę.

W przypadkach, w których ręczna weryfikacja różniących się tożsamości ma miejsce na granicy, odbywa się ona, w miarę możliwości, w ciągu 12 godzin od utworzenia powiązania żółtego zgodnie z art. 28 ust. 4.

5. W razie utworzenia więcej niż jednego powiązania organ odpowiedzialny za ręczną weryfikację różniących się tożsamości ocenia każde powiązanie oddzielnie.

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

Artykuł 30

Powiązanie żółte

1. Jeżeli nie przeprowadzono jeszcze ręcznej weryfikacji różniących się tożsamości, powiązanie między danymi z dwóch lub większej liczby systemów informacyjnych UE klasyfikuje się jako powiązanie żółte w każdym z poniższych przypadków:

a) powiązane ze sobą dane zawierają tożsame dane biometryczne, lecz zbliżone lub różne dane dotyczące tożsamości;

b) powiązane ze sobą dane zawierają różne dane dotyczące tożsamości, lecz tożsame dane dokumentu podróży, a co najmniej jeden z systemów informacyjnych UE nie zawiera danych biometrycznych danej osoby;

c) powiązane ze sobą dane zawierają tożsame dane dotyczące tożsamości, lecz różne dane biometryczne;

d) powiązane ze sobą dane zawierają zbliżone lub różniące się dane dotyczące tożsamości i tożsame dane dokumentu podróży, lecz różne dane biometryczne.

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

Artykuł 31

Powiązanie zielone

1. Powiązanie między danymi zawartymi w dwóch lub większej liczbie systemów informacyjnych UE klasyfikuje się jako zielone, jeśli:

a) powiązane ze sobą dane zawierają różne dane biometryczne, lecz tożsame dane dotyczące tożsamości, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdzi, że powiązane ze sobą dane odnoszą się do dwóch różnych osób;

b) powiązane ze sobą dane zawierają różne dane biometryczne, lecz zbliżone lub różne dane dotyczące tożsamości i tożsame dane dokumentu podróży, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdzi, że powiązane ze sobą dane odnoszą się do dwóch różnych osób;

c) powiązane ze sobą dane zawierają różne dane dotyczące tożsamości, lecz tożsame dane dokumentu podróży, co najmniej jeden z systemów informacyjnych UE nie zawiera danych biometrycznych na temat danej osoby, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdzi, że powiązane ze sobą dane odnoszą się do dwóch różnych osób.

2. Jeśli po przeszukaniu wspólnego repozytorium danych umożliwiających identyfikację lub SIS stwierdzone zostanie istnienie powiązania zielonego między danymi w dwóch systemach informacyjnych UE, detektor wielokrotnych tożsamości wskazuje, że dane dotyczące tożsamości stanowiące część powiązanych ze sobą danych nie należą do tej samej osoby.

3. W przypadku gdy organ państwa członkowskiego posiada dowody sugerujące, że powiązanie zielone zostało niepoprawnie zapisane w detektorze wielokrotnych tożsamości, że powiązanie zielone jest nieaktualne lub że dane zostały przetworzone w detektorze wielokrotnych tożsamości lub systemach informacyjnych UE z naruszeniem niniejszego rozporządzenia, organ ten sprawdza odpowiednie dane przechowywane we wspólnym repozytorium danych umożliwiających identyfikację i w SIS, a w razie konieczności niezwłocznie koryguje lub usuwa powiązanie z detektora wielokrotnych tożsamości. Organ państwa członkowskiego niezwłocznie informuje o tym państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości.

Artykuł 32

Powiązanie czerwone

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

a) powiązane ze sobą dane zawierają tożsame dane biometryczne, lecz zbliżone lub różne dane dotyczące tożsamości, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdził, że powiązane ze sobą dane w sposób nieuzasadniony odnoszą się do tej samej osoby;

b) powiązane ze sobą dane zawierają tożsame, zbliżone lub różne dane dotyczące tożsamości oraz tożsame dane dokumentu podróży, lecz różne dane biometryczne, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdził, że powiązane ze sobą dane odnoszą się one do dwóch różnych osób, z których przynajmniej jedna korzystają w sposób nieuzasadniony z tego samego dokumentu podróży;

c) powiązane ze sobą dane zawierają tożsame dane dotyczące tożsamości, lecz różne dane biometryczne i różne dane dokumentu podróży lub nie zawierają danych dokumentu podróży, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdził, że powiązane ze sobą dane w sposób nieuzasadniony odnoszą się do dwóch różnych osób;

d) powiązane ze sobą dane zawierają różne dane dotyczące tożsamości, lecz tożsame dane dokumentu podróży, co najmniej jeden z systemów informacyjnych UE nie zawiera danych biometrycznych na temat danej osoby, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdził, że powiązane ze sobą dane w sposób nieuzasadniony odnoszą się do tej samej osoby.

2. Jeśli w wyniku przeszukania wspólnego repozytorium danych umożliwiających identyfikację lub SIS stwierdzona zostanie obecność powiązania czerwonego między danymi w dwóch lub większej liczbie systemów informacyjnych UE, detektor wielokrotnych tożsamości wskazuje dane, o których mowa w art. 34. Działania następcze w związku z wystąpieniem powiązania czerwonego są prowadzone zgodnie z przepisami prawa Unii i prawa krajowego, przy czym konsekwencje prawne dla danej osoby opierają się jedynie na odpowiednich danych dotyczących tej osoby. Skutki prawne dla danej osoby nie mogą wynikać z samego zaistnienia powiązania czerwonego.

3. W razie utworzenia powiązania czerwonego między danymi z systemów EES, VIS, ETIAS, Eurodac lub ECRIS-TCN, akta osobowe przechowywane we wspólnym repozytorium danych umożliwiających identyfikację są aktualizowane zgodnie z art. 19 ust. 2.

4. Bez uszczerbku dla przepisów dotyczących rozpatrywania wpisów w SIS zawartych w rozporządzeniach (UE) 2018/1860, (UE) 2018/1861 i (UE) 2018/1862, oraz bez uszczerbku dla ograniczeń koniecznych do ochrony bezpieczeństwa i porządku publicznego, zapobiegania przestępstwom i zagwarantowania, aby żadne prowadzone krajowe postępowanie przygotowawcze nie było zagrożone, w razie utworzenia powiązania czerwonego organ odpowiedzialny za ręczną weryfikację różniących się tożsamości powiadamia osobę, której to dotyczy, o stwierdzeniu obecności niezgodnych z prawem różnych danych dotyczących tożsamości, a także przekazuje tej osobie pojedynczy numer identyfikacyjny, o którym mowa w art 34 lit. c) niniejszego rozporządzenia, odniesienie do organu odpowiedzialnego za ręczną weryfikację różniących się tożsamości, o którym mowa w art. 34 lit. d), oraz adres strony internetowej utworzonej zgodnie z art. 49 niniejszego rozporządzenia.

5. Informacje, o których mowa w ust. 4, są przekazywane na piśmie przy pomocy standardowego formularza przez organ odpowiedzialny za ręczną weryfikację różniących się tożsamości. Komisja określa treść formularza i jego format w drodze aktów wykonawczych. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

6. W razie utworzenia powiązania czerwonego detektor wielokrotnych tożsamości automatycznie powiadamia o tym organy odpowiedzialne za powiązane ze sobą dane.

7. W przypadku gdy organ państwa członkowskiego lub agencja unijna, które mają dostęp do wspólnego repozytorium danych umożliwiających identyfikację lub SIS, posiada dowody wykazujące, że powiązanie czerwone zostało nieprawidłowo zarejestrowane w detektorze wielokrotnych tożsamości lub że dane były przetwarzane w detektorze wielokrotnych tożsamości, wspólnym repozytorium danych umożliwiających identyfikację lub w SIS z naruszeniem niniejszego rozporządzenia, ten organ lub ta agencja sprawdzają odpowiednie dane przechowywane we wspólnym repozytorium danych i SIS oraz:

a) jeżeli powiązanie odnosi się do jednego z wpisów w SIS, o którym mowa w art. 29 ust. 2, natychmiast informuje o tym fakcie właściwe biuro SIRENE państwa członkowskiego, które utworzyło wpis w SIS;

b) we wszystkich innych przypadkach, natychmiast koryguje lub usuwa powiązanie z detektora wielokrotnych tożsamości.

Jeżeli biuro SIRENE zostaje poinformowane zgodnie z akapitem pierwszym lit. a) weryfikuje ono dowody dostarczone przez organ państwa członkowskiego lub agencję unijną, a następnie w odpowiednim przypadku niezwłocznie poprawia lub usuwa powiązanie z detektora wielokrotnych tożsamości;

Organ państwa członkowskiego, który uzyskał dowody, niezwłocznie informuje organ państwa członkowskiego odpowiedzialny za ręczną weryfikację różniących się tożsamości o stosownej korekcie lub usunięciu powiązania czerwonego.

Artykuł 33

Powiązanie białe

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

a) powiązane ze sobą dane zawierają tożsame dane biometryczne i tożsame lub zbliżone dane dotyczące tożsamości;

b) powiązane ze sobą dane zawierają tożsame lub zbliżone dane dotyczące tożsamości, tożsame dane dokumentu podróży, a co najmniej jeden z systemów informacyjnych UE nie zawiera danych biometrycznych danej osoby;

c) powiązane ze sobą dane zawierają tożsame dane biometryczne, tożsame dane dokumentu podróży i zbliżone dane dotyczące tożsamości;

d) powiązane ze sobą dane zawierają tożsame dane biometryczne, lecz zbliżone lub różne dane dotyczące tożsamości, a organ odpowiedzialny za ręczną weryfikację różniących się tożsamości stwierdził, że powiązane ze sobą dane w sposób uzasadniony odnoszą się do tej samej osoby;

2. Jeśli po przeszukaniu wspólnego repozytorium danych umożliwiających identyfikację lub SIS stwierdzone zostanie istnienie powiązania białego między danymi w co najmniej dwóch systemach informacyjnych UE, detektor wielokrotnych tożsamości wskazuje, że dane dotyczące tożsamości należą do tej samej osoby. Wynikiem przeszukiwania systemów informacyjnych UE jest odpowiedź, która w stosownych przypadkach wskazuje wszystkie powiązane ze sobą dane dotyczące danej osoby, co powoduje powstanie dopasowania w stosunku do danych objętych powiązaniem białym, jeśli organ, który dokonał zapytania, ma dostęp do tych powiązanych ze sobą danych na mocy przepisów prawa Unii lub prawa krajowego.

3. W razie utworzenia powiązania czerwonego między danymi z systemów EES, VIS, ETIAS, Eurodac lub ECRIS-TCN, akta osobowe przechowywane we wspólnym repozytorium danych umożliwiających identyfikację są aktualizowane zgodnie z art. 19 ust. 2.

4. Bez uszczerbku dla przepisów związanych z rozpatrywaniem wpisów w SIS zawartych w rozporządzeniach (UE) 2018/1860, (UE) 2018/1861 i (UE) 2018/1862, oraz bez uszczerbku dla ograniczeń koniecznych do ochrony bezpieczeństwa i porządku publicznego, zapobiegania przestępstwom i zagwarantowania, aby żadne prowadzone krajowe postępowanie przygotowawcze nie było zagrożone, w razie utworzenia powiązania białego w wyniku ręcznej weryfikacji różniących się tożsamości, organ odpowiedzialny za ręczną weryfikację różniących się tożsamości powiadamia osobę, której to dotyczy, o stwierdzeniu zbliżonych lub różnych danych dotyczących tożsamości oraz przekazuje tej osobie pojedynczy numer identyfikacyjny, o którym mowa w art 34 lit. c) niniejszego rozporządzenia, odniesienie do organu odpowiedzialnego za ręczną weryfikację różniących się tożsamości, o którym mowa w art. 34 lit. d) niniejszego rozporządzenia, oraz adres strony internetowej utworzonej zgodnie z art. 49 niniejszego rozporządzenia.

5. W przypadku gdy organ państwa członkowskiego posiada dowody wskazujące, że powiązanie białe zostało niepoprawnie zarejestrowane w detektorze wielokrotnych tożsamości, że powiązanie białe jest nieaktualne lub że dane zostały przetworzone w detektorze wielokrotnych tożsamości lub w systemach informacyjnych UE z naruszeniem niniejszego rozporządzenia, organ ten sprawdza odpowiednie dane przechowywane we wspólnym repozytorium danych umożliwiających identyfikację i w SIS, i w razie konieczności niezwłocznie koryguje lub usuwa powiązanie detektora wielokrotnych tożsamości. Ten organ państwa członkowskiego niezwłocznie informuje o tym państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości.

6. Informacje, o których mowa w ust. 4, są przekazywane na piśmie przy pomocy standardowego formularza przez organ odpowiedzialny za ręczną weryfikację różniących się tożsamości. Komisja określa treść formularza i jego format w drodze aktów wykonawczych. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 34

Plik potwierdzający tożsamość

Plik potwierdzający tożsamość zawiera następujące dane:

a) powiązania, o których mowa w art. 30–33;

b) odniesienie do systemów informacyjnych UE, w których są przechowywane powiązane ze sobą dane;

c) pojedynczy numer identyfikacyjny umożliwiający pobranie powiązanych ze sobą danych z odpowiednich systemów informacyjnych UE;

d) organ odpowiedzialny za ręczną weryfikację różniących się tożsamości;

e) datę utworzenia powiązania lub wszelkich jego aktualizacji.

Artykuł 35

Zatrzymywanie danych w detektorze wielokrotnych tożsamości

Pliki potwierdzające tożsamość i zawarte w nich dane, w tym powiązania, są przechowywane w detektorze wielokrotnych tożsamości tylko tak długo, jak długo powiązane ze sobą dane są przechowywane w dwóch lub większej liczbie systemów informacyjnych UE. Są one automatycznie usuwane z detektora wielokrotnych tożsamości.

Artykuł 36

Prowadzenie rejestrów

1. eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w detektorze wielokrotnych tożsamości. Rejestry te obejmują:

a) państwo członkowskie dokonujące zapytania;

b) cel dostępu użytkownika;

c) datę i godzinę zapytania;

d) rodzaj danych użytych w zapytaniu;

e) odniesienie do powiązanych ze sobą danych;

f) historię pliku potwierdzającego tożsamość.

2. Każde państwo członkowskie prowadzi rejestry zapytań dokonywanych przez jego organy i personel tych organów należycie upoważniony do korzystania z detektora wielokrotnych tożsamości. Każda agencja unijna prowadzi rejestry zapytań dokonywanych przez jej należycie upoważniony personel.

3. Rejestry, o których mowa w ust. 1 i 2, można wykorzystywać wyłącznie w celu monitorowania ochrony danych, w tym sprawdzania dopuszczalności zapytania i zgodności przetwarzania danych z prawem, oraz w celu zapewniania bezpieczeństwa i integralności danych. Rejestry te są chronione przed nieuprawnionym dostępem za pomocą odpowiednich środków i usuwane rok po utworzeniu. Jeżeli jednak są one konieczne do prowadzenia już rozpoczętych procedur monitorowania, są one usuwane, gdy tylko przestają być konieczne do celu tych procedur.

ROZDZIAŁ VI

Środki wspierające interoperacyjność

Artykuł 37

Jakość danych

1. Bez uszczerbku dla obowiązków państw członkowskich w odniesieniu do jakości danych wprowadzonych do systemów eu-LISA ustanawia automatyczne mechanizmy kontroli jakości danych i procedury dotyczące danych przechowywanych w systemach EES, VIS, ETIAS, SIS, wspólnym systemie porównywania danych biometrycznych i wspólnym repozytorium danych umożliwiających identyfikację.

2. eu-LISA wdraża mechanizmy oceny dokładności wspólnego systemu porównywania danych biometrycznych, wspólne wskaźniki jakości danych i minimalne normy jakości przechowywania danych w systemach EES, VIS, ETIAS, SIS, wspólnym systemie porównywania danych biometrycznych i wspólnym repozytorium danych umożliwiających identyfikację.

Tylko dane spełniające minimalne normy jakości mogą być wprowadzane do systemów EES, VIS, ETIAS, SIS, wspólnego systemu porównywania danych biometrycznych, wspólnego repozytorium danych umożliwiających identyfikację i detektora wielokrotnych tożsamości.

3. eu-LISA regularnie przedstawia państwom członkowskim sprawozdania z mechanizmów i procedur automatycznej kontroli jakości danych oraz wspólnych wskaźników jakości danych. eu-LISA regularnie przedstawia też Komisji sprawozdania ze zidentyfikowanych problemów i tego, których państw członkowskich dotyczą. eu-LISA przedstawia to sprawozdanie na żądanie także Parlamentowi Europejskiemu i Radzie. Żadne sprawozdania, o których mowa w niniejszym ustępie, nie zawierają danych osobowych.

4. Szczegóły tych mechanizmów i procedur automatycznej kontroli jakości danych, wspólnych wskaźników jakości danych oraz minimalnych norm jakości przechowywania danych w systemach EES, VIS, ETIAS, SIS, wspólnym systemie porównywania danych biometrycznych i wspólnym repozytorium danych umożliwiających identyfikację, zwłaszcza w odniesieniu do danych biometrycznych, określają akty wykonawcze. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

5. Jeden rok po ustanowieniu mechanizmów i procedur automatycznej kontroli jakości danych, wspólnych wskaźników jakości danych i minimalnych standardów jakości danych oraz co roku od tej daty Komisja ocenia wdrożenie jakości danych w państwach członkowskich i sporządza odpowiednie zalecenia. Państwa członkowskie przedstawiają Komisji plan działania mający na celu rozwiązanie problemów zidentyfikowanych w sprawozdaniu oceniającym, a w szczególności kwestii jakości danych wynikających z błędnych danych w systemach informacyjnych UE. Państwa członkowskie regularnie składają Komisji sprawozdania z postępów w realizacji tego planu działania do czasu jego pełnego wdrożenia.

Komisja przekazuje powyższe sprawozdanie oceniające Parlamentowi Europejskiemu, Radzie, Europejskiemu Inspektorowi Danych Osobowych, Europejskiej Radzie Ochrony Danych i Agencji Praw Podstawowych Unii Europejskiej ustanowionej na mocy rozporządzenia Rady (WE) nr 168/2007 ([39]).

Artykuł 38

Uniwersalny format wiadomości

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

2. Standard UMF jest stosowany przy opracowywaniu systemów EES, ETIAS, europejskiego portalu wyszukiwania, wspólnego repozytorium danych umożliwiających identyfikację, detektora wielokrotnych tożsamości, jeśli to możliwe, oraz, w stosownych przypadkach, przy opracowywaniu przez eu-LISA lub inną agencję Unii nowych modeli wymiany informacji i systemów informacyjnych w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych.

3. Komisja przyjmuje akt wykonawczy, aby określić i rozwijać standard UMF, o którym mowa w ust. 1 niniejszego ustępu. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 39

Centralne repozytorium sprawozdawczo-statystyczne

1. Centralne repozytorium sprawozdawczo-statystyczne ustanawia się, aby wspierać realizację celów systemów EES, VIS, ETIAS i SIS zgodnie z odpowiednimi aktami prawnymi regulującymi te systemy oraz zapewniać międzysystemowe dane statystyczne i sprawozdania analityczne służące strategiom politycznym, celom operacyjnym i związanym z jakością danych.

2. eu-LISA ustanawia, wdraża i obsługuje centralne repozytorium sprawozdawczo-statystyczne w swoich centrach technicznych zawierających dane i statystyki, o których mowa w art. 63 rozporządzenia (UE) 2017/2226, art. 17 rozporządzenia (WE) nr 767/2008, art. 84 rozporządzenia (UE) 2018/1240, art. 60 rozporządzenia (UE) 2018/1861 oraz art. 16 rozporządzenia (UE) 2018/1860, logicznie oddzielone według systemu informacyjnego UE. Dostęp do centralnego repozytorium sprawozdawczo-statystycznego w postaci kontrolowanego, bezpiecznego dostępu i określonych profili użytkowników przyznaje się – wyłącznie w celach sprawozdawczo-statystycznych – organom, o których mowa w art. 63 rozporządzenia (UE) 2017/2226, art. 17 rozporządzenia (WE) nr 767/2008, art. 84 rozporządzenia (UE) 2018/1240 i art. 60 rozporządzenia (UE) 2018/1861.

3. eu-LISA poddaje dane anonimizacji i rejestruje takie zanonimizowane dane w repozytorium. Proces anonimizacji danych odbywa się automatycznie.

Dane zawarte w centralnym repozytorium sprawozdawczo-statystycznym nie umożliwiają identyfikacji osób fizycznych.

4. Centralne repozytorium sprawozdawczo-statystyczne składa się z:

a) narzędzi niezbędnych do anonimizacji danych;

b) infrastruktury centralnej, obejmującej repozytorium danych z anonimowymi danymi;

c) bezpiecznej infrastruktury łączności między repozytorium a systemami EES, VIS, ETIAS i SIS oraz infrastrukturą centralną wspólnego systemu porównywania danych biometrycznych, wspólnego repozytorium danych umożliwiających identyfikację i detektora wielokrotnych tożsamości.

5. Komisja przyjmuje zgodnie z art. 73 akt delegowany określający szczegółowe zasady działania centralnego repozytorium sprawozdawczo-statystycznego, w tym szczegółowe zabezpieczenia dotyczące przetwarzania danych osobowych na mocy ust. 2 i 3 niniejszego artykułu, oraz zasady bezpieczeństwa obowiązujące w stosunku do repozytorium.

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

ROZDZIAŁ VII

Ochrona danych

Artykuł 40

Administrator danych

1. W stosunku do przetwarzania danych za pośrednictwem wspólnego systemu porównywania danych biometrycznych organy państw członkowskich będące administratorami danych w odniesieniu do, odpowiednio, systemów EES, VIS i SIS są administratorami zgodnie z art.4 pkt 7 rozporządzenia (UE) 2016/679 lub art. 3 pkt 8 dyrektywy (UE) 2016/680 w stosunku do wzorców biometrycznych uzyskanych na podstawie danych, o których mowa w art.13 niniejszego rozporządzenia, które wprowadzają do odpowiednich systemów, oraz odpowiadają za przetwarzanie wzorców biometrycznych we wspólnym systemie porównywania danych biometrycznych.

2. W stosunku do przetwarzania danych za pośrednictwem wspólnego repozytorium danych umożliwiających identyfikację organy państw członkowskich będące administratorami danych w odniesieniu do, odpowiednio, systemów EES, VIS i ETIAS są administratorami zgodnie z art. 4 pkt 7 rozporządzenia (UE) 2016/679 w stosunku do danych, o których mowa w art. 18 niniejszego rozporządzenia, które wprowadzają do odpowiednich systemów, oraz odpowiadają za przetwarzanie danych osobowych we wspólnym repozytorium danych umożliwiających identyfikację.

3. W stosunku do przetwarzania danych za pośrednictwem detektora wielokrotnych tożsamości:

a) Europejska Agencja Straży Granicznej i Przybrzeżnej jest administratorem danych w rozumieniu art. 3 pkt 8 rozporządzenia (UE) 2018/1725 w związku z przetwarzaniem danych osobowych przez jednostkę centralną ETIAS.

b) organy państw członkowskich, które dodają lub modyfikują dane w pliku potwierdzającym tożsamość, także są administratorami danych zgodnie z art. 4 pkt 7 rozporządzenia (UE) 2016/679 lub art. 3 pkt 8 dyrektywy (UE) 2016/680 i odpowiadają za przetwarzanie danych osobowych w detektorze wielokrotnych tożsamości.

4. Na potrzeby monitorowania ochrony danych, w tym sprawdzania dopuszczalności zapytania oraz zgodności przetwarzania danych z prawem, administratorzy danych mają dostęp do rejestrów, o których mowa w art. 10, 16, 24 i 36, w celu monitorowania własnej działalności, o którym mowa w art. 44.

Artykuł 41

Przetwarzający dane

W przypadku przetwarzania danych osobowych we wspólnym systemie porównywania danych biometrycznych, wspólnym repozytorium danych umożliwiających identyfikację i detektorze wielokrotnych tożsamości eu-LISA jest przetwarzającymi dane w rozumieniu art. 3 pkt 12 lit. a) rozporządzenia (UE) 2018/1725.

Artykuł 42

Bezpieczeństwo przetwarzania danych

1. eu-LISA, jednostka centralna ETIAS, Europol i organy państw członkowskich zapewniają bezpieczeństwo przetwarzania danych osobowych odbywającego się na mocy niniejszego rozporządzenia. eu-LISA, jednostka centralna ETIAS, Europol i organy państw członkowskich współpracują w zakresie realizacji zadań związanych z bezpieczeństwem.

2. Bez uszczerbku dla art. 33 rozporządzenia (UE) 2018/1725 eu-LISA podejmuje konieczne środki, aby zapewnić bezpieczeństwo elementów interoperacyjności i związanej z nimi infrastruktury łączności.

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

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

b) odmowy dostępu osobom nieuprawnionym do sprzętu do przetwarzania danych i do obiektów;

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

d) zapobiegania nieuprawnionemu wprowadzaniu danych i nieuprawnionej inspekcji, zmianie i nieuprawnionemu usuwaniu zarejestrowanych danych osobowych;

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

f) uniemożliwienia wykorzystywania systemów zautomatyzowanego przetwarzania danych przez nieuprawnione osoby korzystające ze sprzętu do przekazywania danych;

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

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

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

j) uniemożliwienia nieuprawnionego odczytu, kopiowania, modyfikowania lub usuwania danych osobowych w trakcie przekazywania danych osobowych do lub z elementów interoperacyjności lub podczas transportu nośników danych, w szczególności za pomocą odpowiednich technik szyfrowania;

k) zapewnienia, by w przypadku przerwy w działaniu zainstalowane systemy można było przywrócić do normalnego funkcjonowania;

l) zapewnienia niezawodności dzięki zapewnieniu właściwego zgłaszanie błędów w funkcjonowaniu elementów interoperacyjności;

m) monitorowania skuteczności środków bezpieczeństwa, o których mowa w niniejszym ustępie, a także podejmowania niezbędnych środków organizacyjnych w obszarze kontroli wewnętrznej, aby zapewnić zgodność z niniejszym rozporządzeniem i ocenić te środki bezpieczeństwa w świetle rozwoju nowych technologii.

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

Artykuł 43

Incydenty bezpieczeństwa

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

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

3. Niezależnie od zgłaszania i zawiadamiania w odniesieniu do naruszenia ochrony danych osobowych zgodnie z art. 33 rozporządzenia (UE) 2016/679 lub art. 30 dyrektywy (UE) 2016/680 lub obu z nich państwa członkowskie niezwłocznie powiadamiają o incydentach bezpieczeństwa Komisję, eu-LISA, właściwe organy nadzorcze i Europejskiego Inspektora Ochrony Danych.

Bez uszczerbku dla art. 34 i 35 rozporządzenia (UE) 2018/1725 i art. 34 rozporządzenia (UE) 2016/794 jednostka centralna ETIAS i Europol niezwłocznie powiadamiają o incydentach bezpieczeństwa Komisję, eu-LISA i Europejskiego Inspektora Ochrony Danych.

W przypadku incydentu bezpieczeństwa związanego z infrastrukturą elementów interoperacyjności eu-LISA niezwłocznie powiadamia Komisję i Europejskiego Inspektora Ochrony Danych.

4. Informacja o incydencie bezpieczeństwa, który ma lub może mieć wpływ na funkcjonowanie elementów interoperacyjności lub na dostępność, integralność i poufność danych, zostaje niezwłocznie przekazana państwom członkowskim, jednostce centralnej ETIAS oraz Europolowi i zgłoszona zgodnie z zapewnionym przez eu-LISA planem zarządzania na wypadek incydentów bezpieczeństwa.

5. W przypadku incydentu bezpieczeństwa zainteresowane państwa członkowskie, jednostka centralna ETIAS, Europol i eu-LISA współpracują ze sobą. Komisja określa specyfikację tej procedury współpracy za pomocą aktów wykonawczych. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 44

Monitorowanie własnej działalności

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

Administratorzy danych, o których mowa w art. 40, podejmują konieczne środki, aby monitorować zgodność przetwarzania danych z niniejszym rozporządzeniem, w tym poprzez częstą weryfikację zapisów w rejestrach, o których mowa w art. 10, 16, 24 i 36, oraz w razie potrzeby współpracę z organami nadzorczymi oraz z Europejskim Inspektorem Ochrony Danych.

Artykuł 45

Kary

Państwa członkowskie dopilnowują, by wykorzystanie danych niezgodnie z przeznaczeniem, przetwarzanie danych lub wymiana danych niezgodnie z niniejszym rozporządzeniem podlegało karze zgodnie z prawem krajowym. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.

Artykuł 46

Odpowiedzialność

1. Bez uszczerbku dla prawa do odszkodowania od administratora lub podmiotu przetwarzającego i odpowiedzialności tych podmiotów na mocy rozporządzenia (UE) 2016/679, dyrektywy (UE) 2016/680 i rozporządzenia (WE) 2018/1725:

a) osoba lub państwo członkowskie, które poniosły materialną lub niematerialną szkodę w wyniku niezgodnej z prawem operacji przetwarzania danych osobowych lub innego działania niezgodnego z niniejszym rozporządzeniem przeprowadzonych przez państwo członkowskie, są uprawnione do otrzymania odszkodowania od tego państwa członkowskiego;

b) osoba lub państwo członkowskie, które poniosły szkodę majątkową lub niemajątkową w wyniku działania niezgodnego z niniejszym rozporządzeniem ze strony Europolu, Europejskiej Agencji Straży Granicznej i Przybrzeżnej lub eu-Lisa, są uprawnione do otrzymania odszkodowania od danej agencji.

Dane państwo członkowskie, Europol, Europejska Agencja Straży Granicznej i Przybrzeżnej lub eu-Lisa są zwolnione z odpowiedzialności na mocy akapitu pierwszego, w całości lub w części, jeżeli udowodnią, że nie ponoszą odpowiedzialności za zdarzenie, które spowodowało szkodę.

2. Jeżeli niewypełnienie przez państwo członkowskie obowiązków spoczywających na nim zgodnie z niniejszym rozporządzeniem spowoduje wyrządzenie szkody elementom interoperacyjności, wówczas państwo to ponosi odpowiedzialność za tę szkodę, chyba że – i w zakresie, w jakim – eu-LISA lub inne państwo członkowskie związane niniejszym rozporządzeniem nie podjęły uzasadnionych środków zapobiegających wystąpieniu takiej szkody lub ograniczających jej skutki.

3. Roszczenia odszkodowawcze wobec państwa członkowskiego za szkody, o których mowa w ust. 1 i 2, są regulowane prawem krajowym pozwanego państwa członkowskiego. Roszczenia odszkodowawcze wnoszone przeciwko administratorowi lub eu-LISA z tytułu szkody, o której mowa w ust. 1 i 2, podlegają warunkom przewidzianym z Traktatach.

Artykuł 47

Prawo do informacji

1. Organ gromadzący dane osobowe, które mają być przechowywane we wspólnym systemie porównywania danych biometrycznych, we wspólnym repozytorium danych umożliwiających identyfikację lub w detektorze wielokrotnych tożsamości, przekazuje osobom, których dane są gromadzone, informacje wymagane zgodnie z art. 13 i 14 rozporządzenia (UE) 2016/679, art. 12 i 13 dyrektywy (UE) 2016/680 oraz art. 15 i 16 rozporządzenia (UE) 2018/1725. Organ ten przekazuje informacje w momencie pobierania takich danych.

2. Wszystkie informacje są udostępniane, przy użyciu jasnego i prostego języka, w wersji językowej, którą dana osoba rozumie lub co do której można zasadnie oczekiwać, że jest dla niej zrozumiała. Obejmuje to przekazywanie informacji w sposób odpowiedni dla wieku w przypadku osób małoletnich, których dotyczą dane.

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

a) tworzenie lub aktualizacja akt osobowych w EES zgodnie z art. 14 rozporządzenia (UE) 2017/2226;

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

c) tworzenie lub aktualizacja pliku danych dotyczących wniosku w systemie ETIAS zgodnie z art. 19 rozporządzenia (UE) 2018/1240.

Artykuł 48

Prawo do dostępu do danych osobowych przechowywanych w detektorze wielokrotnych tożsamości oraz żądania ich sprostowania i usunięcia oraz ograniczenia ich przetwarzania

1. W celu wykonywania swoich praw na mocy art. 15-8 rozporządzenia (UE) 2016/679, art. 17- 20 rozporządzenia (UE) 2018/1725 oraz art. 14, 15 i 16 dyrektywy (UE) 2016/680 każda osoba ma prawo zwrócić się do właściwego organu dowolnego państwa członkowskiego, a organ ten bada jej wniosek i odpowiada na niego.

2. Państwo członkowskie, które rozpatruje taki wniosek, udziela odpowiedzi bez zbędnej zwłoki, a w każdym razie w ciągu 45 dni od otrzymania wniosku. W razie potrzeby termin ten można przedłużyć o kolejnych 15 dni z uwagi na skomplikowany charakter wniosku lub liczbę wniosków. Państwo członkowskie, które rozpatruje taki wniosek, w ciągu 45 dni od otrzymania wniosku informuje osobę, której dane dotyczą, o takim przedłużeniu terminu z podaniem przyczyn opóźnienia. Państwa członkowskie mogą zdecydować, że odpowiedzi te mają być przekazywane przez jednostki centralne.

3. Jeżeli wniosek o sprostowanie lub usunięcie danych osobowych skierowano do państwa członkowskiego innego niż państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości, wówczas państwo członkowskie, do którego skierowano wniosek, w ciągu siedmiu dni kontaktuje się z organami państwa członkowskiego odpowiedzialnymi za ręczną weryfikację różniących się tożsamości. Państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości sprawdza poprawność danych i zgodność ich przetwarzania z prawem bez zbędnej zwłoki, a w każdym razie w ciągu 30 dni od nawiązania takiego kontaktu. W razie potrzeby termin ten można przedłużyć o kolejnych 15 dni z uwagi na skomplikowany charakter wniosku lub liczbę wniosków. Państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości informuje państwo członkowskie, które skontaktowało się z nim o wszelkich takich przedłużeniach terminu podając powody opóźnienia. Państwo członkowskie, które skontaktowało się z organem państwa członkowskiego odpowiedzialnym za ręczną weryfikację różniących się tożsamości, informuje zainteresowaną osobę o dalszej procedurze.

4. Jeżeli wniosek o sprostowanie lub usunięcie danych osobowych skierowano do państwa członkowskiego, w przypadku gdy za ręczną weryfikację różniących się tożsamości odpowiadała jednostka centralna ETIAS, wówczas państwo członkowskie, do którego skierowano wniosek, zwraca się w ciągu siedmiu dni do jednostki centralnej ETIAS o wydanie opinii bez zbędnej zwłoki, a w każdym razie w ciągu 30 dni od takiego kontaktu. W razie potrzeby termin ten można przedłużyć o kolejnych 15 dni z uwagi na skomplikowany charakter wniosku lub liczbę wniosków. Państwo członkowskie, które skontaktowało się z jednostką centralną ETIAS, powiadamia zainteresowaną osobę o dalszej procedurze.

5. W przypadku stwierdzenia, że dane zarejestrowane w detektorze wielokrotnych tożsamości są nieprawidłowe lub zostały zarejestrowane niezgodnie z prawem, państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości lub, w przypadkach gdy nie było państwa członkowskiego odpowiedzialnego za weryfikację ręczną lub gdy za ręczną weryfikację różniących się tożsamości odpowiadała jednostka centralna ETIAS, państwo członkowskie, do którego skierowano wniosek, koryguje lub usuwa te dane bez zbędnej zwłoki. Osoba zainteresowana jest informowana na piśmie o tym, że jej dane zostały poprawione lub usunięte.

6. W przypadku gdy państwo członkowskie sprostuje dane przechowywane w detektorze wielokrotnych tożsamości w okresie ich przechowywania, państwo to dokonuje przetwarzania określonego w art. 27 oraz, w stosownych przypadkach, w art. 29, aby ustalić, czy zmienione dane mają być ze sobą powiązane. Jeśli przetwarzanie nie doprowadzi do żadnego dopasowania, dane państwo członkowskie usuwa dane z pliku potwierdzającego tożsamość. Jeśli przetwarzanie automatyczne doprowadzi do wystąpienia jednego dopasowania lub kilku dopasowań, dane państwo członkowskie tworzy lub aktualizuje powiązanie między danymi zgodnie z odpowiednimi przepisami niniejszego rozporządzenia.

7. Jeżeli państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości lub, w stosownych przypadkach, państwo członkowskie, do którego skierowano wniosek, nie zgadza się z argumentem, że dane zarejestrowane w detektorze wielokrotnych tożsamości są nieprawidłowe lub że zostały zarejestrowane niezgodnie z prawem, wówczas to państwo członkowskie wydaje decyzję administracyjną, w której niezwłocznie wyjaśnia na piśmie osobie zainteresowanej, dlaczego nie jest gotowe sprostować lub usunąć dotyczących jej danych osobowych.

8. Decyzja, o której mowa w ust. 7, zawiera też informacje dla osoby zainteresowanej wyjaśniające możliwość odwołania się od decyzji podjętej w odniesieniu do wniosku o dostęp do danych osobowych, sprostowanie lub usunięcie danych osobowych lub ograniczenie ich przetwarzania, a w stosownych przypadkach informacje dotyczące sposobu wniesienia sprawy lub skargi do właściwych organów lub sądów oraz informacje dotyczące pomocy, w tym ze strony organów nadzorczych.

9. Wnioski o dostęp do danych osobowych, sprostowanie lub usunięcie danych osobowych lub ograniczenie ich przetwarzania zawierają informacje niezbędne do zidentyfikowania osoby zainteresowanej. Informacje te wykorzystuje się wyłącznie w celu zapewnienia możliwości wykonywania praw, o których mowa w niniejszym artykule, po czym natychmiast się je usuwa.

10. Państwo członkowskie odpowiedzialne za ręczną weryfikację różniących się tożsamości lub, w stosownych przypadkach, państwo członkowskie, do którego skierowano wniosek, prowadzi pisemny rejestr złożonych wniosków o udostępnienie, sprostowanie lub usunięcie danych osobowych lub ograniczenie ich przetwarzania, oraz sposób jego rozpatrzenia, a następnie niezwłocznie udostępniają ten rejestr organom nadzorczym.

11. Niniejszy artykuł pozostaje bez uszczerbku dla ograniczeń praw określonych w niniejszym artykule na mocy rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680.

Artykuł 49

Portal internetowy

1. Portal internetowy tworzy się w celu ułatwienia korzystania z praw dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania.

2. Portal internetowy zawiera informacje na temat praw i procedur, o których mowa w art. 47 i 48, oraz interfejs użytkownika umożliwiający osobom, których dane są przetwarzane w detektorze wielokrotnych tożsamości i które zostały poinformowane o wykazaniu połączenia czerwonego zgodnie z art. 32 ust. 4, uzyskanie danych kontaktowych właściwego organu państwa członkowskiego odpowiedzialnego za ręczną weryfikację różniących się tożsamości.

3. W celu uzyskania danych kontaktowych właściwego organu państwa członkowskiego odpowiedzialnego za ręczną weryfikację różniących się tożsamości osoba, której dane są przetwarzane w detektorze wielokrotnych tożsamości, powinna wprowadzić odniesienie do organu odpowiedzialnego za ręczną weryfikację różniących się tożsamości, o których mowa w art. 34 lit. d). Portal internetowy wykorzystuje to odniesienie do wyszukania danych kontaktowych właściwego organu państwa członkowskiego odpowiedzialnego za ręczną weryfikację różniących się tożsamości. Portal internetowy zawiera także wzór wiadomości elektronicznej w celu ułatwienia komunikacji między użytkownikiem portalu a właściwym organem państwa członkowskiego odpowiedzialnym za ręczną weryfikację różniących się tożsamości. Taka wiadomość elektroniczna zawiera pole dla pojedynczego numeru identyfikacyjnego, o którym mowa w art. 34 lit. c), aby umożliwić właściwemu organowi państwa członkowskiego odpowiedzialnego za ręczną weryfikację różniących się tożsamości identyfikację określonych danych.

4. Państwa członkowskie przekazują eu-LISA dane kontaktowe wszystkich organów, które są właściwe do rozpatrywania i odpowiadania na wnioski, o których mowa w art. 47 i 48, oraz dokonują regularnych przeglądów w celu ustalenia, czy te dane kontaktowe są aktualne.

5. eu-LISA rozwija portal internetowy i zarządza nim od strony technicznej.

6. Komisja przyjmuje akt delegowany zgodnie z art. 73 w celu określenia szczegółowych przepisów dotyczących funkcjonowania portalu internetowego, w tym interfejsu użytkownika, języków, w których portal internetowy jest dostępny, oraz wzoru wiadomości elektronicznej.

Artykuł 50

Przekazywanie danych osobowych państwom trzecim, organizacjom międzynarodowym i podmiotom prywatnym

Bez uszczerbku dla art. 65 rozporządzenia (UE) 2018/1240, art. 25 i 26 rozporządzenia (UE) 2016/794, art. 41 rozporządzenia (UE) 2017/2226, art. 31 rozporządzenia (WE) nr 767/2008 oraz przeszukiwania baz danych Interpolu za pomocą europejskiego portalu wyszukiwania zgodnie z art. 9 ust. 5 niniejszego rozporządzenia, które są zgodne z przepisami rozdziału V rozporządzenia (UE) 2018/1725 i rozdziału V rozporządzenia (UE) 2016/679, dane osobowe przechowywane lub udostępniane za pomocą elementów interoperacyjności nie są przekazywane ani udostępniane państwom trzecim, organizacjom międzynarodowym ani podmiotom prywatnym.

Artykuł 51

Nadzór ze strony organów nadzorczych

1. Każde państwo członkowskie zapewnia, by organy nadzorcze monitorowały w sposób niezależny, czy przetwarzanie danych osobowych na mocy niniejszego rozporządzenia przez dane państwo członkowskie – w tym przekazywanie takich danych do i z elementów interoperacyjności – jest zgodne z prawem.

2. Każde państwo członkowskie zapewnia stosowanie krajowych przepisów ustawowych, wykonawczych i administracyjnych przyjętych na mocy dyrektywy (UE) 2016/680 również, w stosownych przypadkach, w kwestiach związanych z dostępem do elementów interoperacyjności przez organy policji i wyznaczone organy, w tym w odniesieniu do praw osób, których danych dostęp ten dotyczy.

3. Organy nadzorcze zapewniają przeprowadzenie co najmniej raz na cztery lata kontroli operacji przetwarzania danych przez właściwe organy krajowe w celach związanych z niniejszym rozporządzeniem zgodnie z odpowiednimi międzynarodowymi standardami kontroli.

Organy nadzorcze publikują co roku informacje na temat liczby wniosków o sprostowanie, usunięcie lub ograniczenie przetwarzania danych, działań podjętych w odpowiedzi na wnioski i liczby sprostowań, usunięć i ograniczeń przetwarzania dokonanych w odpowiedzi na wnioski zainteresowanych osób.

4. Państwa członkowskie zapewniają, aby ich organy nadzorcze dysponowały zasobami i wiedzą fachową wystarczającymi do wykonania zadań powierzonych im na podstawie niniejszego rozporządzenia.

5. Państwa członkowskie dostarczają informacji żądanych przez organy nadzorcze, o których mowa w art. 51 ust. 1 rozporządzenia (UE) 2016/679, a w szczególności przekazują im informacje o działaniach podejmowanych zgodnie ze swoimi obowiązkami na mocy niniejszego rozporządzenia. Państwa członkowskie udzielają organom nadzorczym, o których mowa w art. 51 ust. 1 rozporządzenia (UE) 2016/679, dostępu do swoich rejestrów, o których mowa w art. 10, 16, 24 i 36 niniejszego rozporządzenia, i do uzasadnień, o których mowa w art. 22 ust. 2 niniejszego rozporządzenia, oraz umożliwiają im uzyskanie w dowolnym momencie dostępu do wszystkich pomieszczeń wykorzystywanych do celów interoperacyjności.

Artykuł 52

Kontrole ze strony Europejskiego Inspektora Ochrony Danych

Europejski Inspektor Ochrony Danych zapewnia przeprowadzanie co najmniej raz na cztery lata kontroli operacji przetwarzania danych osobowych przez eu-LISA, jednostkę centralną ETIAS i Europol na potrzeby niniejszego rozporządzenia zgodnie z odpowiednimi międzynarodowymi standardami przeprowadzania kontroli. Sprawozdanie z takiej kontroli przekazuje się Parlamentowi Europejskiemu, Radzie, eu-LISA, Komisji, państwom członkowskim i danej agencji Unii. eu-LISA, jednostka centralna ETIAS i Europol mają możliwość przedstawienia uwag przed przyjęciem sprawozdań.

eu-LISA, jednostka centralna ETIAS i Europol przekazują informacje żądane przez Europejskiego Inspektora Ochrony Danych, udzielają mu dostępu do wszelkich żądanych przez niego dokumentów i do swoich rejestrów, o których mowa w art. 10, 16, 24 i 36, oraz umożliwiają mu uzyskanie dostępu do wszystkich swoich pomieszczeń w dowolnym momencie.

Artykuł 53

Współpraca między organami nadzorczymi a Europejskim Inspektorem Ochrony Danych

1. Organy nadzorcze i Europejski Inspektor Ochrony Danych – działając z poszanowaniem zakresu swoich kompetencji – współpracują ze sobą aktywnie w ramach przysługujących im uprawnień i zapewniają skoordynowany nadzór nad korzystaniem z elementów interoperacyjności i stosowaniem innych przepisów niniejszego rozporządzenia, zwłaszcza jeżeli Europejski Inspektor Ochrony Danych lub organ nadzorczy stwierdzą poważne rozbieżności między praktykami państw członkowskich lub potencjalnie niezgodne z prawem przekazywanie danych przy wykorzystaniu kanałów komunikacyjnych elementów interoperacyjności.

2. W przypadkach, o których mowa w ust. 1 niniejszego rozporządzenia, zapewnia się skoordynowany nadzór zgodnie z art. 62 rozporządzenia (UE) 2018/1725.

3. Dwa lata po wejściu w życie niniejszego rozporządzenia, a następnie co dwa lata Europejska Rada Ochrony Danych przesyła wspólne sprawozdanie ze swojej działalności na podstawie niniejszego artykułu Parlamentowi Europejskiemu, Radzie, Komisji, Europolowi, Europejskiej Agencji Straży Granicznej i Przybrzeżnej oraz eu-LISA do dnia 12 czerwca 2021 r. W sprawozdaniu tym każdemu państwu członkowskiemu poświęcony jest osobny rozdział przygotowany przez organ nadzorczy danego państwa członkowskiego.

ROZDZIAŁ VIII

Obowiązki

Artykuł 54

Obowiązki eu-LISA w fazie projektowania i opracowywania systemu

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

2. Elementy interoperacyjności są obsługiwane przez eu-LISA w jej obiektach technicznych i zapewniają funkcje określone w niniejszym rozporządzeniu zgodnie z warunkami bezpieczeństwa, dostępności, jakości i wydajności, o których mowa w art. 55 ust. 1.

3. eu-LISA odpowiada za tworzenie elementów interoperacyjności i adaptacje konieczne do ustanowienia interoperacyjności między systemami centralnymi EES, VIS, ETIAS, SIS, Eurodac i ECRIS-TCN a europejskim portalem wyszukiwania, wspólnym systemem porównywania danych biometrycznych, wspólnym repozytorium danych umożliwiających identyfikację, detektorem wielokrotnych tożsamości i centralnym repozytorium sprawozdawczo-statystycznym.

Bez uszczerbku dla art. 66 eu-Lisa nie ma dostępu do danych osobowych przetwarzanych za pośrednictwem europejskiego portalu wyszukiwania, wspólnego systemu porównywania danych biometrycznych, wspólnego repozytorium danych umożliwiających identyfikację ani detektora wielokrotnych tożsamości.

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

eu-LISA tworzy i wdraża elementy interoperacyjności tak szybko, jak to tylko możliwe, po wejściu w życie niniejszego rozporządzenia i przyjęciu przez Komisję środków, o których mowa w art. 8 ust. 2, art. 9 ust. 7, art. 28 ust. 5 i 7, art. 37 ust. 4, art. 38 ust. 3, art. 39 ust. 5, art. 43 ust. 5 i art. 78 ust. 10.

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

4. W fazie projektowania i opracowywania powołuje się Komisję ds. Zarządzania Programem składającą się maksymalnie z 10 członków. Składa się ona z siedmiu członków wyznaczonych przez zarząd eu-LISA spośród jego członków lub ich zastępców, przewodniczącego grupy doradczej ds. interoperacyjności, o której mowa w art. 75, członka reprezentującego eu-LISA wyznaczonego przez jej dyrektora wykonawczego i jednego członka wyznaczonego przez Komisję. Członków wyznaczanych przez zarząd eu-LISA wybiera się jedynie spośród tych państw członkowskich, które są w pełni związane na mocy prawa Unii aktami prawnymi regulującymi opracowywanie, tworzenie, funkcjonowanie i użytkowanie wszystkich wielkoskalowych systemów informatycznych UE oraz które będą uczestniczyć w elementach interoperacyjności.

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

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

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

a) przewodniczenia;

b) miejsca odbywania posiedzeń;

c) przygotowywania posiedzeń;

d) dopuszczenia ekspertów na posiedzenia;

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

Komisji ds. Zarządzania Programem przewodniczy państwo członkowskie, które jest w pełni związane na mocy prawa Unii aktami prawnymi regulującymi opracowywanie, rozwój, funkcjonowanie i użytkowanie wszystkich systemów informacyjnych UE i które będzie uczestniczyć w elementach interoperacyjności.

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

Grupa doradcza ds. interoperacyjności, o której mowa w art. 75, spotyka się regularnie do czasu rozpoczęcia funkcjonowania elementów interoperacyjności. Po każdym posiedzeniu grupa doradcza przedkłada sprawozdanie Komisji ds. Zarządzania Programem. Grupa doradcza zapewnia wiedzę techniczną w celu wsparcia Komisji ds. Zarządzania Programem w realizacji jej zadań oraz śledzi stan przygotowania państw członkowskich.

Artykuł 55

Obowiązki eu-LISA po rozpoczęciu funkcjonowania systemów

1. Po rozpoczęciu funkcjonowania każdego z elementów interoperacyjności eu-LISA odpowiada za zarządzanie techniczne infrastrukturą centralną elementów interoperacyjności, w tym za ich obsługę techniczną i zmiany techniczne. We współpracy z państwami członkowskimi zapewnia ona stosowanie najlepszej dostępnej technologii, z uwzględnieniem analizy kosztów i korzyści. eu-LISA odpowiada też za zarządzanie techniczne infrastrukturą komunikacyjną, o której mowa w art. 6, 12, 17, 25 i 39.

Zarządzanie techniczne elementami interoperacyjności obejmuje wszystkie zadania i rozwiązania techniczne niezbędne do zapewnienia funkcjonowania elementów interoperacyjności i zapewniające nieprzerwane usługi państwom członkowskim i agencjom unijnym przez 24 godziny, 7 dni w tygodniu, zgodnie z niniejszym rozporządzeniem. Obejmuje ono w szczególności prace konserwacyjne i zmiany techniczne konieczne do zapewnienia zadowalającego poziomu jakości technicznej funkcjonowania systemu, zwłaszcza jeśli chodzi o czas odpowiedzi podczas wyszukiwania w infrastrukturze centralnej, zgodnie ze specyfikacją techniczną.

Wszystkie elementy interoperacyjności należy opracować i zarządzać nimi w taki sposób, by zapewnić szybki, sprawny, efektywny i kontrolowany dostęp oraz pełną, nieprzerwaną dostępność elementów i danych zarejestrowanych w detektorze wielokrotnych tożsamości, przechowywanych we wspólnym systemie porównywania danych biometrycznych i wspólnym repozytorium danych umożliwiających identyfikację, oraz czas odpowiedzi zgodny z potrzebami operacyjnymi organów państwa członkowskiego i agencji unijnych.

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

Bez uszczerbku dla art. 66, eu-Lisa nie ma dostępu do danych osobowych przetwarzanych za pośrednictwem europejskiego portalu wyszukiwania, wspólnego systemu porównywania danych biometrycznych, wspólnego repozytorium danych umożliwiających identyfikację ani detektora wielokrotnych tożsamości.

3. eu-LISA tworzy i aktualizuje mechanizm i procedury przeprowadzania kontroli jakości danych przechowywanych we wspólnym systemie porównywania danych biometrycznych i wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 37.

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

Artykuł 56

Obowiązki państw członkowskich

1. Każde państwo członkowskie odpowiada za:

a) podłączenie do infrastruktury komunikacyjnej europejskiego portalu wyszukiwania i wspólnego repozytorium danych umożliwiających identyfikację;

b) integrację istniejących krajowych systemów i infrastruktury z europejskim portalem wyszukiwania, wspólnym repozytorium danych umożliwiających identyfikację i detektorem wielokrotnych tożsamości;

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

d) zarządzanie dostępem odpowiednio upoważnionego personelu właściwych organów krajowych do europejskiego portalu wyszukiwania, wspólnego repozytorium danych umożliwiających identyfikację i detektora wielokrotnych tożsamości oraz ustalenia dotyczące tego dostępu, zgodnie z niniejszym rozporządzeniem, a także sporządzenie listy takich członków personelu wraz z ich profilami i jej regularną aktualizację;

e) przyjęcie środków ustawodawczych, o których mowa w art. 20 ust. 5 i 6, aby umożliwić dostęp do wspólnego repozytorium danych umożliwiających identyfikację na potrzeby identyfikacji;

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

g) zgodność z wymaganiami dotyczącymi jakości danych ustanowionymi na mocy prawa Unii;

h) przestrzeganie zasad każdego systemu informacyjnego UE dotyczących zapewnienia bezpieczeństwa i integralności danych osobowych;

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

2. Każde państwo członkowskie podłącza swoje wyznaczone organy do wspólnego repozytorium danych umożliwiających identyfikację.

Artykuł 57

Obowiązki jednostki centralnej ETIAS

Jednostka centralna ETIAS odpowiada za:

a) ręczną weryfikację różniących się tożsamości zgodnie z art. 29;

b) wykrywanie wielokrotnych tożsamości na podstawie danych przechowywanych w systemach EES, VIS, Eurodac i SIS, o którym mowa w art. 59.

ROZDZIAŁ IX

Zmiany w innych aktach prawa Unii

Artykuł 58

Zmiany w rozporządzeniu (WE) nr 767/2008

W rozporządzeniu (WE) nr 767/2008 wprowadza się następujące zmiany:

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

„Poprzez przechowywanie danych dotyczących tożsamości, danych dokumentów podróży i danych biometrycznych we wspólnym repozytorium danych umożliwiających identyfikację ustanowionym na mocy art. 17 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/817 (*) system VIS przyczynia się do ułatwiania i wspomagania poprawnej identyfikacji osób zarejestrowanych w VIS na warunkach i w celach określonych w art. 20 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).".

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

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

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

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

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

„1a. Wspólne repozytorium danych umożliwiających identyfikację zawiera dane, o których mowa w art. 9 ust. 4 lit. a)–c), ust. 5 i 6.„Pozostałe dane zawarte w VIS są przechowywane w systemie centralnym VIS";

4) art. 6 ust. 2 otrzymuje brzmienie:

„2. Dostęp do VIS do celów sprawdzania danych jest zarezerwowany wyłącznie dla odpowiednio upoważnionego personelu organów krajowych każdego państwa członkowskiego, które są organami właściwymi do celów określonych w art. 15–22, oraz dla odpowiednio upoważnionego personelu organów krajowych każdego państwa członkowskiego i agencji unijnych, które są właściwe do celów określonych w art. 20 i 21 rozporządzenia (UE) 2019/817. Taki dostęp jest ograniczony stosownie do zakresu, w jakim dane te są wymagane do realizacji ich zadań w tych celach i proporcjonalnie do zamierzonych celów";

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

„a) nazwisko; imię (imiona); data urodzenia; płeć;

aa) nazwisko rodowe (poprzednie nazwisko lub nazwiska); miejsce i państwo urodzenia; obecne obywatelstwo i obywatelstwo w chwili urodzenia

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

c) data upływu ważności dokumentu lub dokumentów podróży;

ca) organ, który wydał dokument podróży, i data jego wydania;";

Artykuł 59

Zmiany w rozporządzeniu (UE) nr 2016/399

W art. 8 dodaje się ust. 4a w brzmieniu:

„4a. Jeśli podczas wjazdu lub wyjazdu w wyniku sprawdzenia w stosownych bazach danych, w tym w detektorze wielokrotnych tożsamości za pośrednictwem europejskiego portalu wyszukiwania, o których mowa, odpowiednio, w art. 25 ust. 1 i art. 6 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/817 (*) wystąpi powiązanie żółte lub czerwone, straż graniczna dokonuje sprawdzenia we wspólnym repozytorium danych umożliwiających identyfikację ustanowionym w art. 17 ust. 1 tego rozporządzenia lub w SIS lub w obu, aby ocenić różnice w powiązanych danych dotyczących tożsamości lub danych dokumentu podróży. Straż graniczna dokonuje dodatkowej weryfikacji koniecznej do podjęcia decyzji w sprawie statusu i koloru powiązania.

Zgodnie z art. 69 ust. 1 rozporządzenia (UE) 2019/817 niniejszy ustęp obowiązuje wyłącznie od momentu rozpoczęcia funkcjonowania detektora wielokrotnych tożsamości na mocy art. 72 ust. 4 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).";

Artykuł 60

Zmiany w rozporządzeniu (UE) 2017/2226

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

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

„3. Poprzez przechowywanie danych potwierdzających tożsamość, danych dokumentów podróży i danych biometrycznych we wspólnym repozytorium danych umożliwiających identyfikację ustanowionym na mocy art. 17 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/817 (*) EES przyczynia się do ułatwienia i wspomagania poprawnej identyfikacji osób zarejestrowanych w systemie EES na warunkach i w celach określonych w art. 20 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).";

2) w art. 3 ust. 1 wprowadza się następujące zmiany:

a) pkt 22 otrzymuje brzmienie:

„22) »dane EES« oznaczają wszystkie dane przechowywane w systemie centralnym EES i wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 15–20.";

b) dodaje się nowy pkt 22a w brzmieniu:

„22a) »dane dotyczące tożsamości« oznaczają dane, o których mowa w art. 16 ust. 1 lit. a), a także odpowiednie dane, o których mowa w art. 17 ust. 1 i art. 18 ust. 1";

c) dodaje się nowe punkty 32 i 33:

„32) »europejski portal wyszukiwania« oznacza europejski portal wyszukiwania ustanowiony w art. 6 ust. 1 rozporządzenia (UE) 2019/817;

33) »wspólne repozytorium danych umożliwiających identyfikację« oznacza wspólne repozytorium danych umożliwiających identyfikację ustanowione w art. 17 ust. 1 rozporządzenia (UE) 2019/817";

3) w art. 6 ust. 1 dodaje się lit. ca) w brzmieniu:

„j) zapewnić poprawną identyfikację osób.";

4) w art. 7 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

(i) dodaje się literę w brzmieniu:

„aa) infrastruktury centralnej wspólnego repozytorium danych umożliwiających identyfikację, o której mowa w art. 17 ust. 2 lit. a) rozporządzenia (UE) 2019/817;";

(ii) lit. f) otrzymuje brzmienie:

„f) bezpiecznej infrastruktury łączności między systemem centralnym EES a infrastrukturą centralną europejskiego portalu wyszukiwania oraz wspólnego repozytorium danych umożliwiających identyfikację";

b) dodaje się ust. 1a w brzmieniu:

„1a. Wspólne repozytorium danych umożliwiających identyfikację zawiera dane, o których mowa w art. 16 ust. 1 lit. a)–d), art. 17 ust. 1 lit. a), b) i c) oraz art. 18 ust. 1 i 2. Pozostałe dane pochodzące z EES są przechowywane w systemie centralnym EES.";

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

„4. Dostęp do danych pochodzących z EES zawartych we wspólnym repozytorium danych umożliwiających identyfikację jest zarezerwowany wyłącznie dla odpowiednio upoważnionego personelu organów krajowych każdego państwa członkowskiego i odpowiednio upoważnionego personelu agencji unijnych, które są właściwe do celów określonych w art. 20 i 21 rozporządzenia (UE) 2019/817. Dostęp taki jest ograniczony do zakresu, w jakim dane te są niezbędne do wykonywania ich zadań w tych celach oraz proporcjonalnie do wyznaczonych celów.";

6) w art. 21 wprowadza się następujące zmiany:

a) w ust. 1 otrzymuje brzmienie:

„1. Jeżeli nie ma technicznej możliwości wprowadzenia danych do systemu centralnego EES lub wspólnego repozytorium danych umożliwiających identyfikację lub w przypadku awarii systemu centralnego EES lub wspólnego repozytorium danych umożliwiających identyfikację dane, o których mowa w art. 16–20, przechowuje się tymczasowo w jednolitym interfejsie krajowym. Jeżeli nie jest to możliwe, dane tymczasowo przechowuje się lokalnie w formacie elektronicznym. W obydwu przypadkach dane wprowadza się do systemu centralnego EES lub wspólnego repozytorium danych umożliwiających identyfikację, gdy tylko rozwiązany zostanie problem braku technicznej możliwości wprowadzania danych lub zostanie usunięta awaria. Państwa członkowskie podejmują odpowiednie środki i udostępniają wymaganą infrastrukturę, sprzęt i zasoby w celu zapewnienia, by dane mogły być tymczasowo przechowywane lokalnie w każdym momencie i na każdym ich przejściu granicznym.";

b) ust. 2 akapit pierwszy otrzymuje brzmienie:

„2. Bez uszczerbku dla obowiązku dokonywania odpraw granicznych zgodnie z rozporządzeniem (UE) 2016/399 służba graniczna, w sytuacji wyjątkowej, gdy nie ma technicznej możliwości wprowadzenia danych do systemu centralnego EES i wspólnego repozytorium danych umożliwiających identyfikację ani do jednolitego interfejsu krajowego i nie ma technicznej możliwości tymczasowego przechowywania danych lokalnie w formacie elektronicznym, zapisuje ręcznie dane, o których mowa w art. 16–20 niniejszego rozporządzenia, z wyjątkiem danych biometrycznych, i zamieszcza w dokumencie podróży obywatela państwa trzeciego stempel wjazdowy lub wyjazdowy. Dane te wprowadzane są do systemu centralnego EES i do wspólnego repozytorium danych umożliwiających identyfikację, jak tylko jest to technicznie możliwe.";

7) w art. 23 wprowadza się następujące zmiany:

a) dodaje się ust. 2a w brzmieniu:

„2a. Do celów weryfikacji zgodnie z ust. 1 niniejszego artykułu służba graniczna dokonuje zapytania za pośrednictwem europejskiego portalu wyszukiwania, aby porównać dane dotyczące obywatela państwa trzeciego z odpowiednimi danymi EES i VIS.";

b) ust. 4 akapit pierwszy otrzymuje brzmienie:

„4. Jeżeli w wyniku wyszukiwania według danych alfanumerycznych określonych w ust. 2 niniejszego artykułu okazuje się, że dane dotyczące obywatela państwa trzeciego nie są zarejestrowane w EES, a weryfikacja obywatela państwa trzeciego zgodnie z ust. 2 niniejszego artykułu nie powiedzie się lub istnieją wątpliwości co do tożsamości obywatela państwa trzeciego, służby graniczne mają dostęp do danych w celu identyfikacji zgodnie z art. 27 w celu utworzenia lub aktualizacji akt osobowych zgodnie z art. 14.";

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

„1a. Jeżeli wyznaczone organy dokonały zapytania we wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 22 rozporządzenia (UE) 2019/817, mają one dostęp do EES w celu sprawdzenia danych, jeśli spełniono warunki określone w niniejszym artykule oraz jeśli według uzyskanej odpowiedzi, o której mowa w art. 22 ust. 2 rozporządzenia (UE) 2019/817, dane te są przechowywane w EES.";

9) w art. 33 dodaje się nowy ustęp 1a w brzmieniu:

„1a. Jeżeli Europol dokonał zapytania we wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 22 rozporządzenia (UE) 2019/817, ma on dostęp do EES w celu sprawdzenia danych, jeśli spełniono warunki określone w niniejszym artykule oraz jeśli według uzyskanej odpowiedzi, o której mowa w art. 22 ust. 2 rozporządzenia (UE) 2019/817, dane te są przechowywane w EES.";

10) w art. 34 wprowadza się następujące zmiany:

a) w ust. 1 i 2 sformułowanie „w systemie centralnym EES" otrzymuje brzmienie „we wspólnym repozytorium danych umożliwiających identyfikację i w systemie centralnym EES";

b) w ust. 5 sformułowanie „z systemu centralnego EES" otrzymuje brzmienie „z systemu centralnego EES i ze wspólnego repozytorium danych umożliwiających identyfikację";

11) art. 35 ust. 7 otrzymuje brzmienie:

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

12) w art. 36 sformułowanie „systemu centralnego EES" otrzymuje brzmienie „systemu centralnego EES i wspólnego repozytorium danych umożliwiających identyfikację";

13) w art. 37 wprowadza się następujące zmiany:

a) ust. 1 akapit pierwszy otrzymuje brzmienie:

„1. eu-LISA odpowiada za rozwój systemu centralnego EES i wspólnego repozytorium danych umożliwiających identyfikację, jednolitych interfejsów krajowych, infrastruktury łączności i bezpiecznego kanału komunikacyjnego między systemem centralnym EES i systemem centralnym VIS. eu-LISA odpowiada również za rozwój usługi sieciowej, o której mowa w art. 13 zgodnie ze szczegółowymi zasadami, o których mowa w art. 13 ust. 7, oraz specyfikacjami i warunkami przyjętymi zgodnie z art. 36 akapit pierwszy lit h) oraz za rozwój repozytorium danych, o którym mowa w art. 63 ust. 2.";

b) ust. 3 akapit pierwszy otrzymuje brzmienie:

„3. eu-LISA odpowiada za zarządzanie operacyjne systemem centralnym EES i wspólnym repozytorium danych umożliwiających identyfikację, jednolitymi interfejsami krajowymi i bezpiecznym kanałem komunikacyjnym między systemem centralnym EES i systemem centralnym VIS. We współpracy z państwami członkowskimi eu-LISA zapewnia, by – na potrzeby systemu centralnego EES i wspólnego repozytorium danych umożliwiających identyfikację, jednolitych interfejsów krajowych, infrastruktury łączności, bezpiecznego kanału komunikacyjnego między systemem centralnym EES i systemem centralnym VIS, usługi sieciowej, o której mowa w art. 13, i repozytorium danych, o którym mowa w art. 63 ust. 2 –stale wykorzystywana była, z uwzględnieniem analizy kosztów i korzyści, najlepsza dostępna technologia. eu-LISA odpowiada również za zarządzanie operacyjne infrastrukturą łączności między systemem centralnym EES i jednolitymi interfejsami krajowymi, za usługę sieciową, o której mowa w art. 13, i repozytorium danych, o którym mowa w 63 ust. 2.";

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

„f) odniesienie do korzystania z europejskiego portalu wyszukiwania w celu przeszukania EES zgodnie z art. 7 ust. 2 rozporządzenia (UE) 2019/817.";

15) w art. 63 wprowadza się następujące zmiany:

a) ust. 2 otrzymuje brzmienie:

„2. Do celów ust. 1 niniejszego artykułu eu-LISA przechowuje dane określone w ust. 1 w centralnym repozytorium sprawozdawczo-statystycznym, o którym mowa w art. 39 rozporządzenia (UE) 2019/817.";

b) w ust. 4 dodaje się akapit drugi w brzmieniu:

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

Artykuł 61

Zmiany w rozporządzeniu (UE) 2018/1240

W rozporządzeniu (UE) 2018/1240 wprowadza się następujące zmiany:

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

„3. Poprzez przechowywanie danych dotyczących tożsamości i danych dokumentów podróży we wspólnym repozytorium danych umożliwiających identyfikację ustanowionym na mocy art. 17 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/817 (*) system ETIAS przyczynia się do ułatwiania i wspomagania poprawnej identyfikacji osób zarejestrowanych w ETIAS na warunkach i w celach określonych w art. 20 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).";

2) w art. 3 ust. 1 dodaje się litery w brzmieniu:

„23) »wspólne repozytorium danych umożliwiających identyfikację« oznacza wspólne repozytorium danych umożliwiających identyfikację ustanowione na mocy art. 17 ust. 1 rozporządzenia (UE) 2019/817;

24) »europejski portal wyszukiwania« oznacza europejski portal wyszukiwania ustanowiony na mocy art. 6 ust. 1 rozporządzenia (UE) 2019/817;

25) »system centralny ETIAS« oznacza system centralny, o którym mowa w art. 6 ust. 2 lit. a) wraz ze wspólnym repozytorium danych umożliwiających identyfikację w zakresie, w jakim wspólne repozytorium danych umożliwiających identyfikację zawiera dane, o których mowa w art. 6 ust. 2a;

26) »dane dotyczące tożsamości« oznaczają dane, o których mowa w art. 17 ust. 2 lit. a), b) i c);

27) »dane dokumentu podróży« oznaczają dane, o których mowa w art. 17 ust. 2 lit. d) i e), oraz trzyliterowy kod państwa wydającego dokument podróży, o którym mowa w art. 19 ust. 3 lit. c);";

3) w art. 4 dodaje się punkt w brzmieniu:

„g) zapewniać poprawną identyfikację osób;";

4) w art. 6 wprowadza się następujące zmiany:

a) w ust. 2 wprowadza się następujące zmiany:

(i) lit. a) otrzymuje brzmienie:

„a) systemu centralnego, obejmującego listę ostrzegawczą ETIAS, o której mowa w art. 34;";

(ii) dodaje się literę w brzmieniu:

„aa) wspólnego repozytorium danych;";

(iii) lit. d) otrzymuje brzmienie:

„d) bezpiecznej infrastruktury łączności między systemem centralnym a infrastrukturą centralną europejskiego portalu wyszukiwania i wspólnego repozytorium danych umożliwiających identyfikację;"

b) dodaje się ustęp w brzmieniu:

„2a. Wspólne repozytorium danych umożliwiających identyfikację zawiera dane dotyczące tożsamości i dane dokumentów podróży. Pozostałe dane są przechowywane w systemie centralnym.";

5) w art. 13 wprowadza się następujące zmiany:

a) dodaje się następujący ustęp w brzmieniu:

„4a. Dostęp do danych dotyczących tożsamości i danych dokumentów podróży przechowywanych we wspólnym repozytorium danych umożliwiających identyfikację jest również zarezerwowany wyłącznie dla odpowiednio upoważnionego personelu organów krajowych każdego państwa członkowskiego i odpowiednio upoważnionego personelu agencji unijnych, które są właściwe do celów określonych w art. 20 i 21 rozporządzenia (UE) 2019/817. Dostęp taki jest ograniczony stosownie do zakresu, w jakim dane są niezbędne do wykonywania ich zadań we wspomnianych celach oraz proporcjonalnie do wyznaczonych celów.";

b) ust. 5 otrzymuje brzmienie:

„5. Każde państwo członkowskie wyznacza właściwe organy krajowe, o których mowa w ust. 1, 2, 4 i 4a niniejszego artykułu, oraz niezwłocznie przekazuje wykaz tych organów eu-LISA zgodnie z art. 87 ust. 2. W wykazie określa się, do jakich celów należycie upoważniony personel każdego z organów ma dostęp do danych przechowywanych w systemie informacyjnym ETIAS zgodnie z ust. 1, 2, 4 i 4a niniejszego artykułu.";

6) w art. 17 ust. 2 wprowadza się następujące zmiany:

a) lit. a) otrzymuje brzmienie:

„a) nazwisko, imię/imiona (imiona nadane), nazwisko przy urodzeniu; data urodzenia, miejsce urodzenia, płeć, aktualne obywatelstwo;";

b) dodaje się literę w brzmieniu:

„aa) państwo urodzenia, imię/imiona rodziców wnioskodawcy;";

7) w art. 19 ust. 4 wyrazy „art. 17 ust. 2 lit. a)" zastępuje się wyrazami „art. 17 ust. 2 lit. a) i aa)";

8) w art. 20 wprowadza się następujące zmiany:

a) akapit pierwszy w ust. 2 otrzymuje brzmienie:

„2. System centralny ETIAS uruchamia zapytanie za pośrednictwem europejskiego portalu wyszukiwania w celu porównania odpowiednich danych, o których mowa w art. 17 ust. 2 lit. a), aa), b), c), d), f), g), j), k) i m) i art. 17 ust. 8, z danymi obecnymi w rekordzie danych, pliku lub wpisie zarejestrowanym w pliku wniosku przechowywanym w systemie centralnym ETIAS, SIS, EES, VIS, Eurodac, danych Europolu i w bazach danych Interpolu.";

b) w ust. 4 wyrazy „art. 17 ust. 2 lit. a), b), c), d), f), g), j), k) i m)" zastępuje się słowami „art. 17 ust. 2 lit. a), aa), b), c), d), f), g), j), k) i m)";

c) w art. 5 wyrazy „art. 17 ust. 2 lit. a), c), f), h) i i)" zastępuje się wyrazami „art. 17 ust. 2 lit. a), aa), c), f), h) i i) ";

9) art. 23 ust. 1 otrzymuje brzmienie:

„1. System centralny ETIAS uruchamia zapytanie za pośrednictwem europejskiego portalu wyszukiwania w celu porównania odpowiednich danych, o których mowa w art. 17 ust. 2 lit. a), aa), b) i d), z danymi obecnymi w SIS w celu ustalenia, czy wnioskodawca podlega jednemu z następujących wpisów:

a) wpis dotyczący osób zaginionych;

b) wpis dotyczący osób, których obecność jest wymagana do celów postępowania sądowego;

c) wpis wprowadzony w celu przeprowadzenia kontroli niejawnej lub kontroli szczególnej.";

10) w art. 52 dodaje się ustęp w brzmieniu:

„1a. W przypadku gdy wyznaczone organy dokonały zapytania we wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 22 rozporządzenia (UE) 2019/817, mogą one uzyskać dostęp do plików wniosków przechowywanych w systemie centralnym ETIAS zgodnie z niniejszym artykułem w celu sprawdzenia danych, jeśli z uzyskanej odpowiedzi, o której mowa w art. 22 ust. 2 rozporządzenia (UE) 2019/817, wynika, że dane te są przechowywane w plikach wniosków przechowywanych w systemie centralnym ETIAS.";

11) w art. 53 dodaje się ustęp w brzmieniu:

„1a. W przypadku gdy Europol dokonał zapytania we wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 22 rozporządzenia (UE) 2019/817, może on uzyskać dostęp do plików wniosków przechowywanych w systemie centralnym ETIAS zgodnie z niniejszym artykułem w celu sprawdzenia danych, jeśli z uzyskanej odpowiedzi, o której mowa w art. 22 ust. 2 rozporządzenia (UE) 2019/817, wynika, że dane te są przechowywane w plikach wniosków przechowywanych w systemie centralnym ETIAS.";

12) w art. 65 ust. 3 akapit piąty słowa „art. 17 ust. 2 lit. a), b), d), e) i f)" zastępuje się słowami „art. 17 ust. 2 lit. a), aa), b), d), e) i f)";

13) w art. 69 ust. 1 dodaje się lit. ca) w brzmieniu:

„ca) w razie potrzeby odniesienie do korzystania z europejskiego portalu wyszukiwania w celu przeszukania systemu centralnego ETIAS, o którym mowa w art. 7 ust. 2 rozporządzenia (UE) 2019/817;";

14) w art. 73 ust. 2 słowa „centralne repozytorium danych" zastępuje się słowami „centralne repozytorium sprawozdawczo-statystyczne, o którym mowa w art. 39 rozporządzenia (UE) 2019/817, w zakresie, w jakim zawiera dane uzyskane z systemu centralnego ETIAS zgodnie z art. 84 niniejszego rozporządzenia";

15) art. 74 ust. 1 akapit pierwszy otrzymuje brzmienie:

„1. Po uruchomieniu ETIAS eu-LISA odpowiada za zarządzanie techniczne systemem centralnym ETIAS i jednolitymi interfejsami krajowymi. eu-LISA odpowiada również za testy techniczne wymagane do utworzenia i aktualizacji reguł kontroli przesiewowej ETIAS. We współpracy z państwami członkowskimi zapewnia korzystanie przez cały czas z najlepszej dostępnej technologii, z zastrzeżeniem analizy kosztów i korzyści. eu-LISA odpowiada również za zarządzanie techniczne infrastrukturą łączności między systemem centralnym ETIAS i jednolitymi interfejsami krajowymi oraz za ogólnodostępną stronę internetową, aplikację mobilną na urządzenia mobilne, funkcję poczty elektronicznej, funkcję zabezpieczonego konta, narzędzie weryfikacji dla wnioskodawców, narzędzie dysponowania zgodą przez wnioskodawców, narzędzie oceny do celów listy ostrzegawczej ETIAS, portal dla przewoźników, usługę sieciową oraz oprogramowanie umożliwiające przetwarzanie wniosków.";

16) art. 84 ust. 2 akapit pierwszy otrzymuje brzmienie:

„2. Do celów ust. 1 niniejszego artykułu eu-LISA przechowuje dane określone w tym ustępie w centralnym repozytorium sprawozdawczo-statystycznym, o którym mowa w art. 39 rozporządzenia (UE) 2019/817. Zgodnie z art. 39 tego rozporządzenia międzysystemowe dane statystyczne i sprawozdania analityczne umożliwiają organom wymienionym w ust. 1 niniejszego artykułu uzyskanie sprofilowanych sprawozdań i statystyk w celu wsparcia wdrażania reguł kontroli przesiewowej ETIAS, o których mowa w art. 33, poprawy oceny zagrożeń dla bezpieczeństwa, ryzyka nielegalnej imigracji i wysokiego ryzyka epidemiologicznego, zwiększenia efektywności odpraw granicznych oraz wsparcia jednostki centralnej ETIAS i jednostek krajowych ETIAS w rozpatrywaniu wniosków o zezwolenie na podróż.";

17) w art. 84 ust. 4 dodaje się akapit w brzmieniu:

„Statystyki dzienne są przechowywane w centralnym repozytorium sprawozdawczo-statystycznym, o którym mowa w art. 39 rozporządzenia (UE) 2019/817.".

Artykuł 62

Zmiany w rozporządzeniu (UE) 2018/1726

W rozporządzeniu (UE) 2018/1726 wprowadza się następujące zmiany:

1) art. 12 otrzymuje brzmienie:

„*Artykuł 12*

Jakość danych

1. Bez uszczerbku dla odpowiedzialności państw członkowskich w zakresie danych wprowadzonych do systemów zarządzanych operacyjnie przez Agencję, ustanawia ona – przy ścisłym udziale swoich grup doradczych – dla wszystkich systemów zarządzanych operacyjnie przez agencję, zautomatyzowane mechanizmy i procedury kontroli jakości danych, wspólne wskaźniki jakości danych i minimalne normy jakości przechowywania danych, zgodnie z odpowiednimi przepisami aktów prawnych regulujących te systemy informacyjne oraz art. 37 rozporządzeń Parlamentu Europejskiego i Rady (UE) 2019/817 (*) i (UE) 2019/818 (**).

2. Agencja ustanawia centralne repozytorium zawierające wyłącznie zanonimizowane dane sprawozdawczo-statystyczne zgodnie z art. 39 rozporządzeń (UE) 2019/817 i (UE) 2019/818 podlegające szczegółowym przepisom w ramach instrumentów prawnych regulujących opracowywanie, tworzenie, funkcjonowanie i użytkowanie wielkoskalowych systemów informatycznych zarządzanych przez Agencję.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).

(**) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/818 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze współpracy policyjnej i sądowej oraz zmieniające rozporządzenia (UE) 2018/1726, (UE) 2018/1862 i (UE) 2019/816 (Dz.U. L 135 z 22.5.2019, s. 85).";

2) w art. 19 ust. 1 wprowadza się następujące zmiany:

a) dodaje się następującą literę:

„eea) przyjmuje sprawozdania ze stanu prac nad rozwojem elementów interoperacyjności zgodnie z art. 78 ust. 2 rozporządzenia (UE) 2019/817 i art. 74 ust. 2 rozporządzenia (UE) 2019/818;";

b) lit. ff) otrzymuje brzmienie:

„ff) przyjmuje sprawozdania dotyczące technicznego funkcjonowania systemu SIS II – na podstawie art. 60 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1861 (*) oraz art. 74 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1862 (**), systemu VIS – na podstawie art. 50 ust. 3 rozporządzenia (WE) nr 767/2008 i art. 17 ust. 3 decyzji 2008/633/WSiSW, systemu EES – na podstawie art. 72 ust. 4 rozporządzenia (UE) 2017/2226, systemu ETIAS – na podstawie art. 92 ust. 4 rozporządzenia (UE) 2018/1240 w sprawie systemu ECRIS-TCN i wzorcowej implementacji ECRIS – na podstawie art. 36 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/816 (***) oraz elementów interoperacyjności – na podstawie art. 78 ust. 3 rozporządzenia (UE) 2019/817 i art. 74 ust. 3 rozporządzenia (UE) 2019/818;

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmieniające konwencję wykonawczą do układu z Schengen oraz zmieniające i uchylające rozporządzenie (WE) nr 1987/2006 (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmieniające konwencję wykonawczą do układu z Schengen oraz zmieniające i uchylające rozporządzenie (WE) nr 1987/2006) (Dz.U. L 312 z 7.12.2018, s. 14).

(**) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmieniające i uchylające decyzję Rady 2007/533/WSiSW oraz uchylające rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady i decyzję Komisji 2010/261/UE (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmieniające i uchylające decyzję Rady 2007/533/WSiSW oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzję Komisji 2010/261/UE) (Dz.U. L 312 z 7.12.2018, s. 56).

(***) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system identyfikacji państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) nr 2018/1726 (Dz.U. L 135 z 22.5.2019, s. 1).";

c) lit. hh) otrzymuje brzmienie:

„hh) przyjmuje oficjalne uwagi do sprawozdań Europejskiego Inspektora Ochrony Danych z audytów, na podstawie art. 56 ust. 2 rozporządzenia (UE) nr 2018/1861, art. 42 ust. 2 rozporządzenia (WE) nr 767/2008 i art. 31 ust. 2 rozporządzenia (UE) nr 603/2013, art. 56 ust. 2 rozporządzenia (UE) 2017/2226, art. 67 rozporządzenia (UE) 2018/1240. art. 29 ust. 2 rozporządzenia (UE) 2019/816 oraz art. 52 rozporządzeń (UE) 2019/817 i (UE) 2019/818, a także zapewnia odpowiednie działania następcze w sprawie tych audytów;";

d) lit. mm) otrzymuje brzmienie:

„mm) zapewnia coroczną publikację wykazu właściwych organów upoważnionych do bezpośredniego wyszukiwania danych zawartych w SIS II zgodnie z art. 41 ust. 8 rozporządzenia (UE) nr 2018/1861 i art. 56 ust. 7 rozporządzenia (UE) 2018/1862, wraz z wykazem biur krajowych systemów SIS (N.SIS) i biur SIRENE zgodnie z art. 7 ust. 3 rozporządzenia (UE) 2018/1861 i art. 7 ust. 3 rozporządzenia (UE) 2018/1862, jak również wykazu właściwych organów zgodnie z art. 65 ust. 2 rozporządzenia (UE) nr 2017/2226, wykazu właściwych organów zgodnie z art. 87 ust. 2 rozporządzenia (UE) 2018/1240, wykazu organów centralnych zgodnie z art. 34 ust. 2 rozporządzenia (UE) 2019/816 oraz wykazu organów zgodnie z art. 71 ust. 1 rozporządzenia (UE) 2019/817 i art. 67 ust. 1 rozporządzenia (UE) 2019/818;";

3) art. 22 ust. 4 otrzymuje brzmienie:

„4. Europol i Eurojust mogą uczestniczyć w posiedzeniach zarządu jako obserwatorzy, gdy porządek obrad zawiera kwestię dotyczącą SIS II, w związku ze stosowaniem decyzji 2007/533/WSiSW.

Europejska Straż Graniczna i Przybrzeżna może uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad zawiera kwestię dotyczącą SIS w związku ze stosowaniem rozporządzenia (UE) 2016/1624.

Europol może uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad zawiera kwestię dotyczącą VIS, w związku ze stosowaniem decyzji 2008/633/WSiSW, lub kwestię dotyczącą systemu Eurodac, w związku ze stosowaniem rozporządzenia (UE) nr 603/2013.

Europol może uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad zawiera kwestię dotyczącą EES, w związku ze stosowaniem rozporządzenia (UE) 2017/2226, lub kwestię dotyczącą ETIAS, w związku ze stosowaniem rozporządzenia (UE) 2018/1240.

Europejska Agencja Straży Granicznej i Przybrzeżnej może uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad obejmuje kwestię dotyczącą systemu ETIAS z związku ze stosowaniem rozporządzenia (UE) 2018/1240.

Eurojust, Europol i Prokuratura Europejska mogą uczestniczyć w posiedzeniach zarządu jako obserwatorzy, gdy porządek obrad obejmuje kwestię dotyczącą rozporządzenia (UE) 2019/816.

Europol, Eurojust i Europejska Agencja Straży Granicznej i Przybrzeżnej mogą uczestniczyć w posiedzeniach zarządu jako obserwatorzy, gdy porządek obrad obejmuje kwestię dotyczącą rozporządzenia (UE) 2019/817 i (EU) 2019/818.

Zarząd może zaprosić dowolną inną osobę, której opinia może mieć znaczenie, do uczestnictwa w posiedzeniach jako obserwator.";

4) art. 24 ust. 3 lit. p) otrzymuje brzmienie:

„p) bez uszczerbku dla art. 17 regulaminu pracowniczego urzędników, określenie wymogów poufności w celu wykonania art. 17 rozporządzenia (WE) nr 1987/2006, art. 17 decyzji 2007/533/WSiSW, art. 26 ust. 9 rozporządzenia (WE) nr 767/2008, art. 4 ust. 4 rozporządzenia (UE) nr 603/2013; art. 37 ust. 4 rozporządzenia (UE) 2017/2226, art. 74 ust. 2 rozporządzenia (UE) 2018/1240, art. 11 ust. 16 rozporządzenia (UE) 2019/816 i art. 55 ust. 2 rozporządzeń (UE) 2019/817 i (UE) 2019/818";

5) w art. 27 wprowadza się następujące zmiany:

a) w ust. 1 dodaje się literę w brzmieniu:

„da) grupa doradcza ds. interoperacyjności;";

b) ust. 3 otrzymuje brzmienie:

„3. Europol, Eurojust i Europejska Agencja Straży Granicznej i Przybrzeżnej mogą powołać po jednym przedstawicielu do grupy doradczej ds. SIS II.

Europol może także powołać przedstawiciela do grupy doradczej ds. VIS i grupy doradczej ds. systemu Eurodac oraz grupy doradczej ds. EES/ETIAS.

Europejska Agencja Straży Granicznej i Przybrzeżnej może także powołać przedstawiciela do grupy doradczej ds. EES-ETIAS.

Europol, Eurojust i Prokuratura Europejska mogą również powołać po jednym przedstawicielu do grupy doradczej ds. systemu ECRIS-TCN.

Europol, Eurojust oraz Europejska Agencja Straży Granicznej i Przybrzeżnej mogą powołać po jednym przedstawicielu do grupy doradczej ds. interoperacyjności.".

Artykuł 63

Zmiany w rozporządzeniu (UE) 2018/1861

W rozporządzeniu (UE) 2018/1861 wprowadza się następujące zmiany:

1) w art. 3 dodaje się litery w brzmieniu:

„22) »europejski portal wyszukiwania« oznacza europejski portal wyszukiwania ustanowiony na mocy art. 6 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/817 (*);

23) »wspólny system porównywania danych biometrycznych« oznacza wspólny system porównywania danych biometrycznych ustanowiony na mocy art. 12 ust. 1 rozporządzenia (UE) 2019/817;

24) »wspólne repozytorium danych umożliwiających identyfikację« oznacza wspólne repozytorium danych umożliwiających identyfikację ustanowione na mocy art. 17 ust. 1 rozporządzenia (UE) 2019/817;

25) »detektor wielokrotnych tożsamości« oznacza detektor wielokrotnych tożsamości ustanowiony na mocy art. 25 ust. 1 rozporządzenia (UE) 2019/817.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).";

2) w art. 4 wprowadza się następujące zmiany:

a) w ust.1 lit. b) i c) otrzymują brzmienie:

„b) systemu krajowego (N.SIS) w każdym państwie członkowskim, składającego się z krajowych systemów danych, które łączą się z systemem centralnym SIS w tym co najmniej jednej krajowej lub wspólnej wersji zapasowej N.SIS;

c) infrastruktury łączności pomiędzy CS-SIS, wersją zapasową CS-SIS i NI-SIS (zwanej dalej »infrastrukturą łączności«), która zapewnia zaszyfrowaną wirtualną sieć na potrzeby danych SIS oraz wymiany danych między biurami SIRENE, o której mowa w art. 7 ust. 2; oraz

d) bezpiecznej infrastruktury komunikacji między systemem centralnym CS-SIS a infrastrukturą centralną europejskiego portalu wyszukiwania, wspólnego systemu porównywania danych biometrycznych i detektora wielokrotnych tożsamości.";

b) dodaje się ustępy w brzmieniu:

„8. Bez uszczerbku dla ust. 1–5 dane SIS można również wyszukiwać za pośrednictwem europejskiego portalu wyszukiwania.

9. Bez uszczerbku dla ust. 1–5 dane SIS można również przekazywać za pośrednictwem bezpiecznej infrastruktury łączności, o której mowa w ust. 1 lit. d). Takie przekazywanie odbywa się tylko w takim zakresie, w jakim dane te są wymagane do celów rozporządzenia (UE) 2019/817.";

3) w art. 7 dodaje się następujący ustęp:

„2a. Biura SIRENE zapewniają również ręczną weryfikację różniących się tożsamości zgodnie z art. 29 rozporządzenia (UE) 2019/817. W zakresie niezbędnym do wypełnienia tego zadania biura SIRENE mają dostęp do danych przechowywanych we wspólnym repozytorium danych umożliwiających identyfikację i w detektorze wielokrotnych tożsamości w celach określonych w art. 21 i 26 rozporządzenia (UE) 2019/817.";

4) w art. 12 ust. 1 otrzymuje brzmienie:

„1. Państwa członkowskie zapewniają rejestrowanie w N.SIS każdego przypadku uzyskania dostępu do CS-SIS lub dokonania wymiany danych osobowych z CS-SIS w celu sprawdzenia, czy dane wyszukiwanie było zgodne z prawem, monitorowania przetwarzania danych, aby stwierdzić, czy jest ono zgodne z prawem, autokontroli, zapewnienia prawidłowego działania N.SIS, a także integralności i bezpieczeństwa danych. Wymóg ten nie dotyczy procesów automatycznych, o których mowa w art. 4 ust. 6 lit. a), b) i c).

Państwa członkowskie zapewniają rejestrowanie każdego przypadku uzyskania dostępu do danych osobowych za pośrednictwem europejskiego portalu wyszukiwania w celu sprawdzenia, czy dane wyszukiwanie było zgodne z prawem, monitorowania przetwarzania danych, aby stwierdzić, czy jest ono zgodne z prawem, autokontroli oraz zapewnienia integralności i bezpieczeństwa danych.";

5) w art. 34 ust. 1 dodaje się lit. g) w brzmieniu:

„g) weryfikacji różniących się tożsamości i zwalczania oszustw dotyczących tożsamości zgodnie z rozdziałem V rozporządzenia (UE) 2019/817.";

6) art. 60 ust. 6 otrzymuje brzmienie:

„6. Do celów art. 15 ust. 4 oraz ust. 3, 4 i 5 niniejszego artykułu eu-LISA przechowuje dane, o których mowa w art. 15 ust. 4 i w ust. 3 niniejszego artykułu, które nie pozwalają na identyfikację osób fizycznych w centralnym repozytorium sprawozdawczo-statystycznym, o którym mowa w art. 39 rozporządzenia (UE) 2019/817.

eu-LISA umożliwia Komisji i organom, o których mowa w ust. 5 niniejszego artykułu, uzyskanie indywidualnych sprawozdań i statystyk. eu-LISA udziela państwom członkowskim, Komisji, Europolowi i Europejskiej Agencji Straży Granicznej i Przybrzeżnej, na ich wniosek, dostępu do centralnego repozytorium sprawozdawczo-statystycznego zgodnie z art. 39 rozporządzenia (UE) 2019/817.".

Artykuł 64

Zmiany w decyzji 2004/512/WE

Art. 1 ust. 2 decyzji 2004/512/WE otrzymuje brzmienie:

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

a) centralna infrastruktura wspólnego repozytorium danych umożliwiających identyfikację, o którym mowa w art. 17 ust. 2 lit. a) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/817 (*),

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

c) interfejs krajowy w każdym państwie członkowskim, zwany dalej „interfejsem krajowym" (NI-VIS), zapewniający połączenie z odpowiednimi centralnymi organami krajowymi danego państwa członkowskiego;

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

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

f) bezpiecznej infrastruktury łączności między systemem centralnym VIS a infrastrukturą centralną europejskiego portalu wyszukiwania ustanowionego na mocy art. 6 ust. 1 rozporządzenia (UE) 2019/817 oraz wspólnego repozytorium danych umożliwiających identyfikację ustanowionego na mocy art. 17 ust. 1 rozporządzenia (UE) 2019/817.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).".

Artykuł 65

Zmiany w decyzji 2008/633/WSiSW

W decyzja 2008/633/WSiSW wprowadza się następujące zmiany:

1) w art. 5 dodaje się nowy ustęp w brzmieniu:

„1a. Jeżeli wyznaczone organy dokonały zapytania we wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/817 (*) i jeżeli spełniono warunki udzielenia dostępu określone w niniejszym artykule, mają one dostęp do systemu VIS w celu sprawdzenia danych, jeśli według uzyskanej odpowiedzi, o której mowa w art. 22 ust. 2 tego rozporządzenia, dane te są przechowywane w VIS.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 i (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (Dz.U. L 135 z 22.5.2019, s. 27).";

2. w art. 7 dodaje się nowy ustęp w brzmieniu:

„1a. Jeżeli Europol dokonał zapytania we wspólnym repozytorium danych umożliwiających identyfikację zgodnie z art. 22 rozporządzenia (UE) 2019/817 i jeżeli spełniono warunki udzielenia dostępu określone w niniejszym artykule, Europol ma dostęp do systemu VIS w celu sprawdzenia danych, jeśli według uzyskanej odpowiedzi, o której mowa w art. 22 ust. 2 tego rozporządzenia, dane te są przechowywane w VIS.".

ROZDZIAŁ X

Przepisy końcowe

Artykuł 66

Sprawozdawczość i statystyki

1. Odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji i eu-LISA ma możliwość dokonywania sprawdzeń następujących danych związanych z europejskim portalem wyszukiwania, wyłącznie do celów sporządzania sprawozdań i statystyk:

a) liczba wyszukiwań przypadających na użytkownika profilu europejskiego portalu wyszukiwania;

b) liczba wyszukiwań w każdej bazie danych Interpolu.

W oparciu o dane nie może być możliwa identyfikacja poszczególnych osób.

2. Odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji, eu-LISA i jednostki centralnej ETIAS ma możliwość dokonywania sprawdzeń następujących danych związanych ze wspólnym repozytorium danych umożliwiających identyfikację, wyłącznie do celów sporządzania sprawozdań i statystyk:

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

b) obywatelstwo, płeć i rok urodzenia osoby;

c) rodzaj dokumentu podróży oraz trzyliterowy kod państwa wydającego;

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

W oparciu o dane nie może być możliwa identyfikacja poszczególnych osób.

3. Odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji, eu-LISA i jednostki centralnej ETIAS ma możliwość dokonywania sprawdzeń następujących danych związanych z detektorem wielokrotnych tożsamości, wyłącznie do celów sporządzania sprawozdań i statystyk:

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

b) liczba powiązań każdego rodzaju oraz systemy informacyjne UE zawierające powiązane ze sobą dane;

c) okres, przez jaki powiązanie żółte i czerwone pozostawało w systemie.

W oparciu o dane nie może być możliwa identyfikacja poszczególnych osób.

4. Odpowiednio upoważniony personel Europejskiej Agencji Straży Granicznej i Przybrzeżnej ma możliwość dokonywania sprawdzeń danych, o których mowa w ust. 1, 2 i 3 niniejszego artykułu, na potrzeby przeprowadzania analiz ryzyka i ocen narażenia, o których mowa w art. 11 i 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1624 ([40]).

5. Odpowiednio upoważniony personel Europolu ma dostęp możliwość dokonywania sprawdzeń danych, o których mowa w ust. 2 i 3 niniejszego artykułu, na potrzeby przeprowadzania analiz strategicznych, tematycznych i operacyjnych, o których mowa w art. 18 ust. 2 lit. b) i c) rozporządzenia (UE) 2016/794.

6. Do celów ust. 1, 2 i 3 eu-LISA przechowuje dane, o których mowa w tych ustępach, w centralnym repozytorium sprawozdań i statystyk. W oparciu o dane zawarte w tym repozytorium nie może być możliwa identyfikacja poszczególnych osób, ale dane te pozwalają organom wymienionym w ust. 1, 2 i 3 na uzyskanie sprofilowanych sprawozdań i statystyk w celach zwiększenia efektywności odpraw granicznych, wsparcia organów w rozpatrywaniu wniosków wizowych oraz wsparcia kształtowania unijnej polityki w zakresie migracji i bezpieczeństwa w Unii w oparciu o dowody.

7. Komisja udostępnia Agencji Praw Podstawowych Unii Europejskiej, na wniosek, istotne informacje do celów oceny wpływu niniejszego rozporządzenia na prawa podstawowe.

Artykuł 67

Okres przejściowy funkcjonowania europejskiego portalu wyszukiwania

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

2. Komisja jest uprawniona do przyjęcia aktu delegowanego zgodnie z art. 73 w celu zmiany niniejszego rozporządzenia poprzez jednorazowe przedłużenie okresu, o którym mowa w ust. 1 niniejszego artykułu, o nie dłużej niż jeden rok, jeżeli ocena wdrażania europejskiego portalu wyszukiwania wykazała, że takie przedłużenie jest konieczne, w szczególności ze względu na wpływ, jaki miałoby wprowadzenie europejskiego portalu wyszukiwania na organizację i czas trwania kontroli granicznej.

Artykuł 68

Okres przejściowy obowiązujący w stosunku do przepisów w sprawie dostępu do wspólnego repozytorium danych umożliwiających identyfikację do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywania ich lub prowadzenia w ich sprawie postępowań przygotowawczych

Art. 22, art. 60 pkt 8 i 9, art. 61 pkt 10 i 11 oraz art. 65 obowiązują od dnia rozpoczęcia działania wspólnego repozytorium danych umożliwiających identyfikację, o których mowa w art. 72 ust. 1.

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

Artykuł 69

Okres przejściowy obowiązujący w stosunku do wykrywania wielokrotnych tożsamości

1. Przez okres jednego roku od wystosowania przez eu-LISA powiadomienia o zakończeniu testu detektora wielokrotnych tożsamości, o którym mowa w art. 72 ust. 1 lit. b), i przed rozpoczęciem jego funkcjonowania, jednostka centralna ETIAS odpowiada za wykrywanie wielokrotnych tożsamości przy pomocy danych przechowywanych w systemach EES, VIS, Eurodac i SIS. Operacje wykrywania wielokrotnych tożsamości są przeprowadzane przy użyciu wyłącznie danych biometrycznych.

2. Jeśli zapytanie wykaże jedno lub kilka dopasowań, a dane dotyczące tożsamości zawarte w powiązanych ze sobą aktach osobowych są tożsame lub zbliżone, ustanawia się powiązanie białe zgodnie z art. 33.

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

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

3. W razie utworzenia powiązania żółtego detektor wielokrotnych tożsamości udostępnia jednostce centralnej ETIAS dane dotyczące tożsamości obecne w różnych systemach informacyjnych UE.

4. W razie utworzenia powiązania do wpisu w SIS innego niż wpis dokonany na mocy art. 3 rozporządzenia (UE) 2018/1860, art. 24 i 25 rozporządzenia (UE) 2018/1861 lub art. 38 rozporządzenia (UE) 2018/1862, detektor wielokrotnych tożsamości udostępnia dostęp do danych dotyczących tożsamości obecnych w różnych systemach informacyjnych biuru SIRENE państwa członkowskiego, które dokonało wpisu.

5. Jednostka centralna ETIAS lub w przypadkach, o których mowa w ust. 4 niniejszego artykułu, biuro Sirene państwa członkowskiego, które dokonało wpisu, mają dostęp do danych zawartych w pliku potwierdzającym tożsamość i analizują różne tożsamości, a także aktualizują powiązanie zgodnie z art. 31, 32 i 33 oraz dodają je do pliku potwierdzającego tożsamość.

6. Jednostka centralna ETIAS powiadamia Komisję zgodnie z art. 71 ust. 3 dopiero po ręcznym zweryfikowaniu wszystkich powiązań żółtych i zaktualizowaniu ich statusu na powiązania zielone, białe lub czerwone.

7. Państwa członkowskie w razie potrzeby pomagają jednostce centralnej ETIAS w wykrywaniu wielokrotnych tożsamości na mocy niniejszego artykułu.

8. Komisja jest uprawniona do przyjęcia aktu delegowanego zgodnie z art. 73 w celu zmiany niniejszego rozporządzenia poprzez przedłużenie o sześć miesięcy okresu, o którym mowa w ust. 1 niniejszego artykułu, z możliwością dwukrotnego przedłużenia go za każdym razem o sześć miesięcy. Przedłużenie takie przyznaje się wyłącznie w przypadku, gdy ocena przewidywanego czasu na ukończenie wykrywania multiplikacji tożsamości na mocy niniejszego artykułu wskazuje, że wykrywanie wielokrotnych tożsamości nie może zostać ukończone przed upływem pozostałego terminu na podstawie ust. 1 niniejszego artykułu lub przed upływem trwającego przedłużenia, z powodów niezależnych od jednostki centralnej ETIAS oraz że nie można zastosować działań naprawczych. Ocena zostaje przeprowadzona nie później niż trzy miesiące przed upływem takiego terminu lub trwającego przedłużenia.

Artykuł 70

Koszty

1. Koszty poniesione w związku z ustanowieniem i funkcjonowaniem europejskiego portalu wyszukiwania, wspólnego systemu porównywania danych biometrycznych, wspólnego repozytorium danych umożliwiających identyfikację i detektora wielokrotnych tożsamości są pokrywane z budżetu ogólnego Unii.

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

Wyłącza się następujące koszty:

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

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

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

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

3. Bez uszczerbku dla dalszego finansowania w tym celu z innych źródeł budżetu ogólnego Unii Europejskiej, kwota 32 077 000 EUR zostaje uruchomiona z puli 791 000 000 EUR przewidzianej na mocy art. 5 ust. 5 lit. b) rozporządzenia (UE) nr 515/2014 na pokrycie kosztów wdrożenia niniejszego rozporządzenia, jak przewidziano w ust. 1 i 2 niniejszego artykułu.

4. Z puli środków, o której mowa w ust. 3, kwota 22 861 000 EUR zostaje przydzielona eu-LISA, kwota 9 072 000 EUR Europolowi, a kwota 144 000 EUR Agencji Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL), aby wesprzeć te agencje w wykonywaniu ich odpowiednich zadań na mocy niniejszego rozporządzenia. Tego rodzaju finansowanie wdraża się w ramach zarządzania pośredniego.

5. Koszty poniesione przez wyznaczone organy są pokrywane, odpowiednio, przez wyznaczające państwa członkowskie. Koszty podłączenia każdego wyznaczonego organu do wspólnego repozytorium danych umożliwiających identyfikację ponoszą poszczególne państwa członkowskie.

Koszty poniesione przez Europol, w tym koszty podłączenia do wspólnego repozytorium danych umożliwiających identyfikację, ponosi Europol.

Artykuł 71

Powiadomienia

1. Państwa członkowskie powiadamiają eu-LISA o organach, o których mowa w art. 7, 20, 21 i 26, które mogą korzystać z europejskiego portalu wyszukiwania, wspólnego repozytorium danych umożliwiających identyfikację i detektora wielokrotnych tożsamości oraz uzyskiwać do nich dostęp.

Skonsolidowany wykaz tych organów jest publikowany w Dzienniku Urzędowym Unii Europejskiej w terminie trzech miesięcy od daty uruchomienia poszczególnych elementów interoperacyjności zgodnie z art. 72. W przypadku zmian w wykazie eu-LISA raz w roku publikuje zaktualizowany skonsolidowany wykaz.

2. eu-LISA informuje Komisję o pomyślnym zakończeniu testu, o którym mowa w art. 72 ust. 1 lit. b), ust. 2 lit. b), ust. 3 lit. b), ust. 4 lit. b), ust. 5 lit. b) i ust. 6 lit. b).

3. Jednostka centralna ETIAS powiadamia Komisję o zakończeniu z powodzeniem okresu przejściowego, o którym mowa w art. 69.

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

Artykuł 72

Uruchomienie systemu

1. Komisja określa datę planowanego uruchomienia europejskiego portalu wyszukiwania w drodze aktów wykonawczych po tym, jeżeli spełnione zostaną następujące warunki:

a) przyjęto środki, o których mowa w art. 8 ust. 2, art. 9 ust. 7 i art. 43 ust. 5;

b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test europejskiego portalu wyszukiwania, który eu-LISA przeprowadziła we współpracy z organami państw członkowskich i agencjami unijnymi, które mogą korzystać z europejskiego portalu wyszukiwania;

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

Europejski portal wyszukiwania przeszukuje bazy danych Interpolu dopiero wówczas, gdy rozwiązania techniczne umożliwiają spełnienie wymogów art. 9 ust. 5. W wyniku niemożności spełnienia tego wymogu europejski portal wyszukiwania nie przeszukuje baz danych Interpolu, lecz nie powinien opóźniać rozpoczęcia funkcjonowania europejskiego portalu wyszukiwania.

Komisja wyznacza termin, o którym mowa w akapicie pierwszym, na jeden z dni w ciągu 30 dni od przyjęcia aktu wykonawczego.

2. Komisja decyduje o dacie planowanego uruchomienia wspólnego systemu porównywania danych biometrycznych po tym, jak spełnione zostaną następujące warunki:

a) przyjęto środki, o których mowa w art. 13 ust. 5 i art. 43 ust. 5;

b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test wspólnego systemu porównywania danych biometrycznych, który przeprowadziła we współpracy z organami państw członkowskich;

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

d) eu-LISA oświadczyła, że test, o którym mowa w ust. 5 lit. b), zakończył się pomyślnie.

Komisja wyznacza termin, o którym mowa w akapicie pierwszym, na jeden z dni w ciągu 30 dni od przyjęcia aktu wykonawczego.

3. Komisja decyduje o dacie planowanego uruchomienia wspólnego repozytorium danych umożliwiających identyfikację po tym, jak spełnione zostaną następujące warunki:

a) przyjęto środki, o których mowa w art. 43 ust. 5 i art. 78 ust. 10;

b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test wspólnego repozytorium danych umożliwiających identyfikację, który przeprowadziła we współpracy z organami państw członkowskich;

c) eu-LISA zatwierdziła uzgodnienia techniczne i prawne dotyczące zbierania i przekazywania danych, o których mowa w art. 18, oraz powiadomiła o nich Komisję;

d) eu-LISA oświadczyła, że test, o którym mowa w ust. 5 lit. b), zakończył się pomyślnie.

Komisja wyznacza termin, o którym mowa w akapicie pierwszym, na jeden z dni w ciągu 30 dni od przyjęcia aktu wykonawczego.

4. Komisja decyduje o dacie planowanego uruchomienia detektora wielokrotnych tożsamości po tym, jak spełnione zostaną następujące warunki:

a) przyjęto środki, o których mowa w art. 28 ust. 5 i 7, art. 33 ust. 6, art. 33 ust. 6, art. 43 ust. 5 i art. 49 ust. 6;

b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test detektora wielokrotnych tożsamości, który przeprowadziła we współpracy z organami państw członkowskich i jednostką centralną ETIAS;

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

d) jednostka centralna ETIAS powiadomiła Komisję zgodnie z art. 71 ust. 3;

e) eu-LISA oświadczyła, że testy, o których mowa w ust. 1 lit. b), ust. 2 lit. b), ust. 3 lit. b) i ust. 5 lit. b), zakończyły się pomyślnie.

Komisja wyznacza termin, o którym mowa w akapicie pierwszym, na jeden z dni w ciągu 30 dni od przyjęcia aktu wykonawczego.

5. Komisja określa – w drodze aktów wykonawczych – datę, od której mechanizmy i procedury automatycznej kontroli jakości danych, wspólne wskaźniki jakości danych i minimalne normy jakości danych mają być stosowane, gdy spełnione zostaną następujące warunki:

a) przyjęto środki, o których mowa w art. 37 ust. 4;

b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test mechanizmów i procedur automatycznej kontroli jakości danych, wspólnych wskaźników jakości danych i minimalnych norm jakości danych, który przeprowadziła we współpracy z organami państw członkowskich.

Komisja wyznacza termin, o którym mowa w akapicie pierwszym, na jeden z dni w ciągu 30 dni od przyjęcia aktu wykonawczego.

6. Komisja określa datę planowanego uruchomienia centralnego repozytorium sprawozdawczo-statystycznego po tym, jak spełnione zostaną następujące warunki:

a) przyjęto środki, o których mowa w art. 39 ust. 5 i art. 43 ust. 5;

b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test centralnego repozytorium sprawozdawczo-statystycznego, który przeprowadziła we współpracy z organami państw członkowskich;

c) eu-LISA zatwierdziła uzgodnienia techniczne i prawne dotyczące zbierania i przekazywania danych, o których mowa w art. 39 oraz powiadomiła o nich Komisję.

Komisja wyznacza termin, o którym mowa w akapicie pierwszym, na jeden z dni w ciągu 30 dni od przyjęcia aktu wykonawczego.

7. Komisja informuje Parlament Europejski i Radę o wynikach testów przeprowadzonych zgodnie z ust. 1 lit. b), ust. 2 lit. b), ust. 3 lit. b), ust. 4 lit. b), ust. 5 lit. b) i ust. 6 lit. b).

8. Państwa członkowskie, jednostka centralna ETIAS i Europol rozpoczynają korzystanie z każdego z elementów interoperacyjności od daty określonej przez Komisję zgodnie z odpowiednio ust. 1, 2, 3 i 4.

Artykuł 73

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 28 ust. 5, art. 39 ust. 5, art. 49 ust. 6, art. 67 ust. 2 i art. 69 ust. 8, powierza się Komisji na okres pięciu lat od dnia 11 czerwca 2019 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

3. Przekazanie uprawnień, o których mowa w art. 28 ust. 5, art. 39 ust. 5, art. 49 ust. 6, art. 67 ust. 2 i art. 69 ust. 8, może zostać odwołane w dowolnym momencie przez Parlament Europejski lub Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

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

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

6. Akt delegowany przyjęty na podstawie art. 28 ust. 5, art. 39 ust. 5, art. 49 ust. 6, art. 67 ust. 2 i art. 69 ust. 8 wchodzi w życie tylko wówczas, gdy Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 74

Procedura komitetowa

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

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

Jeżeli komitet nie wyda opinii, Komisja nie przyjmuje projektu aktu wykonawczego i stosuje się art. 5 ust. 4 akapit trzeci rozporządzenia (UE) nr 182/2011.

Artykuł 75

Grupa doradcza

eu-LISA ustanawia grupę doradczą ds. interoperacyjności. W fazie projektowania i rozwoju elementów interoperacyjności stosuje się przepisy art. 54 ust. 4, 5 i 6.

Artykuł 76

Szkolenia

eu-LISA wykonuje zadania związane z zapewnianiem szkoleń z zakresu technicznego użytkowania elementów interoperacyjności zgodnie z rozporządzeniem (UE) 2018/1726.

Organy państw członkowskich i agencje unijne zapewniają swojemu personelowi uprawnionemu do przetwarzania danych za pomocą elementów interoperacyjności odpowiedni program szkoleniowy dotyczący bezpieczeństwa danych, jakości danych, zasad ochrony danych, procedur mających zastosowanie do przetwarzania danych i obowiązku informowania na mocy art. 32 ust. 4, art. 33 ust. 4 i art. 47.

W stosowanych przypadkach wspólne szkolenia na te tematy organizuje się na szczeblu Unii w celu zacieśnienia współpracy i wymiany najlepszych praktyk między personelem organów państw członkowskich i agencji unijnych, które są uprawnione do przetwarzania danych przy pomocy elementów interoperacyjności. Szczególną uwagę należy zwrócić na proces wykrywania wielokrotnych tożsamości, w tym na ręczną weryfikację różniących się tożsamości i towarzyszącą temu potrzebę utrzymania odpowiednich zabezpieczeń praw podstawowych.

Artykuł 77

Praktyczny podręcznik

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

Artykuł 78

Monitorowanie i ocena

1. eu-LISA zapewnia wdrożenie procedur w zakresie monitorowania rozwoju elementów interoperacyjności i ich połączenia z jednolitymi interfejsami krajowymi pod kątem celów dotyczących planowania i kosztów oraz procedur w zakresie monitorowania funkcjonowania elementów interoperacyjności pod kątem celów w zakresie rezultatów technicznych, efektywności kosztowej, bezpieczeństwa i jakości działania.

2. Do dnia 12 grudnia 2019 r. i co sześć miesięcy od tego dnia w trakcie fazy rozwojowej elementów interoperacyjności eu-LISA przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie z aktualnej sytuacji w zakresie opracowywania każdego z elementów interoperacyjności, a także ich połączenia z jednolitymi interfejsami krajowymi. Po zakończeniu tworzenia systemu przekazuje się Parlamentowi Europejskiemu i Radzie sprawozdanie zawierające szczegółowe wyjaśnienia dotyczące sposobu osiągnięcia celów, w szczególności w zakresie planowania i kosztów, a także zawierające uzasadnienie rozbieżności.

3. Cztery lata po rozpoczęciu funkcjonowania poszczególnych elementów interoperacyjności zgodnie z art. 72, a następnie co cztery lata, eu-LISA przedkłada Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie dotyczące technicznego funkcjonowania elementów interoperacyjności, w tym ich bezpieczeństwa.

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

a) ocenę stosowania niniejszego rozporządzenia;

b) analizę osiągniętych wyników w stosunku do celów niniejszego rozporządzenia i ocenę wpływu na prawa podstawowe, w tym w szczególności ocenę wpływu elementów interoperacyjności na prawo do niedyskryminacji;

c) ocenę funkcjonowania portalu internetowego, w tym dane liczbowe dotyczące korzystania z portalu internetowego oraz liczby wniosków, które zostały rozpatrzone;

d) ocenę aktualności przesłanek do stworzenia elementów interoperacyjności;

e) ocenę bezpieczeństwa elementów interoperacyjności;

f) ocenę korzystania ze wspólnego repozytorium danych umożliwiających identyfikację do celów identyfikacji;

g) ocenę korzystania ze wspólnego repozytorium danych umożliwiających identyfikację w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywania ich lub prowadzenia w ich sprawie postępowań przygotowawczych;

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

i) ocenę przeszukiwania baz danych Interpolu za pośrednictwem europejskiego portalu wyszukiwania, w tym informacje na temat liczby dopasowań w bazach danych Interpolu i informacje na temat napotkanych problemów.

Ocena ogólna na mocy akapitu pierwszego niniejszego ustępu zawiera konieczne zalecenia. Komisja przekazuje powyższe sprawozdanie oceniające Parlamentowi Europejskiemu, Radzie, Europejskiemu Inspektorowi Danych Osobowych i Agencji Praw Podstawowych Unii Europejskiej.

5. Do dnia 12 czerwca 2020 r., a następnie co roku do czasu przyjęcia przez Komisję aktów wykonawczych, o których mowa w ust. 72, Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie o stanie przygotowań do pełnego wdrożenia niniejszego rozporządzenia. Sprawozdanie zawiera także szczegółowe informacje o poniesionych kosztach oraz informacje dotyczące rodzajów ryzyka, które mogą mieć wpływ na ogólne koszty.

6. Dwa lata po rozpoczęciu funkcjonowania detektora wielokrotnych tożsamości zgodnie z art. 72 ust. 4 Komisja bada wpływ detektora wielokrotnych tożsamości na prawo do niedyskryminacji. Po tym pierwszym sprawozdaniu badanie wpływu detektora wielokrotnych tożsamości na prawo do niedyskryminacji stanowi część badania, o którym mowa w ust. 4 lit. b) niniejszego artykułu.

7. Państwa członkowskie i Europol dostarczają eu-LISA i Komisji informacji niezbędnych do sporządzania sprawozdań, o których mowa w ust. 3-6. Informacje te nie mogą stwarzać zagrożenia dla metod pracy ani ujawniać informacji o źródłach, członkach personelu lub postępowaniach przygotowawczych prowadzonych przez wyznaczone organy.

8. eu-LISA przekazuje Komisji informacje niezbędne do sporządzenia oceny ogólnej, o której mowa w ust. 4.

9. Z poszanowaniem przepisów prawa krajowego dotyczących publikacji danych szczególnie chronionych i bez uszczerbku dla ograniczeń koniecznych do ochrony bezpieczeństwa i porządku publicznego, zapobiegania przestępstwom i zagwarantowania, aby żadne prowadzone krajowe postępowanie przygotowawcze nie było zagrożone, każde państwo członkowskie i Europol przygotowują coroczne sprawozdania na temat skuteczności dostępu do danych przechowywanych we wspólnym repozytorium danych umożliwiających identyfikację na potrzeby zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywania ich lub prowadzenia w ich sprawie postępowań przygotowawczych, zawierające informacje i dane statystyczne na temat:

a) dokładnego celu sprawdzania danych, w tym rodzaju przestępstw terrorystycznych lub innych poważnych przestępstw;

b) przedstawionych uzasadnionych podstaw zasadnego podejrzenia, że osoba podejrzana, sprawca lub ofiara są objęci zakresem rozporządzenia (UE) 2017/2226, rozporządzenia (WE) nr 767/2008 lub rozporządzenia (UE) 2018/1240;

c) liczby wniosków o dostęp do wspólnego repozytorium danych umożliwiających identyfikację na potrzeby zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, wykrywania tych przestępstw i prowadzenia postępowań przygotowawczych w ich sprawie;

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

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

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

10. Aby zarządzać wnioskami użytkowników o udzielenie dostępu, o których mowa w art. 22, oraz ułatwiać zbieranie informacji na podstawie ust. 7 i 9 niniejszego artykułu w celu generowania sprawozdań i statystyk, o których mowa w tych ustępach, państwom członkowskim udostępnia się rozwiązanie techniczne. Komisja przyjmuje akty wykonawcze określające specyfikacje rozwiązania technicznego. Akty te przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 79

Wejście w życie i stosowanie

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

Przepisy niniejszego rozporządzenia dotyczące europejskiego portalu wyszukiwania mają zastosowanie od dnia określonego przez Komisję zgodnie z art. 72 ust. 1.

Przepisy niniejszego rozporządzenia dotyczące wspólnego systemu porównywania danych biometrycznych mają zastosowanie od dnia określonego przez Komisję zgodnie z art. 72 ust. 2.

Przepisy niniejszego rozporządzenia dotyczące wspólnego repozytorium danych umożliwiających identyfikację mają zastosowanie od dnia określonego przez Komisję zgodnie z art. 72 ust. 3.

Przepisy niniejszego rozporządzenia dotyczące detektora wielokrotnych tożsamości mają zastosowanie od dnia określonego przez Komisję zgodnie z art. 72 ust. 4.

Przepisy niniejszego rozporządzenia dotyczące zautomatyzowanych mechanizmów i procedur kontroli jakości danych, wspólnych wskaźników jakości danych i minimalnych norm jakości danych mają zastosowanie od dnia określonego przez Komisję zgodnie z art. 72 ust. 5.

Przepisy niniejszego rozporządzenia dotyczące centralnego repozytorium sprawozdawczo-statystycznego mają zastosowanie od dnia określonego przez Komisję zgodnie z art. 72 ust. 6.

Art. 6, 12, 17, 25, 38, 42, 54, 56, 57, 70, 71, 73, 74, 75, 77 i art. 78 ust. 1 mają zastosowanie od dnia 11 czerwca 2019 r.

Niniejsze zastosowanie ma zastosowanie do Eurodac od dnia, w którym zaczyna obowiązywać rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 w wersji przekształconej.

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

Sporządzono w Brukseli dnia 20 maja 2019 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
A. TAJANI	G. CIAMBA
Przewodniczący	*Przewodniczący*