



ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2024/982

z dnia 13 marca 2024 r.

w sprawie zautomatyzowanego przeszukania danych i zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej oraz zmieniające decyzje Rady 2008/615/WSiSW i 2008/616/WSiSW oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1726, (UE) 2019/817 i (UE) 2019/818 (rozporządzenie Prüm II)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 ust. 2, art. 87 ust. 2 lit. a) oraz art. 88 ust. 2,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ⁽¹⁾,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ⁽²⁾,

a także mając na uwadze, co następuje:

- (1) Unia wyznaczyła sobie cel polegający na zapewnieniu swoim obywatelom przestrzeni wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych, w której zapewniony jest swobodny przepływ osób. Cel ten ma być osiągnięty, między innymi, za pomocą odpowiednich środków służących zapobieganiu przestępczości i innym zagrożeniom dla bezpieczeństwa publicznego – w tym przestępczości zorganizowanej i terroryzmowi – i ich zwalczaniu, zgodnie z komunikatem Komisji z dnia 24 lipca 2020 r. zatytułowanym „Strategia UE w zakresie unii bezpieczeństwa”. Mając na względzie ten cel, organy ścigania powinny wymieniać dane w sposób efektywny i terminowy, aby skutecznie zapobiegać przestępczości, wykrywać przestępstwa i prowadzić postępowania przygotowawcze w sprawach karnych.
- (2) Celem niniejszego rozporządzenia jest poprawa, usprawnienie i ułatwienie wymiany informacji kryminalnych i danych rejestracyjnych pojazdów w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych między właściwymi organami państw członkowskich, i między państwami członkowskimi a Agencją Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) ustanowioną rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794 ⁽³⁾, w pełnej zgodności z przepisami dotyczącymi praw podstawowych i ochrony danych.
- (3) Decyzje Rady 2008/615/WSiSW ⁽⁴⁾ i 2008/616/WSiSW ⁽⁵⁾, które ustanawiają zasady wymiany informacji między organami odpowiedzialnymi za zapobieganie przestępczości i prowadzenie postępowań przygotowawczych w sprawach karnych przez umożliwienie zautomatyzowanego przekazywania profili DNA, danych daktyloskopijnych i niektórych danych rejestracyjnych pojazdów, okazały się istotne w zwalczaniu terroryzmu i przestępczości transgranicznej, a tym samym dla ochrony bezpieczeństwa wewnętrznego Unii i jej obywateli.
- (4) Bazując na obecnych procedurach zautomatyzowanego przeszukania danych, w niniejszym rozporządzeniu określa się warunki i procedury zautomatyzowanego przeszukania i wymiany profili DNA, danych daktyloskopijnych, niektórych danych rejestracyjnych pojazdów, wizerunków twarzy i informacji z rejestrów policyjnych. Powinno to pozostać bez uszczerbku dla przetwarzania takich danych w Systemie Informacyjnym Schengen (SIS), wymiany

⁽¹⁾ Dz.U. C 323 z 26.8.2022, s. 69.

⁽²⁾ Stanowisko Parlamentu Europejskiego z dnia 8 lutego 2024 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 26 lutego 2024 r.

⁽³⁾ 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).

⁽⁴⁾ Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 1).

⁽⁵⁾ Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (Dz.U. L 210 z 6.8.2008, s. 12).

informacji uzupełniających związanych z takimi danymi za pośrednictwem biur SIRENE na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1862 ⁽⁶⁾ lub dla praw osób, których dane są w nich przetwarzane.

- (5) W niniejszym rozporządzeniu ustanawia się ramy wymiany informacji między organami odpowiedzialnymi za zapobieganie przestępczości, wykrywanie przestępstw i prowadzenie postępowań przygotowawczych w sprawach karnych (zwane dalej „ramami z Prüm II”). Zgodnie z art. 87 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) obejmuje ono wszystkie właściwe organy państw członkowskich, w tym między innymi policję, służby celne i inne wyspecjalizowane organy ścigania w zakresie zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych. W związku z tym w kontekście niniejszego rozporządzenia każdy organ, który jest odpowiedzialny za zarządzanie krajową bazą danych objętą niniejszym rozporządzeniem lub który udziela zgody na udostępnienie wszelkich danych, należy uznać za objęty zakresem stosowania niniejszego rozporządzenia, o ile informacje są wymieniane w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych.
- (6) Wszelkie przetwarzanie lub wymiana danych osobowych do celów niniejszego rozporządzenia nie powinny prowadzić do dyskryminacji osób z jakichkolwiek względów. Powinny się one odbywać z pełnym poszanowaniem godności ludzkiej i integralności osoby oraz innych praw podstawowych, w tym prawa do poszanowania życia prywatnego i do ochrony danych osobowych, zgodnie z Kartą praw podstawowych Unii Europejskiej.
- (7) Wszelkie przetwarzanie lub wymiana danych osobowych powinny podlegać przepisom o ochronie danych zawartym w rozdziale 6 niniejszego rozporządzenia, a w stosownych przypadkach – przepisom dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ⁽⁷⁾ lub rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ⁽⁸⁾, rozporządzenia (UE) 2016/794 lub rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ⁽⁹⁾. Dyrektywa (UE) 2016/680 ma zastosowanie do korzystania z ram z Prüm II w odniesieniu do poszukiwania osób zaginionych i identyfikacji niezidentyfikowanych szczątków ludzkich w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych. Rozporządzenie (UE) 2016/679 ma zastosowanie do korzystania z ram z Prüm II do poszukiwania osób zaginionych i identyfikacji niezidentyfikowanych szczątków ludzkich do innych celów.
- (8) Przewidując zautomatyzowane przeszukanie profili DNA, danych daktyloskopijnych, niektórych danych rejestracyjnych pojazdów, wizerunków twarzy i informacji z rejestrów policyjnych, jako cel niniejszego rozporządzenia ustanowiono również umożliwienie poszukiwania osób zaginionych i identyfikację niezidentyfikowanych szczątków ludzkich. To zautomatyzowane przeszukanie powinno odbywać się zgodnie z zasadami i procedurami określonymi w niniejszym rozporządzeniu. To zautomatyzowane przeszukanie pozostaje bez uszczerbku dla wprowadzania do SIS wpisów dotyczących osób zaginionych oraz wymiany informacji uzupełniających dotyczących takich wpisów na podstawie rozporządzenia (UE) 2018/1862.
- (9) W przypadku gdy państwa członkowskie chcą korzystać z ram z Prüm II do poszukiwania osób zaginionych i identyfikowania szczątków ludzkich, powinny one przyjąć krajowe środki ustawodawcze wyznaczające właściwe w tym celu organy krajowe oraz określające szczegółowe procedury, warunki i kryteria w tym zakresie. W przypadku poszukiwania osób zaginionych poza obszarem postępowań przygotowawczych w sprawach karnych krajowe środki ustawodawcze powinny jasno określać względy humanitarne, dla których można przeprowadzić poszukiwa-

⁽⁶⁾ 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).

⁽⁷⁾ 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

⁽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).

⁽⁹⁾ 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).

nie osób zaginionych. Takie poszukiwania powinny być zgodne z zasadą proporcjonalności. Względy humanitarne powinny obejmować klęski żywiołowe i katastrofy spowodowane przez człowieka oraz inne równie uzasadnione względy, takie jak podejrzenie samobójstwa.

- (10) W niniejszym rozporządzeniu określa się warunki i procedury zautomatyzowanego przeszukania profili DNA, danych daktyloskopijnych, niektórych danych rejestracyjnych pojazdów, wizerunków twarzy i informacji z rejestrów policyjnych oraz zasady dotyczące wymiany danych podstawowych po ustaleniu potwierzonego dopasowania danych biometrycznych. Rozporządzenie to nie ma zastosowania do wymiany informacji uzupełniających wykraczających poza jego zakres, która jest regulowana dyrektywą Parlamentu Europejskiego i Rady (UE) 2023/977 ⁽¹⁰⁾.
- (11) Dyrektywa (UE) 2023/977 stanowi spójne unijne ramy prawne w celu zapewnienia właściwym organom państwa członkowskiego równoważnego dostępu do informacji będących w posiadaniu innych państw członkowskich, gdy potrzebują one takich informacji do zwalczania przestępczości i terroryzmu. Aby usprawnić wymianę informacji, w dyrektywie tej formalizuje się i wyjaśnia zasady i procedury wymiany informacji między właściwymi organami państw członkowskich, w szczególności do celów dochodzeniowo-śledczych, w tym znaczenie „pojedynczego punktu kontaktowego” każdego państwa członkowskiego dla takiej wymiany.
- (12) Cele wymiany profili DNA na podstawie niniejszego rozporządzenia pozostają bez uszczerbku dla wyłącznej kompetencji państw członkowskich do decydowania o celu krajowych baz danych DNA, w tym o zapobieganiu przestępczości lub wykrywaniu przestępstw.
- (13) Państwa członkowskie powinny, w momencie początkowego połączenia z routerem ustanowionym w niniejszym rozporządzeniu, przeprowadzać zautomatyzowane przeszukanie profili DNA przez porównanie wszystkich profili DNA przechowywanych w swoich bazach danych ze wszystkimi profilami DNA przechowywanymi w bazach danych wszystkich pozostałych państw członkowskich i danymi Europolu. Celem tego początkowego zautomatyzowanego przeszukania jest niedopuszczenie do luk w identyfikowaniu dopasowań między profilami DNA przechowywanymi w bazie danych tego państwa członkowskiego a tymi przechowywanymi w bazach danych wszystkich innych państw członkowskich i danymi Europolu. Początkowe zautomatyzowane przeszukanie powinno być przeprowadzane dwustronnie i nie musi być prowadzone równocześnie z bazami danych wszystkich pozostałych państw członkowskich i danymi Europolu. Ustalenia dla przeprowadzania takich przeszukań, w tym harmonogram i wielkość partii profili, należy uzgodnić dwustronnie zgodnie z zasadami i procedurami określonymi w niniejszym rozporządzeniu.
- (14) Po zautomatyzowanym przeszukaniu profili DNA państwa członkowskie powinny przeprowadzać zautomatyzowane przeszukania przez porównanie wszystkich nowych profili DNA dodanych do ich bazy danych DNA ze wszystkimi profilami DNA przechowywanymi w bazach danych wszystkich pozostałych państw członkowskich i danymi Europolu. Takie zautomatyzowane przeszukiwanie nowych profili DNA powinno odbywać się regularnie. W przypadku gdy takie przeszukiwanie nie mogłyby zostać przeprowadzone, zainteresowane państwo członkowskie powinno mieć możliwość ich przeprowadzenia na późniejszym etapie, aby upewnić się, że nie pominięto dopasowań. Ustalenia dotyczące przeprowadzania takich późniejszych przeszukań, w tym harmonogram i wielkość partii profili, należy uzgodnić dwustronnie, zgodnie z zasadami i procedurami określonymi w niniejszym rozporządzeniu.
- (15) Do celów zautomatyzowanego przeszukania danych rejestracyjnych pojazdów państwa członkowskie i Europol powinny korzystać ze specjalnie zaprojektowanego do tego celu europejskiego systemu informacji o pojazdach i prawach jazdy (Eucaris) utworzonego na mocy Traktatu dotyczącego europejskiego systemu informacji o pojazdach i prawach jazdy (EUCARIS) i łączącego wszystkie uczestniczące państwa członkowskie w sieć. Nie ma potrzeby użycia centralnego komponentu w celu nawiązania łączności, ponieważ każde państwo członkowskie komunikuje się bezpośrednio z pozostałymi połączonymi państwami członkowskimi, a Europol komunikuje się bezpośrednio z połączonymi bazami danych.
- (16) Identyfikacja przestępcy ma zasadnicze znaczenie dla skutecznego ścigania przestępstw i prowadzenia postępowań przygotowawczych. Zautomatyzowane przeszukiwanie zgromadzonych zgodnie z prawem krajowym wizerunków twarzy osób skazanych za przestępstwo lub podejrzanych o popełnienie takiego przestępstwa, lub, jeśli jest dozwolone na mocy prawa krajowego odpytywanego państwa członkowskiego ofiar przestępstwa, może dostarczyć dodatkowych informacji umożliwiających skuteczną identyfikację przestępców i zwalczanie przestępczości. Biorąc

⁽¹⁰⁾ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/977 z dnia 10 maja 2023 r. w sprawie wymiany informacji między organami ścigania państw członkowskich i uchylająca decyzję ramową Rady 2006/960/WSiSW (Dz.U. L 134 z 22.5.2023, s. 1).

pod uwagę wrażliwość odpowiednich danych, zautomatyzowane przeszukiwanie powinno być możliwe wyłącznie w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych, gdzie kara maksymalna wynosi co najmniej jeden rok pozbawienia wolności na mocy prawa pytającego państwa członkowskiego.

- (17) Zautomatyzowane przeszukiwanie danych biometrycznych przez właściwe organy państw członkowskich odpowiedzialne za zapobieganie przestępczości, wykrywanie przestępstw i prowadzenie postępowań przygotowawczych w sprawach karnych na podstawie niniejszego rozporządzenia powinno dotyczyć wyłącznie danych zawartych w bazach danych utworzonych w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych.
- (18) Udział w zautomatyzowanym przeszukaniu i wymianie informacji z rejestrów policyjnych powinien pozostać dobrowolny. W przypadku gdy państwa członkowskie zdecydują się na udział, powinny mieć one jedynie możliwość dokonywania, w duchu wzajemności, kwerend w bazach danych innych państw członkowskich, jeżeli nie udostępniają własnych danych do celów kwerend innych państw członkowskich. Uczestniczące państwa członkowskie powinny utworzyć indeksy krajowego rejestru policyjnego. Państwa członkowskie powinny móc zdecydować, z których krajowych baz danych ustanowionych do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych skorzystają w celu stworzenia własnych indeksów krajowych rejestrów policyjnych. Indeksy te obejmują dane z krajowych baz danych, które policja zazwyczaj sprawdza, gdy otrzymuje zapytania o informacje od innych organów ścigania. W niniejszym rozporządzeniu ustanawia się europejski system przekazywania informacji z rejestrów policyjnych (EPRIS) zgodnie z zasadą uwzględniania ochrony prywatności już w fazie projektowania. Zabezpieczenia ochrony danych obejmują pseudonimizację, ponieważ indeksy i kwerendy nie zawierają jednoznacznych danych osobowych, lecz ciągi alfanumeryczne. Istotne jest, aby EPRIS uniemożliwiał państwom członkowskim lub Europolowi odwrócenie pseudonimizacji i ujawnienie danych identyfikacyjnych, na podstawie których uzyskano dopasowanie. Biorąc pod uwagę wrażliwość przedmiotowych danych, wymiany indeksów krajowego rejestru policyjnego na mocy niniejszego rozporządzenia powinna dotyczyć wyłącznie danych osób skazanych za popełnienie przestępstwa lub podejrzanych o jego popełnienie. Ponadto zautomatyzowane przeszukiwanie indeksów krajowego rejestru policyjnego powinno być możliwe wyłącznie w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych, gdzie kara maksymalna wynosi co najmniej jeden rok pozbawienia wolności na mocy prawa pytającego państwa członkowskiego.
- (19) Wymiana informacji z rejestrów policyjnych na mocy niniejszego rozporządzenia nie narusza wymiany danych w ramach istniejącego europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), ustanowionego decyzją ramową Rady 2009/315/WSiSW⁽¹¹⁾.
- (20) W ostatnich latach Europol otrzymał od organów państw trzecich, zgodnie z rozporządzeniem (UE) 2016/794, dużą ilość danych biometrycznych podejrzanych i osób skazanych za terroryzm i przestępstwa, w tym informacje z pola walki z obszarów objętych działaniami wojennymi. W wielu przypadkach pełne wykorzystanie takich danych nie było możliwe, ponieważ nie zawsze są one dostępne dla właściwych organów państw członkowskich. Włączenie danych dostarczonych przez państwa trzecie i przechowywanych w Europol do ram z Prüm II, a tym samym udostępnienie tych danych właściwym organom państw członkowskich, zgodnie z rolą Europolu jako naczelnego unijnego centrum informacji o przestępstwach, jest konieczne do lepszego zapobiegania poważnej przestępczości, wykrywania poważnych przestępstw i prowadzenia postępowań przygotowawczych w ich sprawie. Przyczynia się ono również do tworzenia synergii między różnymi narzędziami egzekwowania prawa i gwarantuje wykorzystywanie danych w najbardziej efektywny sposób.
- (21) Na mocy ram z Prüm II Europol powinien mieć możliwość przeszukania baz danych państw członkowskich z wykorzystaniem danych otrzymanych od organów państw trzecich, przy pełnym poszanowaniu przepisów i warunków przewidzianych w rozporządzeniu (UE) 2016/794, w celu ustalenia transgranicznych powiązań między sprawami karnymi, w których właściwy jest Europol. Możliwość korzystania przez Europol z danych Prüm, obok innych dostępnych baz danych, pozwoliłaby na przeprowadzenie pełniejszej i dogłębniejszej analizy, umożliwiając tym samym Europolowi udzielanie lepszego wsparcia właściwym organom państw członkowskich w zakresie zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych.

⁽¹¹⁾ Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji (Dz.U. L 93 z 7.4.2009, s. 23).

- (22) Europol powinien zapewnić, aby jego zapytania dotyczące przeszukania nie przekraczały określonych przez państwa członkowskie możliwości przeszukania w odniesieniu do danych daktyloskopijnych i wizerunków twarzy. W przypadku stwierdzenia dopasowania między danymi wykorzystanymi do przeszukania a danymi przechowywanymi w bazach danych państw członkowskich, państwa członkowskie powinny móc podjąć decyzję o przekazaniu Europolowi informacji niezbędnych do wykonywania jego zadań.
- (23) Rozporządzenie (UE) 2016/794 ma w całości zastosowanie do udziału Europolu w ramach z Prüm II. Wszelkie wykorzystanie przez Europol danych otrzymanych od państw trzecich podlega art. 19 rozporządzenia (UE) 2016/794. Na wszelkie wykorzystanie przez Europol danych uzyskanych ze zautomatyzowanych przeszukiwań na mocy ram z Prüm II powinno wydać zgodę państwo członkowskie, które dostarczyło dane, a w przypadku gdy dane są przekazywane państwu trzecim wykorzystanie takie powinno podlegać art. 25 rozporządzenia (UE) 2016/794.
- (24) Decyzje 2008/615/WSiSW i 2008/616/WSiSW przewidują sieć dwustronnych połączeń między krajowymi bazami danych państw członkowskich. W rezultacie tej architektury technicznej każde państwo członkowskie musiało utworzyć połączenie z każdym państwem członkowskim uczestniczącym w wymianie, co oznaczało co najmniej 26 połączeń na państwo członkowskie, dla każdej kategorii danych. Router i EPRIIS uproszcza architekturę techniczną przewidzianą w ramach z Prüm i będą służyć jako punkty łączące wszystkie państwa członkowskie. Router powinien wymagać jednego podłączenia na państwo członkowskie w odniesieniu do danych biometrycznych. EPRIIS powinien wymagać jednego podłączenia na uczestniczące państwo członkowskie w odniesieniu do rejestrów policyjnych.
- (25) Router powinien być połączony z europejskim portalem wyszukiwania ustanowionym w rozporządzeniach Parlamentu Europejskiego i Rady (UE) 2019/817 ⁽¹²⁾ oraz (UE) 2019/818 ⁽¹³⁾, aby umożliwić właściwym organom państw członkowskich i Europolowi uruchamianie kwerend w krajowych bazach danych na podstawie niniejszego rozporządzenia jednocześnie z kwerendami we wspólnym repozytorium danych umożliwiających identyfikację, ustanowionym na mocy tych rozporządzeń, na potrzeby ochrony porządku publicznego zgodnie z tymi rozporządzeniami. W związku z tym te rozporządzenia należy odpowiednio zmienić. Ponadto należy zmienić rozporządzenie (UE) 2019/818, aby umożliwić przechowywanie sprawozdań i statystyk dotyczących routera w centralnym repozytorium sprawozdawczo-statystycznym.
- (26) Powinno być możliwe, aby oznaczeniem referencyjnymi dla danych biometrycznych było tymczasowe oznaczenie referencyjne lub numer kontrolny transakcji.
- (27) Zautomatyzowane systemy identyfikacji daktyloskopijnej i systemy rozpoznawania wizerunku twarzy korzystają z wzorców biometrycznych zawierających dane uzyskane w wyniku ekstrakcji cech z rzeczywistych próbek biometrycznych. Wzorce biometryczne powinno się uzyskiwać z danych biometrycznych, ale nie powinno być możliwe uzyskanie tych samych danych biometrycznych z wzorców biometrycznych.
- (28) W przypadku gdy tak zdecyduje pytające państwo członkowskie i w przypadkach stosownych do rodzaju danych biometrycznych, router powinien uszeregować odpowiedzi od odpytywanego państwa członkowskiego lub odpytywanych państw członkowskich lub Europolu poprzez porównanie danych biometrycznych wykorzystanych do kwerend z danymi biometrycznymi przekazanymi w odpowiedziach odpytywanego państwa członkowskiego lub odpytywanych państw członkowskich lub Europolu.
- (29) W przypadku stwierdzenia dopasowania między danymi wykorzystanymi do przeszukania a danymi przechowywanymi w krajowej bazie danych odpytywanego państwa członkowskiego lub odpytywanych państw członkowskich, po ręcznym potwierdzeniu dopasowania przez odpowiednio wykwalifikowanego pracownika pytającego państwa członkowskiego i po przekazaniu opisu faktów i wskazaniu przestępstwa, które jest podstawą zapytania i znajduje się we wspólnej tabeli kategorii przestępstw, określonej w akcie wykonawczym, który ma zostać przyjęty na mocy decyzji ramowej 2009/315/WSiSW, odpytywane państwo członkowskie, powinno w ciągu 48 godzin odesłać za pośrednictwem routera ograniczony zbiór danych podstawowych, o ile takie dane podstawowe są dostępne. Ograni-

⁽¹²⁾ 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).

⁽¹³⁾ 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).

czony zbiór danych podstawowych powinien zostać odesłany za pośrednictwem routera, chyba że na mocy prawa krajowego wymagana jest zgoda organu sądowego, w ciągu 48 godzin od spełnienia odpowiednich warunków. Termin ten zapewni szybką wymianę informacji między właściwymi organami państw członkowskich. Państwa członkowskie powinny zachować kontrolę nad udostępnianiem ograniczonego zbioru danych podstawowych. Należy utrzymać interwencję ludzką na kluczowych etapach procesu, w tym w odniesieniu do decyzji o uruchomieniu kwerendy, decyzji o potwierdzeniu dopasowania, decyzji o złożeniu zapytania w celu otrzymania zbioru danych podstawowych po potwierdzeniu dopasowania oraz w odniesieniu do decyzji o udostępnieniu danych osobowych pytającemu państwu członkowskiemu, aby zapewnić, aby nie doszło do zautomatyzowanej wymiany danych podstawowych.

- (30) W konkretnym przypadku DNA odpytywane państwo członkowskie, powinno również móc potwierdzić dopasowanie dwóch profili DNA, o ile jest to istotne do celów prowadzenia postępowań przygotowawczych w sprawach karnych. Po potwierdzeniu takiego dopasowania przez odpytywane państwo członkowskie oraz po przekazaniu opisu faktów i wskazaniu przestępstwa, które jest podstawą zapytania i znajduje się we wspólnej tabeli kategorii przestępstw, określonej w akcie wykonawczym, który ma zostać przyjęty na mocy decyzji ramowej Rady 2009/315/WSiSW, pytające państwo członkowskie powinno odesłać za pośrednictwem routera ograniczony zbiór danych podstawowych w ciągu 48 godzin od spełnienia odpowiednich warunków, chyba że na mocy prawa krajowego wymagana jest zgoda organu sądowego.
- (31) Dane dostarczone i otrzymane na mocy niniejszego rozporządzenia podlegają terminom przechowywania i przeglądu ustanowionym zgodnie z dyrektywą (UE) 2016/680.
- (32) Przy opracowywaniu routera i EPRIIS należy, o ile ma to zastosowanie, należy stosować standard uniwersalnego formatu wiadomości (UMF). W każdej zautomatyzowanej wymianie danych na podstawie niniejszego rozporządzenia należy, o ile ma to zastosowanie, stosować standard UMF. Zachęca się również właściwe organy państw członkowskich i Europol do stosowania standardu UMF w odniesieniu do wszelkiej dalszej wymiany danych między nimi w kontekście ram z Prüm II. Standard UMF powinien stanowić standard dla uporządkowanej, transgranicznej wymiany informacji między systemami informacyjnymi, organami lub organizacjami działającymi w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych.
- (33) Na podstawie ram z Prüm II należy wymieniać wyłącznie informacje jawne.
- (34) Każde państwo członkowskie powinno poinformować inne państwa członkowskie, Komisję, Agencję Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) ustanowioną rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1726 ⁽¹⁴⁾ oraz Europol, o treści swoich krajowych baz danych udostępnionych za pośrednictwem ram z Prüm II i o warunkach zautomatyzowanego przeszukania.
- (35) Niektóre aspekty ram z Prüm II nie mogą zostać wyczerpująco ujęte w niniejszym rozporządzeniu z uwagi na ich techniczny charakter, wysoki poziom szczegółowości i potrzebę regularnej aktualizacji. Aspekty te obejmują na przykład ustalenia i specyfikacje techniczne dotyczące procedur zautomatyzowanego przeszukania, norm wymiany danych, w tym minimalnych norm jakości, oraz elementów danych podlegających wymianie. W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia w odniesieniu do takich aspektów należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ⁽¹⁵⁾.
- (36) Jakość danych ma ogromne znaczenie jako zabezpieczenie i niezbędny warunek wstępny zapewnienia skuteczności niniejszego rozporządzenia. W kontekście zautomatyzowanego przeszukania danych biometrycznych oraz w celu zapewnienia dostatecznej jakości przekazywanych danych i ograniczenia przypadków dopasowań fałszywie pozytywnych, należy ustanowić minimalne standardy jakościowe i regularnie poddawać je przeglądowi.

⁽¹⁴⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia (UE) nr 1077/2011 (Dz.U. L 295 z 21.11.2018, s. 99).

⁽¹⁵⁾ 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).

- (37) Biorąc pod uwagę skalę i wrażliwość danych osobowych wymienianych do celów niniejszego rozporządzenia oraz istnienie różnych przepisów krajowych dotyczących przechowywania informacji na temat osób fizycznych w krajowych bazach danych, ważne jest zapewnienie, aby bazy danych wykorzystywane do zautomatyzowanego przeszukiwania na podstawie niniejszego rozporządzenia były tworzone zgodnie z prawem krajowym oraz z dyrektywą (UE) 2016/680. Dlatego przed połączeniem krajowych baz danych z routerem lub EPRIS państwa członkowskie powinny przeprowadzić ocenę skutków dla ochrony danych, o której mowa w dyrektywie (UE) 2016/680, i w stosownych przypadkach skonsultować się z organem nadzorczym przewidzianym w tej dyrektywie.
- (38) Państwa członkowskie i Europol powinny zapewniać prawidłowość i stosowność danych osobowych przetwarzanych na podstawie niniejszego rozporządzenia. W przypadku gdy państwo członkowskie lub Europol uzyskają wiedzę, że dane, które dostarczono, są nieścisłe, lub nieaktualne, lub są danymi, których nie należało dostarczyć, bez zbędnej zwłoki powiadamiają one o tym odpowiednio państwo członkowskie, które otrzymało dane, lub Europol. Wszystkie zainteresowane państwa członkowskie lub Europol, w zależności od przypadku, powinny korygować lub usuwać dane odpowiednio i bez zbędnej zwłoki. W przypadku gdy państwo członkowskie, które otrzymało dane, lub Europol mają podstawy, by przypuszczać, że otrzymane dane są nieścisłe lub powinny zostać usunięte, powinno ono poinformować o tym bez zbędnej zwłoki państwo członkowskie, które przekazało dane.
- (39) Ścisłe monitorowanie wdrażania niniejszego rozporządzenia ma ogromne znaczenie. W szczególności przestrzeganie przepisów dotyczących przetwarzania danych osobowych powinno podlegać skutecznym zabezpieczeniom oraz należy zapewnić regularne monitorowanie i kontrolę ze strony administratorów danych, organów nadzorczych i Europejskiego Inspektora Ochrony Danych, stosownie do przypadku. Należy wprowadzić także przepisy umożliwiające regularne sprawdzanie dopuszczalności kwerend i zgodności przetwarzania danych z prawem.
- (40) Organy nadzorcze i Europejski Inspektor Ochrony Danych powinni zapewnić skoordynowany nadzór nad stosowaniem niniejszego rozporządzenia w ramach swoich obowiązków, w szczególności w przypadku stwierdzenia poważnych rozbieżności między praktykami państw członkowskich lub potencjalnie niezgodnego z prawem przekazywania danych.
- (41) Przy wdrażaniu niniejszego rozporządzenia istotne jest, aby państwa członkowskie i Europol uwzględniły orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej w odniesieniu do wymiany danych biometrycznych.
- (42) Trzy lata po rozpoczęciu eksploatacji routera i EPRIS, a następnie co cztery lata, Komisja powinna sporządzać sprawozdanie oceniające, które zawiera ocenę stosowania niniejszego rozporządzenia przez państwa członkowskie i Europol, w szczególności ocenę przestrzegania przez nie odpowiednich zabezpieczeń w zakresie ochrony danych. Sprawozdania oceniające powinny również zawierać analizę osiągniętych wyników w odniesieniu do celów niniejszego rozporządzenia i jego wpływu na prawa podstawowe. Sprawozdania oceniające powinny również oceniać wpływ, skuteczność, efektywność, bezpieczeństwo i metody pracy ram z Prüm II.
- (43) Ponieważ niniejsze rozporządzenie przewiduje ustanowienie nowych ram z Prüm, należy uchylić przepisy decyzji 2008/615/WSiSW i 2008/616/WSiSW, które nie są już stosowne. Należy odpowiednio zmienić te decyzje.
- (44) Ponieważ router ma zostać opracowany i być zarządzany przez eu-LISA, rozporządzenie (UE) 2018/1726 powinno zostać zmienione poprzez dodanie tego zadania do zadań eu-LISA.
- (45) Ponieważ cele niniejszego rozporządzenia, mianowicie zacieśnienie transgranicznej współpracy policyjnej oraz umożliwienie właściwym organom państw członkowskich prowadzenia poszukiwań osób zaginionych i identyfikacji niezidentyfikowanych szczątków ludzkich, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki działań możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania 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 tych celów.

- (46) 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.
- (47) Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do TUE i do TFUE, Irlandia powiadomiła o chęci uczestniczenia w przyjęciu i stosowaniu niniejszego rozporządzenia.
- (48) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 2 marca 2022 r. ⁽¹⁶⁾,

PRZYMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ 1

Przepisy ogólne

Artykuł 1

Przedmiot

Niniejszym rozporządzeniem ustanawia się ramy przeszukania i wymiany informacji między właściwymi organami państw członkowskich (zwane dalej „ramami z Prüm II”), określając:

- a) warunki i procedury zautomatyzowanego przeszukania profili DNA, danych daktyloskopijnych, niektórych danych rejestracyjnych pojazdów, wizerunków twarzy i informacji z rejestrów policyjnych, oraz
- b) reguły dotyczące wymiany danych podstawowych po stwierdzeniu potwierdzonego dopasowania danych biometrycznych.

Artykuł 2

Cel

Celem ram z Prüm II jest zacieśnienie współpracy transgranicznej w sprawach objętych częścią III tytuł V rozdział 4 i 5 Traktatu o funkcjonowaniu Unii Europejskiej, w szczególności dzięki ułatwianiu wymiany informacji między właściwymi organami państw członkowskich, przy pełnym poszanowaniu praw podstawowych osób fizycznych, w tym prawa do poszanowania życia prywatnego i prawa do ochrony danych osobowych, zgodnie z Kartą praw podstawowych Unii Europejskiej.

Ponadto celem ram z Prüm II jest umożliwienie właściwym organom państw członkowskich prowadzenia poszukiwań osób zaginionych w kontekście postępowań przygotowawczych w sprawach karnych lub ze względów humanitarnych oraz w celu identyfikacji niezidentyfikowanych szczątków ludzkich, zgodnie z art. 29, pod warunkiem że organy te zostały upoważnione do prowadzenia takich poszukiwań i przeprowadzania takich identyfikacji na mocy prawa krajowego.

Artykuł 3

Zakres stosowania

Niniejsze rozporządzenie ma zastosowanie do baz danych, ustanowionych zgodnie z prawem krajowym i wykorzystywanych do zautomatyzowanego przekazywania profili DNA, danych daktyloskopijnych, niektórych danych rejestracyjnych pojazdów, wizerunków twarzy i informacji z rejestrów policyjnych, zgodnie z – stosownie do przypadku – dyrektywą (UE) 2016/680 lub rozporządzeniem (UE) 2018/1725, (UE) 2016/794 lub (UE) 2016/679.

⁽¹⁶⁾ Dz.U. C 225 z 9.6.2022, s. 6.

Artykuł 4

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

- 1) „loci” (liczba pojedyncza: „locus”) oznaczają miejsca DNA, które zawierają charakterystyczne cechy identyfikacyjne analizowanej próbki ludzkiego DNA;
- 2) „profil DNA” oznacza kod literowy lub numeryczny reprezentujący zestaw loci lub szczególną strukturę molekularną w różnych loci;
- 3) „dane referencyjne DNA” oznaczają profil DNA oraz oznaczenie referencyjne, o którym mowa w art. 7;
- 4) „zidentyfikowany profil DNA” oznacza profil DNA pochodzący od zidentyfikowanej osoby;
- 5) „niezidentyfikowany profil DNA” oznacza profil DNA zebrany podczas prowadzenia postępowania przygotowawczego w sprawie karnej i należący do dotychczas niezidentyfikowanej osoby, w tym profil DNA uzyskany ze śladów;
- 6) „dane daktyloskopijne” oznaczają obrazy odbitek linii papilarnych palców, obrazy śladów palców, obrazy odbitek dłoni, obrazy śladów dłoni oraz wzory takich obrazów (zakodowane minucje), które są przechowywane i przetwarzane w zautomatyzowanej bazie danych;
- 7) „daktyloskopijne dane referencyjne” oznaczają dane daktyloskopijne i oznaczenie referencyjne, o których mowa w art. 12;
- 8) „niezidentyfikowane dane daktyloskopijne” oznaczają dane daktyloskopijne zebrane podczas prowadzenia postępowania przygotowawczego w sprawie karnej i należące do dotychczas niezidentyfikowanej osoby, w tym dane daktyloskopijne uzyskane ze śladów;
- 9) „zidentyfikowane dane daktyloskopijne” oznaczają dane daktyloskopijne zidentyfikowanej osoby;
- 10) „indywidualna sprawa” oznacza pojedyncze akta związane z zapobieganiem przestępczości, wykrywaniem przestępstw lub prowadzeniem postępowań przygotowawczych w sprawach karnych, z poszukiwaniem osoby zaginionej lub z identyfikacją niezidentyfikowanych szczątków ludzkich;
- 11) „wizerunek twarzy” oznacza cyfrowy wizerunek twarzy;
- 12) „dane referencyjne wizerunku twarzy” oznaczają wizerunek twarzy oraz oznaczenie referencyjne, o którym mowa w art. 21;
- 13) „niezidentyfikowany wizerunek twarzy” oznacza wizerunek twarzy zebrany podczas prowadzenia postępowania przygotowawczego w sprawie karnej, należący do dotychczas niezidentyfikowanej osoby, w tym wizerunek twarzy uzyskany ze śladów;
- 14) „zidentyfikowany wizerunek twarzy” oznacza wizerunek twarzy zidentyfikowanej osoby;
- 15) „dane biometryczne” oznaczają profile DNA, dane daktyloskopijne lub wizerunki twarzy;
- 16) „dane alfanumeryczne” oznaczają dane wyrażone literami, cyframi, znakami specjalnymi, odstępami i znakami przestankowymi;
- 17) „dopasowanie” oznacza istnienie zgodności ustalone w wyniku zautomatyzowanego porównania danych osobowych przetrzymywanych w bazie danych;
- 18) „kandydat” oznacza dane, z którymi stwierdzono dopasowanie;
- 19) „pytające państwo członkowskie” oznacza państwo członkowskie, które przeprowadza przeszukanie za pośrednictwem ram z Prüm II;
- 20) „odpytywane państwo członkowskie” oznacza państwo członkowskie, w którego bazach danych pytające państwo członkowskie przeprowadza przeszukanie za pośrednictwem ram z Prüm II;

- 21) „rejesty policyjne” oznaczają dane biograficzne osób podejrzanych i skazanych dostępne w krajowych bazach danych ustanowionych do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych;
- 22) „pseudonimizacja” oznacza pseudonimizację zdefiniowaną w art. 3 pkt 5 dyrektywy (UE) 2016/680;
- 23) „podejrzany” oznacza osobę, o której mowa w art. 6 lit. a) dyrektywy (UE) 2016/680;
- 24) „dane osobowe” oznaczają dane osobowe zdefiniowane w art. 3 pkt 1 dyrektywy (UE) 2016/680;
- 25) „dane Europolu” oznaczają wszelkie operacyjne dane osobowe przetwarzane przez Europol zgodnie z rozporządzeniem (UE) 2016/794;
- 26) „właściwy organ” oznacza każdy organ publiczny właściwy do zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych, lub każdy inny organ lub podmiot, któremu na mocy prawa państwa członkowskiego powierzono wykonywanie władzy publicznej i uprawnień publicznych do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych;
- 27) „organ nadzorczy” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 41 dyrektywy (UE) 2016/680;
- 28) „SIENA” oznacza aplikację sieci bezpiecznej wymiany informacji, zarządzaną i rozwijaną przez Europol zgodnie z rozporządzeniem (UE) 2016/794;
- 29) „incydent” oznacza incydent w rozumieniu art. 6 pkt 6 dyrektywy (UE) 2022/2555 Parlamentu Europejskiego i Rady ⁽¹⁷⁾;
- 30) „znaczący incydent” oznacza każdy incydent, chyba że jego skutki są ograniczone i prawdopodobnie został on już dobrze zrozumiany pod względem metody lub technologii;
- 31) „znaczące cyberzagrożenie” oznacza cyberzagrożenie charakteryzujące się możliwością i zdolnością oraz celem, którym jest spowodowanie znaczącego incydentu;
- 32) „znacząca podatność” oznacza podatność, która prawdopodobnie doprowadzi do znaczącego incydentu, jeżeli zostanie wykorzystana.

ROZDZIAŁ 2

Wymiana danych

Sekcja 1

Profile DNA

Artykuł 5

Dane referencyjne DNA

1. Państwa członkowskie zapewniają dostępność danych referencyjnych DNA pochodzących z krajowych baz danych DNA do celów zautomatyzowanego przeszukania danych przez inne państwa członkowskie i Europol na podstawie niniejszego rozporządzenia.

Dane referencyjne DNA nie mogą zawierać żadnych dodatkowych danych, które umożliwiają bezpośrednią identyfikację osoby.

Niezidentyfikowane profile DNA muszą być rozpoznawalne jako takie.

2. Dane referencyjne DNA są przetwarzane zgodnie z niniejszym rozporządzeniem i zgodnie z prawem krajowym mającym zastosowanie do przetwarzania tych danych.

⁽¹⁷⁾ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

3. Komisja przyjmuje akt wykonawczy w celu określenia charakterystycznych cech identyfikacyjnych profilu DNA podlegających wymianie. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 6

Zautomatyzowane przeszukiwanie profili DNA

1. Do celów prowadzenia postępowań przygotowawczych w sprawach karnych państwa członkowskie, w momencie początkowego połączenia z routerem za pośrednictwem swoich krajowych punktów kontaktowych, przeprowadzają zautomatyzowane przeszukiwanie poprzez porównanie wszystkich profili DNA przechowywanych w ich bazach danych DNA ze wszystkimi profilami DNA przechowywanymi w bazach danych wszystkich pozostałych państw członkowskich i danymi Europolu. Każde państwo członkowskie podejmuje dwustronnie ustalenia z innym państwem członkowskim i z Europolem dotyczące tych zautomatyzowanych przeszukań zgodnie z zasadami i procedurami określonymi w niniejszym rozporządzeniu.

2. Do celów prowadzenia postępowań przygotowawczych w sprawach karnych państwa członkowskie, za pośrednictwem swoich krajowych punktów kontaktowych, przeprowadzają zautomatyzowane przeszukania poprzez porównanie wszystkich swoich nowych profili DNA dodanych do ich bazy danych DNA ze wszystkimi profilami DNA przechowywanymi w bazach danych wszystkich pozostałych państw członkowskich i danymi Europolu.

3. W przypadku gdy przeszukania, o których mowa w ust. 2, nie mogły mieć miejsca, dane państwo członkowskie może uzgodnić dwustronnie z każdym z pozostałych państw członkowskich i z Europolem, że przeprowadzą je na późniejszym etapie poprzez porównanie profili DNA ze wszystkimi profilami DNA przechowywanymi w bazach danych DNA wszystkich pozostałych państw członkowskich i danymi Europolu. Dane państwo członkowskie podejmuje dwustronnie z każdym z pozostałych państw członkowskich i z Europolem ustalenia dotyczące tych zautomatyzowanych przeszukań zgodnie z zasadami i procedurami określonymi w niniejszym rozporządzeniu.

4. Przeszukania, o których mowa w ust. 1, 2 i 3, są prowadzone wyłącznie w ramach indywidualnych spraw i zgodnie z prawem krajowym pytającego państwa członkowskiego.

5. W przypadku gdy podczas zautomatyzowanego przeszukiwania danych okaże się, że występuje dopasowanie między dostarczonym profilem DNA a profilami DNA przechowywanymi w przeszukiwanej bazie danych lub przeszukiwanych bazach danych odpytywanego państwa członkowskiego, krajowy punkt kontaktowy pytającego państwa członkowskiego otrzymuje w sposób zautomatyzowany dane referencyjne DNA, z którymi stwierdzono dopasowanie.

6. Krajowy punkt kontaktowy pytającego państwa członkowskiego może podjąć decyzję o potwierdzeniu dopasowania dwóch profili DNA. W przypadku gdy podejmie on decyzję o potwierdzeniu dopasowania dwóch profili DNA, informuje odpytywane państwo członkowskie, i zapewnia, by co najmniej jeden wykwalifikowany członek personelu przeprowadził weryfikację w celu potwierdzenia tego dopasowania z danymi referencyjnymi DNA otrzymanymi od odpytywanego państwa członkowskiego.

7. W przypadku gdy jest to istotne dla prowadzenia postępowań przygotowawczych w sprawach karnych, krajowy punkt kontaktowy odpytywanego państwa członkowskiego, może podjąć decyzję o potwierdzeniu dopasowania dwóch profili DNA. W przypadku gdy podejmie on decyzję o potwierdzeniu dopasowania dwóch profili DNA, informuje pytające państwo członkowskie i zapewnia, by co najmniej jeden wykwalifikowany członek personelu przeprowadził weryfikację w celu potwierdzenia tego dopasowania z danymi referencyjnymi DNA otrzymanymi od pytającego państwa członkowskiego.

Artykuł 7

Oznaczenia referencyjne profili DNA

Oznaczenia referencyjne profili DNA składają się z następujących elementów:

- a) oznaczenia referencyjnego, które w przypadku stwierdzenia dopasowania umożliwia państwom członkowskim pozyskanie dalszych danych i innych informacji znajdujących się w ich krajowych bazach danych DNA w celu przekazania ich do jednego państwa członkowskiego, kilku lub wszystkich pozostałych państw członkowskich zgodnie z art. 47, lub do Europolu zgodnie z art. 49 ust. 6;

- b) oznaczenia referencyjnego, które w przypadku stwierdzenia dopasowania umożliwi Europolowi pozyskanie dalszych danych i innych informacji do celów art. 48 ust. 1 niniejszego rozporządzenia w celu przekazania ich do jednego państwa członkowskiego, kilku państw członkowskich lub wszystkich państw członkowskich zgodnie z rozporządzeniem (UE) 2016/794;
- c) kodu oznaczającego państwo członkowskie, w którego zbiorze znajduje się dany profil DNA;
- d) kodu wskazującego czy profil DNA jest zidentyfikowanym profilem DNA czy niezidentyfikowanym profilem DNA).

Artykuł 8

Zasady wymiany profili DNA

1. Państwa członkowskie podejmują odpowiednie środki w celu zapewnienia poufności i integralności danych referencyjnych DNA przekazywanych innym państwom członkowskim lub Europolowi, w tym szyfrowanie tych danych. Europol podejmuje odpowiednie środki w celu zapewnienia poufności i integralności danych referencyjnych DNA przekazywanych państwom członkowskim, w tym szyfrowanie tych danych.
2. Każde państwo członkowskie i Europol zapewniają odpowiednią jakość przekazywanych przez siebie profili DNA, umożliwiającą ich zautomatyzowane porównanie. Komisja ustanawia, w drodze aktów wykonawczych, minimalny standard jakości w celu umożliwienia porównywania profili DNA.
3. Komisja przyjmuje akty wykonawcze określające odpowiednie normy europejskie lub międzynarodowe, które mają być stosowane przez państwa członkowskie i Europol do wymiany danych referencyjnych DNA.
4. Akty wykonawcze, o których mowa w ust. 2 i 3 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 9

Zasady dotyczące zapytań i odpowiedzi dotyczących profili DNA

1. Zapytanie dotyczący zautomatyzowanego przeszukania profili DNA zawiera jedynie następujące informacje:
 - a) kod pytającego państwa członkowskiego;
 - b) datę i godzinę oraz numer zapytania;
 - c) dane referencyjne DNA;
 - d) czy przekazywane profile DNA są niezidentyfikowanymi profilami DNA czy zidentyfikowanymi profilami DNA.
2. Odpowiedź na zapytanie, o którym mowa w ust. 1, zawiera jedynie następujące informacje:
 - a) wskazanie, czy stwierdzono co najmniej jedno dopasowanie, czy też go nie stwierdzono;
 - b) datę i godzinę oraz numer zapytania;
 - c) datę i godzinę oraz numer odpowiedzi;
 - d) kody pytającego państwa członkowskiego i = odpytywanego państwa członkowskiego;
 - e) oznaczenia referencyjne profili DNA ze zbiorów pytającego o i odpytywanego państwa członkowskiego;
 - f) czy przekazywane profile DNA są niezidentyfikowanymi profilami DNA czy zidentyfikowanymi profilami DNA;
 - g) profile DNA, w przypadku których stwierdzono dopasowanie.

3. Dopasowanie jest automatycznie notyfikowane jedynie wtedy, gdy wynikiem zautomatyzowanego przeszukania jest dopasowanie minimalnej liczby loci. Komisja przyjmuje akty wykonawcze określające minimalną liczbę loci w tym celu zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

4. Jeżeli w wyniku przeszukania niezidentyfikowanych profili DNA stwierdzono dopasowanie, każde odpytywane państwo członkowskie, w którego zbiorze znajdują się dane wykazujące dopasowanie, może wprowadzić do swojej krajowej bazy danych adnotację informującą, że w wyniku przeszukania przez inne państwo członkowskie stwierdzono dopasowanie z danym profilem DNA. Adnotacja zawiera oznaczenie referencyjne profilu DNA użyte przez pytające państwo członkowskie.

5. Państwa członkowskie zapewniają zgodność zapytań, o których mowa w ust. 1 niniejszego artykułu, z powiadomieniami przesłanymi na podstawie art. 74. Powiadomienia te zostają przedstawione w praktycznym podręczniku, o którym mowa w art. 79.

Sekcja 2

Dane daktyloskopijne

Artykuł 10

Daktyloskopijne dane referencyjne

1. Państwa członkowskie zapewniają dostępność daktyloskopijnych danych referencyjnych z krajowych baz danych utworzonych w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych.
2. Daktyloskopijne dane referencyjne nie mogą zawierać żadnych dodatkowych danych, które umożliwiają bezpośrednią identyfikację osoby.
3. Niezidentyfikowane dane daktyloskopijne muszą być rozpoznawalne jako takie.

Artykuł 11

Zautomatyzowane przeszukanie danych daktyloskopijnych

1. Do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych państwa członkowskie umożliwiają krajowym punktom kontaktowym innych państw członkowskich i Europolowi dostęp do daktyloskopijnych danych referencyjnych z krajowych baz danych utworzonych w tym celu, na potrzeby zautomatyzowanego przeszukania tych danych przez porównanie daktyloskopijnych danych referencyjnych.

Przeszukania, o których mowa w akapicie pierwszym, jest prowadzone wyłącznie w ramach indywidualnych spraw i zgodnie z prawem krajowym pytającego państwa członkowskiego.

2. Krajowy punkt kontaktowy pytającego państwa członkowskiego może podjąć decyzję o potwierdzeniu dopasowania dwóch zbiorów danych daktyloskopijnych. W przypadku gdy podejmie on decyzję o potwierdzeniu dopasowania dwóch zbiorów danych daktyloskopijnych, informuje odpytywane państwo członkowskie, i zapewnia, by co najmniej jeden wykwalifikowany członek personelu przeprowadził weryfikację w celu potwierdzenia tego dopasowania z daktyloskopijnymi danymi referencyjnymi otrzymanymi od odpytywanego państwa członkowskiego.

Artykuł 12

Oznaczenia referencyjne danych daktyloskopijnych

Oznaczenia referencyjne danych daktyloskopijnych składają się z następujących elementów:

- a) oznaczenia referencyjne, które w przypadku stwierdzenia dopasowania umożliwia państwom członkowskim pozyskanie dalszych danych i innych informacji znajdujących się w ich bazach danych, o których mowa w art. 10, w celu przekazania ich do jednego państwa członkowskiego, kilku z pozostałych państw członkowskich lub wszystkich takich państw zgodnie z art. 47, lub do Europolu zgodnie z art. 49 ust. 6;

- b) oznaczenia referencyjnego, które w przypadku stwierdzenia dopasowania umożliwi Europolowi pozyskanie dalszych danych i innych informacji do celów art. 48 ust. 1 niniejszego rozporządzenia w celu przekazania ich do jednego państwa członkowskiego, kilku państw członkowskich lub wszystkich państw członkowskich zgodnie z rozporządzeniem (UE) 2016/794;
- c) kodu oznaczającego państwo członkowskie, w którego zbiorze znajdują się odpowiednie dane daktyloskopijne.

Artykuł 13

Zasady wymiany danych daktyloskopijnych

1. Państwa członkowskie podejmują odpowiednie środki aby zapewnić poufność i integralność danych daktyloskopijnych przekazywanych innym państwom członkowskim lub Europolowi, w tym szyfrowanie danych. Europol podejmuje odpowiednie środki aby zapewnić poufność i integralność danych daktyloskopijnych przekazywanych innym państwom członkowskim, w tym szyfrowanie danych
2. Każde państwo członkowskie i Europol zapewniają odpowiednią jakość przekazywanych przez siebie danych daktyloskopijnych, umożliwiającą ich zautomatyzowane porównanie. Komisja ustanawia w drodze aktów wykonawczych minimalny standard jakości aby umożliwić porównanie danych daktyloskopijnych.
3. Dane daktyloskopijne przekształca się w formę cyfrową i przekazuje się je innym państwom członkowskim lub Europolowi zgodnie ze standardami europejskimi lub międzynarodowymi. Komisja przyjmuje akty wykonawcze określające odpowiednie standardy europejskie lub międzynarodowe, które mają być stosowane przez państwa członkowskie i Europol do wymiany daktyloskopijnych danych referencyjnych.
4. Akty wykonawcze, o których mowa w ust. 2 i 3 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 14

Możliwości przeszukania danych daktyloskopijnych

1. Każde państwo członkowskie zapewnia, aby jego zapytania dotyczące przeszukania nie przekraczały możliwości przeszukania określonych przez odpytywane państwo członkowskie, lub Europol w celu zapewnienia gotowości systemu i uniknięcia jego przeciążenia. W tym samym celu Europol zapewnia, aby jego zapytania dotyczące przeszukania nie przekraczały możliwości przeszukania określonych przez odpytywane państwo członkowskie.

Państwa członkowskie informują pozostałe państwa członkowskie, Komisję, eu-LISA i Europol o swoich maksymalnych dziennych możliwościach przeszukania zidentyfikowanych i niezidentyfikowanych danych daktyloskopijnych. Europol informuje państwa członkowskie, Komisję i eu-LISA o swoich maksymalnych dziennych możliwościach przeszukania zidentyfikowanych i niezidentyfikowanych danych daktyloskopijnych. Państwa członkowskie lub Europol mogą tymczasowo lub na stałe zwiększyć te możliwości przeszukania w dowolnym momencie, w tym w pilnych przypadkach. W przypadku gdy państwo członkowskie zwiększy te maksymalne możliwości przeszukania, powiadamia pozostałe państwa członkowskie, Komisję, eu-LISA i Europol o nowych maksymalnych możliwościach przeszukania. W przypadku gdy Europol zwiększy te maksymalne możliwości przeszukania, powiadamia państwa członkowskie, Komisję i eu-LISA o nowych maksymalnych możliwościach przeszukania.

2. Komisja przyjmuje akty wykonawcze określające maksymalną liczbę kandydatów zaakceptowanych do porównania na jedno przekazanie oraz rozdzielenie niewykorzystanych możliwości przeszukania między państwa członkowskie zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 15

Zasady dotyczące zapytań i odpowiedzi dotyczących danych daktyloskopijnych

1. Zapytanie dotyczące zautomatyzowanego przeszukania danych daktyloskopijnych zawiera jedynie następujące informacje:
 - a) kod pytającego państwa członkowskiego;

- b) datę i godzinę oraz numer zapytania;
 - c) referencyjne dane daktyloskopijne.
2. Odpowiedź na zapytanie, o którym mowa w ust. 1, zawiera jedynie następujące informacje:
- a) wskazanie, czy stwierdzono co najmniej jedno dopasowanie, czy też go nie stwierdzono;
 - b) datę i godzinę oraz numer zapytania;
 - c) datę i godzinę oraz numer odpowiedzi;
 - d) kody pytającego i państwa członkowskiego;
 - e) oznaczenia referencyjne danych daktyloskopijnych ze zbiorów pytającego i odpytywanego państwa członkowskiego
 - f) dane daktyloskopijne, w przypadku których stwierdzono dopasowanie.
3. Państwa członkowskie zapewniają zgodność swoich zapytań, o których mowa w ust. 1 niniejszego artykułu, z powiadomieniami przesłanymi na podstawie art. 74. Powiadomienia te zostają przedstawione w praktycznym podręczniku, o którym mowa w art. 79.

Sekcja 3

Dane rejestracyjne pojazdów

Artykuł 16

Zautomatyzowane przeszukanie danych rejestracyjnych pojazdów

1. Do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych państwa członkowskie umożliwiają krajowym punktom kontaktowym innych państw członkowskich i Europolowi dostęp do następujących danych rejestracyjnych pojazdów w celu zautomatyzowanego przeszukania tych danych w indywidualnych sprawach:
- a) dane właściciela lub posiadacza pojazdu;
 - b) dane pojazdu.
2. Przeszukania, o których mowa w ust. 1, przeprowadza się jedynie według następujących danych:
- a) pełnego numeru podwozia,
 - b) pełnego numeru rejestracyjnego, lub
 - c) w przypadku gdy zezwala na to prawo krajowe odpytywanego państwa członkowskiego – danych dotyczących właściciela lub posiadacza pojazdu.
3. Przeszukania, o których mowa w ust. 1 przeprowadzone z użyciem danych dotyczących właściciela lub posiadacza pojazdu przeprowadza się wyłącznie w przypadku osób podejrzanych lub skazanych. Do celów takiego przeszukania wykorzystuje się wszystkie następujące dane identyfikacyjne:
- a) w przypadku gdy właściciel lub posiadacz pojazdu jest osobą fizyczną:
 - (i) imię lub imiona osoby fizycznej;
 - (ii) nazwisko lub nazwiska osoby fizycznej; oraz
 - (iii) datę urodzenia osoby fizycznej;
 - b) w przypadku gdy właściciel lub posiadacz pojazdu jest osobą prawną, nazwę tej osoby prawnej.
4. Przeszukanie, o którym mowa w ust. 1, może być prowadzone wyłącznie zgodnie z prawem krajowym pytającego państwa członkowskiego.

*Artykuł 17***Zasady zautomatyzowanego przeszukania danych rejestracyjnych pojazdów**

1. Do zautomatyzowanego przeszukania danych rejestracyjnych pojazdów państwa członkowskie wykorzystują europejski system informacji o pojazdach i prawach jazdy (EUCARIS).
2. Informacje wymieniane za pośrednictwem EUCARIS są przekazywane w formie zaszyfrowanej.
3. Komisja przyjmuje akty wykonawcze określające elementy danych rejestracyjnych pojazdów, które mogą podlegać wymianie, oraz procedurę techniczną, zgodnie z którą Eucaris dokonuje kwerendy w bazach danych państw członkowskich. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

*Artykuł 18***Prowadzenie rejestrów**

1. Każde państwo członkowskie prowadzi rejestry kwerend dokonywanych przez personel jego właściwych organów należycie upoważniony do wymiany danych rejestracyjnych pojazdów oraz rejestry kwerend, co do których wysłały zapytania inne państwa członkowskie. Europol prowadzi rejestry kwerend dokonywanych przez jego należycie upoważniony personel.

Każde państwo członkowskie i Europol prowadzą rejestry wszystkich operacji przetwarzania danych dotyczących danych rejestracyjnych pojazdów. Rejestry te obejmują:

- a) informację, czy zapytania w celu kwerendy dokonało państwo członkowskie czy Europol; w przypadku gdy zapytania w celu kwerendy dokonało państwo członkowskie – nazwę danego państwa członkowskiego
- b) datę i godzinę zapytania;
- c) datę i godzinę odpowiedzi;
- d) krajowe bazy danych, do których przesłano zapytanie w celu kwerendy;
- e) krajowe bazy danych, z których otrzymano odpowiedź twierdzącą.

2. Rejestry, o których mowa w ust. 1, wykorzystuje się wyłącznie w celu zbierania danych statystycznych i monitorowania ochrony danych, w tym sprawdzania dopuszczalności kwerendy 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 trzy lata 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.

3. Na potrzeby monitorowania ochrony danych, w tym sprawdzania dopuszczalności kwerendy i zgodności przetwarzania danych z prawem, administratorzy danych mają dostęp do rejestrów w celu monitorowania własnej działalności, o którym mowa w art. 55.

Sekcja 4

Wizerunki twarzy*Artykuł 19***Dane referencyjne wizerunków twarzy**

1. Państwa członkowskie zapewniają dostępność danych referencyjnych wizerunków twarzy osób podejrzanych i skazanych oraz, jeśli jest dozwolone na mocy prawa krajowego, ofiar przestępstwa, ze swoich krajowych baz danych utworzonych w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych.

2. Dane referencyjne wizerunków twarzy nie zawierają żadnych dodatkowych danych, które umożliwiają bezpośrednią identyfikację osoby.
3. Niezidentyfikowane wizerunki twarzy muszą być rozpoznawalne jako takie.

Artykuł 20

Zautomatyzowane przeszukiwanie wizerunków twarzy

1. Do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych, gdzie kara maksymalna wynosi co najmniej jeden rok pozbawienia wolności na mocy prawa pytającego państwa członkowskiego, państwa członkowskie umożliwiają krajowym punktom kontaktowym innych państw członkowskich i Europolowi dostęp do danych referencyjnych wizerunków twarzy przechowywanych w krajowych bazach danych w celu ich zautomatyzowanego przeszukania.

Przeszukiwanie, o którym mowa w akapicie pierwszym, jest prowadzone wyłącznie w ramach indywidualnych spraw i zgodnie z prawem krajowym pytającego państwa członkowskiego.

Profilowanie, o którym mowa w art. 11 ust. 3 dyrektywy (UE) 2016/680, jest zakazane.

2. Krajowy punkt kontaktowy pytającego państwa członkowskiego może podjąć decyzję o potwierdzeniu dopasowania dwóch wizerunków twarzy, w przypadku gdy podejmie on decyzję o potwierdzeniu dopasowania dwóch wizerunków twarzy, informuje odpytywane państwo członkowskie, i zapewnia, by co najmniej jeden wykwalifikowany członek personelu przeprowadził weryfikację w celu potwierdzenia tego dopasowania z danymi referencyjnymi wizerunków twarzy otrzymanymi od odpytywanego państwa członkowskiego.

Artykuł 21

Oznaczenia referencyjne wizerunków twarzy

Oznaczenia referencyjne wizerunków twarzy składają się z następujących elementów:

- a) oznaczenia referencyjnego, które w przypadku stwierdzenia dopasowania umożliwia państwom członkowskim pozyskanie dalszych danych i innych informacji znajdujących się w ich bazach danych, o których mowa w art. 19, w celu przekazania ich do jednego państwa członkowskiego, kilku z pozostałych państw członkowskich lub wszystkich takich państw zgodnie z art. 47, lub do Europolu zgodnie z art. 49 ust. 6;
- b) oznaczenia referencyjnego, które w przypadku stwierdzenia dopasowania umożliwia Europolowi pozyskanie dalszych danych i innych informacji, do celów art. 48 ust. 1 niniejszego rozporządzenia, w celu przekazania ich do jednego państwa członkowskiego, kilku państw członkowskich lub wszystkich państw członkowskich zgodnie z rozporządzeniem (UE) 2016/794;
- c) kodu oznaczającego państwo członkowskie, w którego zbiorze znajduje się dany wizerunek twarzy.

Artykuł 22

Zasady wymiany wizerunków twarzy

1. Państwa członkowskie podejmują odpowiednie środki aby zapewnić poufność i integralność wizerunków twarzy przekazywanych innym państwom członkowskim lub Europolowi, w tym szyfrowanie danych. Europol podejmuje odpowiednie środki aby zapewnić poufność i integralność wizerunków twarzy przekazywanych państwom członkowskim, w tym szyfrowanie danych.

2. Każde państwo członkowskie i Europol zapewniają odpowiednią jakość przekazywanych przez siebie wizerunków twarzy, umożliwiającą ich zautomatyzowane porównanie. Komisja ustanawia w drodze aktów wykonawczych minimalny standard jakości aby umożliwić porównanie wizerunków twarzy. W przypadku gdy sprawozdanie, o którym mowa w art. 80 ust. 7, wykazuje wysokie ryzyko fałszywych dopasowań, Komisja przeprowadza przegląd tych aktów wykonawczych.

3. Komisja przyjmuje akty wykonawcze określające odpowiednie standardy europejskie lub międzynarodowe, które mają być stosowane przez państwa członkowskie i Europol przy wymianie wizerunków twarzy.

4. Akty wykonawcze, o których mowa w ust. 2 i 3 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 23

Możliwości przeszukania wizerunków twarzy

1. Każde państwo członkowskie zapewnia, aby jego zapytania dotyczące przeszukania nie przekraczały możliwości przeszukiwania określonych przez odpytywane państwo członkowskie lub Europol w celu zapewnienia gotowości systemu i uniknięcia jego przeciążenia. W tym samym celu Europol zapewnia, aby jego zapytania dotyczące przeszukania nie przekraczały możliwości przeszukania określonych przez odpytywane państwo członkowskie.

Państwa członkowskie informują pozostałe państwa członkowskie, Komisję, eu-LISA i Europol o swoich maksymalnych dziennych możliwościach przeszukania zidentyfikowanych i niezidentyfikowanych wizerunków twarzy. Europol informuje państwa członkowskie, Komisję i eu-LISA o swoich maksymalnych dziennych możliwościach przeszukania zidentyfikowanych i niezidentyfikowanych wizerunków twarzy. Państwa członkowskie lub Europol mogą tymczasowo lub na stałe zwiększyć te możliwości przeszukania w dowolnym momencie, w tym w pilnych przypadkach. W przypadku gdy państwo członkowskie zwiększy te maksymalne możliwości przeszukania, powiadamia pozostałe państwa członkowskie, Komisję, eu-LISA i Europol o nowych maksymalnych możliwościach przeszukania. W przypadku gdy Europol zwiększy te maksymalne możliwości przeszukania, powiadamia państwa członkowskie, Komisję i eu-LISA o nowych maksymalnych możliwościach przeszukania.

2. Komisja przyjmuje akty wykonawcze określające maksymalną liczbę kandydatów zaakceptowanych do porównania na jedno przekazanie oraz rozdzielenie niewykorzystanych możliwości przeszukania między państwa członkowskie zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 24

Zasady dotyczące zapytań i odpowiedzi dotyczących wizerunków twarzy

1. Zapytanie dotyczący zautomatyzowanego przeszukania wizerunków twarzy zawiera jedynie następujące informacje:

- a) kod pytającego państwa członkowskiego;
- b) datę i godzinę oraz numer zapytania;
- c) dane referencyjne wizerunków twarzy.

2. Odpowiedź na zapytanie, o którym mowa w ust. 1, zawiera jedynie następujące informacje:

- a) wskazanie, czy stwierdzono jedno dopasowanie lub większą liczbę dopasowań, czy też nie stwierdzono dopasowań;
- b) datę i godzinę oraz numer zapytania;
- c) datę i godzinę oraz numer odpowiedzi;
- d) kody pytającego i odpytywanego państwa członkowskiego;
- e) oznaczenia referencyjne wizerunków twarzy ze zbiorów pytającego i odpytywanego państwa członkowskiego;
- f) wizerunki twarzy, w przypadku których stwierdzono dopasowanie.

3. Państwa członkowskie zapewniają zgodność zapytań, o których mowa w ust. 1 niniejszego artykułu, z powiadomieniami przesłanymi na podstawie art. 74. Powiadomienia te zostają przedstawione w praktycznym podręczniku, o którym mowa w art. 79.

Sekcja 5

Rejestry policyjne

Artykuł 25

Rejestry policyjne

1. Państwa członkowskie mogą brać udział w zautomatyzowanej wymianie informacji z rejestrów policyjnych. Do celów takiej wymiany uczestniczące państwa członkowskie zapewniają dostępność indeksów krajowego rejestru policyjnego zawierających zbiory danych biograficznych osób podejrzanych i skazanych z krajowych baz danych utworzonych do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych. Te zbiory danych, zawierają wyłącznie następujące dane w zakresie, w jakim są one dostępne:

- a) imię lub imiona;
 - b) nazwisko lub nazwiska;
 - c) alias lub alias-y oraz poprzednio używane imię i nazwisko lub imiona i nazwiska;
 - d) datę urodzenia;
 - e) obywatelstwo lub obywatelstwa;
 - f) państwo urodzenia;
 - g) płeć.
2. Dane, o których mowa w ust. 1 lit. a), b) i c), są pseudonimizowane.

Artykuł 26

Zautomatyzowane przeszukanie indeksów krajowego rejestru policyjnego

Do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych, gdzie kara maksymalna wynosi co najmniej jeden rok pozbawienia wolności na mocy prawa pytającego państwa członkowskiego, państwa członkowskie uczestniczące w zautomatyzowanej wymianie informacji z rejestrów policyjnych umożliwiają krajowym punktom kontaktowym innych uczestniczących państw członkowskich i Europolowi dostęp do danych z indeksów krajowego rejestru policyjnego w celu zautomatyzowanego przeszukania takich danych.

Przeszukanie, o którym mowa w akapicie pierwszym, jest prowadzone wyłącznie w ramach indywidualnych spraw i zgodnie z prawem krajowym pytającego państwa członkowskiego.

Artykuł 27

Oznaczenia referencyjne informacji z rejestrów policyjnych

Oznaczenia referencyjne informacji z rejestrów policyjnych składają się z następujących elementów:

- a) oznaczenia referencyjnego, które w przypadku stwierdzenia dopasowania umożliwi państwom członkowskim pozyskanie danych biograficznych i innych informacji znajdujących się w ich indeksach krajowego rejestru policyjnego, o których mowa w art. 25, w celu przekazania ich do jednego państwa członkowskiego, kilku państw członkowskich lub wszystkich państw członkowskich zgodnie z art. 44;
- b) kodu oznaczającego państwo członkowskie, które przechowuje rejestry policyjne

Artykuł 28

Zasady dotyczące zapytań i odpowiedzi dotyczących rejestrów policyjnych

1. Zapytanie dotyczące zautomatyzowanego przeszukania indeksów krajowego rejestru policyjnego zawiera jedynie następujące informacje:

- a) kod pytającego państwa członkowskiego;

- b) datę i godzinę oraz numer zapytania;
 - c) dane, o których mowa w art. 25, o ile są one dostępne.
2. Odpowiedź na zapytanie, o którym mowa w ust. 1, zawiera jedynie następujące informacje:
- a) wskazanie liczby dopasowań;
 - b) datę i godzinę oraz numer zapytania;
 - c) datę i godzinę oraz numer odpowiedzi;
 - d) kody pytającego państwa członkowskiego i odpytywanego państwa członkowskiego;
 - e) oznaczenia referencyjne rejestrów policyjnych odpytywanego państwa członkowskiego.
3. Państwa członkowskie zapewniają zgodność zapytań, o których mowa w ust. 1 niniejszego artykułu, z powiadomieniami przesłanymi na podstawie art. 74. Powiadomienia te zostają przedstawione w praktycznym podręczniku, o którym mowa w art. 79.

Sekcja 6

Przepisy wspólne

Artykuł 29

Osoby zaginione i niezidentyfikowane szczątki ludzkie

1. W przypadku gdy organ krajowy został do tego upoważniony na mocy krajowych środków ustawodawczych, o których mowa w ust. 2, może on przeprowadzać zautomatyzowane przeszukiwanie z wykorzystaniem ram z Prüm II wyłącznie do następujących celów:
- a) poszukiwania osób zaginionych w kontekście postępowań przygotowawczych lub ze względów humanitarnych;
 - b) identyfikowania szczątków ludzkich.
2. Państwa członkowskie, które chcą skorzystać z możliwości przewidzianej w ust. 1, wyznaczają, w drodze krajowych środków ustawodawczych, organy krajowe właściwe do celów w nich określonych oraz określają procedury, warunki i kryteria, w tym względy humanitarne, w oparciu o które zezwala się na przeprowadzanie poszukiwania osób zaginionych, o czym mowa w ust. 1 lit. a).

Artykuł 30

Krajowe punkty kontaktowe

Każde państwo członkowskie wyznacza co najmniej jeden krajowy punkt kontaktowy do celów art. 6, 11, 16, 20 i 26.

Artykuł 31

Środki wykonawcze

Komisja przyjmuje akty wykonawcze określające rozwiązania techniczne dla państw członkowskich w odniesieniu do procedur, o których mowa w art. 6, 11, 16, 20 i 26. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

*Artykuł 32***Dostępność zautomatyzowanej wymiany danych na poziomie krajowym**

1. Państwa członkowskie przyjmują wszelkie środki niezbędne do zapewnienia, aby zautomatyzowane przeszukanie profili DNA, danych daktyloskopijnych, niektórych danych rejestracyjnych pojazdów, wizerunków twarzy i informacji z rejestrów policyjnych było możliwe całodobowo, przez 7 dni w tygodniu.

2. Krajowe punkty kontaktowe niezwłocznie informują siebie nawzajem, Komisję, eu-LISA i Europol o każdym przypadku niedostępności zautomatyzowanej wymiany danych, w tym, w stosownych przypadkach, o każdej awarii technicznej powodującej taką niedostępność.

Krajowe punkty kontaktowe uzgadniają, zgodnie z mającymi zastosowanie przepisami unijnymi i prawem krajowym, tymczasowe alternatywne sposoby wymiany informacji, które należy stosować, gdy zautomatyzowana wymiana danych jest niedostępna.

3. W przypadku gdy zautomatyzowana wymiana danych jest niedostępna, krajowe punkty kontaktowe zapewniają wszelkimi koniecznymi środkami jej bezzwłoczne przywrócenie.

*Artykuł 33***Uzasadnienie przetwarzania danych**

1. Każde państwo członkowskie przechowuje zapisy uzasadnień kwerend dokonywanych przez jego właściwe organy.

Europol przechowuje zapisy uzasadnień własnych kwerend.

2. Uzasadnienie, o którym mowa w ust. 1, zawiera:

- a) cel kwerendy, w tym odniesienie do konkretnej sprawy lub konkretnego postępowania przygotowawczego, oraz, w odpowiednich przypadkach, do konkretnego przestępstwa;
- b) wskazanie, czy kwerenda dotyczy podejrzanego, osoby skazanej za przestępstwo, ofiary przestępstwa, osoby zaginionej lub niezidentyfikowanych szczątków ludzkich;
- c) wskazanie, czy celem kwerendy jest zidentyfikowanie osoby, czy też uzyskanie większej ilości danych na temat osoby znanej.

3. Uzasadnienia, o których mowa w ust. 1 niniejszego artykułu, są powiązane z rejestrami, o których mowa w art. 18, 40 i 45. Te uzasadnienia są wykorzystywane wyłącznie w celu oceny czy przeszukania są proporcjonalne i konieczne w celu zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych, monitorowania ochrony danych, w tym sprawdzania dopuszczalności kwerendy i zgodności przetwarzania danych z prawem, oraz w celu zapewniania bezpieczeństwa i integralności danych. Uzasadnienia te są chronione przed nieuprawnionym dostępem za pomocą odpowiednich środków i usuwane trzy lata po utworzeniu. Jeżeli jednak są one wymagane do prowadzenia już rozpoczętych procedur monitorowania, usuwa się je, gdy tylko przestaną być konieczne do tego celu.

4. Aby ocenić proporcjonalność i konieczność przeszukań do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych, oraz na potrzeby monitorowania praw podstawowych i ochrony danych, w tym sprawdzania dopuszczalności kwerendy i zgodności przetwarzania danych z prawem, administratorzy danych mają dostęp do tych uzasadnień w celu monitorowania własnej działalności, jak określono w art. 55.

*Artykuł 34***Stosowanie uniwersalnego formatu wiadomości**

1. Przy opracowywaniu routera, o którym mowa w art. 35 niniejszego rozporządzenia, i europejskiego systemu przekazywania informacji z rejestrów policyjnych (EPRIS) stosuje się, o ile to możliwe, standard uniwersalnego formatu wiadomości (UMF) ustanowiony w art. 38 rozporządzenia (UE) 2019/818.

2. W każdej zautomatyzowanej wymianie danych zgodnie z niniejszym rozporządzeniem stosuje się, o ile to możliwe, standard UMF.

ROZDZIAŁ 3

Architektura

Sekcja 1

Router

Artykuł 35

Router

1. Aby ułatwić ustanowienie połączeń między państwami członkowskimi oraz między państwami członkowskimi a Europolem w celu dokonywania kwerend z wykorzystaniem danych biometrycznych, pozyskiwania takich danych oraz ich oceny punktowej, a także w celu pozyskiwania danych alfanumerycznych zgodnie z niniejszym rozporządzeniem, tworzy się router.

2. Router składa się z:

- a) infrastruktury centralnej obejmującej narzędzie do przeszukania umożliwiające jednoczesną kwerendę w krajowych bazach danych, o których mowa w art. 5, 10 i 19, oraz w danych Europolu;
- b) bezpiecznego kanału komunikacji między infrastrukturą centralną, właściwymi organami upoważnionymi do korzystania z routera zgodnie z art. 36 a Europolem;
- c) bezpiecznej infrastruktury łączności między infrastrukturą centralną a europejskim portalem wyszukiwania, ustanowionym w art. 6 rozporządzenia (UE) 2019/817 i art. 6 rozporządzenia (UE) 2019/818, do celów art. 39.

Artykuł 36

Korzystanie z routera

Korzystanie z routera jest zastrzeżone dla właściwych organów państw członkowskich, które są upoważnione do dostępu do profili DNA, danych daktyloskopijnych i wizerunków twarzy oraz ich wymiany zgodnie z niniejszym rozporządzeniem, oraz dla Europolu zgodnie z niniejszym rozporządzeniem i rozporządzeniem (UE) 2016/794.

Artykuł 37

Procesy

1. Właściwe organy upoważnione do korzystania z routera na podstawie art. 36 lub Europol składają zapytanie w celu kwerendy, przesyłając dane biometryczne do routera. Router przesyła zapytanie w celu kwerendy do baz danych wszystkich lub poszczególnych państw członkowskich i danych Europolu jednocześnie z danymi przekazanymi przez użytkownika zgodnie z przysługującymi mu prawami dostępu.

2. Po otrzymaniu od routera zapytania w celu kwerendy każde odpytywane państwo członkowskie w sposób zautomatyzowany i bezzwłocznie uruchamiają kwerendę w swoich bazach danych. Po otrzymaniu od routera zapytania w celu kwerendy Europol w sposób zautomatyzowany i bezzwłocznie uruchamia kwerendę swoich danych.

3. Wszelkie dopasowania wynikające z kwerend, o których mowa w ust. 2, są w sposób zautomatyzowany odsyłane do routera. W przypadku braku dopasowania pytające państwo członkowskie zostaje o tym automatycznie powiadomione.

4. Router szereguje odpowiedzi, w przypadku gdy pytającego państwo członkowskie tak postanowi i w stosownych przypadkach, poprzez porównanie danych biometrycznych wykorzystywanych do przeprowadzenia kwerendy z danymi biometrycznymi przekazanymi w odpowiedziach przez odpytywane państwo członkowskie lub odpytywane państwa członkowskie lub Europol.
5. Router zwraca użytkownikowi wykaz danych biometrycznych, w przypadku których stwierdzono dopasowanie, wraz z oceną punktową.
6. Komisja przyjmuje akty wykonawcze określające procedurę techniczną, zgodnie z którą router dokonuje kwerendy w bazach danych państw członkowskich i w danych Europolu, formatu odpowiedzi routera na takie kwerendy oraz zasad technicznych dotyczących porównywania i szeregowania zgodności danych biometrycznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 38

Kontrola jakości

Odpytywane państwo członkowskie sprawdza w sposób zautomatyzowany jakość przekazanych danych.

Odpytywane państwo członkowskie bezzwłocznie informuje za pośrednictwem routera pytające państwo członkowskie, jeżeli dane nie nadają się do zautomatyzowanego porównywania.

Artykuł 39

Interoperacyjność między routerem a wspólnym repozytorium danych umożliwiających identyfikację na potrzeby dostępu organów ścigania

1. W przypadku gdy wyznaczone organy w rozumieniu art. 4 pkt (20) rozporządzenia (UE) 2019/817 i art. 4 pkt (20) rozporządzenia (UE) 2019/818 są upoważnione do korzystania z routera na podstawie art. 36 niniejszego rozporządzenia mogą one uruchamiać kwerendy w bazach danych państw członkowskich i w danych Europolu jednocześnie z kwerendą we wspólnym repozytorium danych umożliwiających identyfikację, ustanowionym w art. 17 rozporządzenia (UE) 2019/817 i art. 17 rozporządzenia (UE) 2019/818, z zastrzeżeniem że spełnione są odpowiednie warunki przewidziane w prawie Unii, a kwerendę uruchomiono zgodnie z prawami dostępu przysługującymi tym organom. W tym celu router uruchamia kwerendę we wspólnym repozytorium danych umożliwiających identyfikację za pośrednictwem europejskiego portalu wyszukiwania.

2. Kwerendy na potrzeby ochrony porządku publicznego we wspólnym repozytorium danych umożliwiających identyfikację przeprowadza się zgodnie z art. 22 rozporządzenia (UE) 2019/817 i art. 22 rozporządzenia (UE) 2019/818. Wszelkie wyniki takich kwerend są przekazywane za pośrednictwem europejskiego portalu wyszukiwania.

Jednoczesne kwerendy w bazach danych państw członkowskich i w danych Europolu oraz we wspólnym repozytorium danych umożliwiających identyfikację uruchamia się wyłącznie w przypadkach, gdy istnieją uzasadnione powody, by sądzić, że dane dotyczące podejrzanego, sprawcy lub ofiary przestępstwa terrorystycznego lub innego poważnego przestępstwa, określonych odpowiednio w art. 4 pkt 21 i 22 rozporządzenia (UE) 2019/817 oraz odpowiednio w art. 4 pkt 21 i 22 rozporządzenia (UE) 2019/818, są przechowywane we wspólnym repozytorium danych umożliwiających identyfikację.

Artykuł 40

Prowadzenie rejestrów

1. eu-LISA prowadzi rejestry dotyczące wszystkich operacji przetwarzania danych w routerze. Rejestry te obejmują:
 - a) informację czy zapytania w celu kwerendy dokonało państwo członkowskie czy Europol; w przypadku gdy zapytania w celu kwerendy dokonało państwo członkowskie – nazwa danego państwa członkowskiego;
 - b) datę i godzinę zapytania;
 - c) datę i godzinę odpowiedzi;

- d) krajowe bazy danych lub dane Europolu, do których przesłano zapytanie w celu kwerendy;
- e) krajowe bazy danych lub dane Europolu, w przypadku których otrzymano odpowiedź;
- f) w stosownych przypadkach fakt, że prowadzono jednoczesną kwerendę we wspólnym repozytorium danych umożliwiających identyfikację.

2. Każde państwo członkowskie prowadzi rejestry kwerend dokonywanych przez personel jego właściwych organów należycie upoważniony do korzystania z routera oraz rejestry kwerend, co do których wysłały zapytanie inne państwa członkowskie.

Europol prowadzi rejestry kwerend dokonywanych przez jego należycie upoważniony personel.

3. Rejestry, o których mowa w ust. 1 i 2, wykorzystuje się wyłącznie w celu zbierania danych statystycznych i monitorowania ochrony danych, w tym sprawdzania dopuszczalności kwerendy 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 trzy lata po utworzeniu. Jeżeli jednak są konieczne do prowadzenia już rozpoczętych procedur monitorowania, są one usuwane, gdy tylko przestają być konieczne do celu tych procedur.

4. Na potrzeby monitorowania ochrony danych, w tym sprawdzania dopuszczalności kwerendy i zgodności przetwarzania danych z prawem, administratorzy danych mają dostęp do rejestrów w celu monitorowania własnej działalności, o którym mowa w art. 55.

Artykuł 41

Procedury powiadamiania w przypadku braku technicznej możliwości korzystania z routera

1. Jeśli korzystanie z routera w celu kwerendy w krajowej bazie danych lub krajowych bazach danych, lub w danych Europolu nie jest technicznie możliwe z powodu awarii routera, eu-LISA automatycznie powiadamia o tym fakcie użytkowników routera, o których mowa w art. 36. eu-LISA niezwłocznie podejmuje odpowiednie działania mające na celu usunięcie braku technicznej możliwości korzystania z routera.

2. Jeśli korzystanie z routera w celu kwerendy w krajowej bazie danych lub krajowych bazach danych nie jest technicznie możliwe z powodu awarii infrastruktury krajowej w jednym z państw członkowskich, to państwo członkowskie automatycznie powiadamia o tym fakcie pozostałe państwa członkowskie, Komisję, eu-LISA i Europol. Dane państwo członkowskie niezwłocznie podejmuje odpowiednie działania mające na celu usunięcie braku technicznej możliwości korzystania z routera.

3. Jeśli korzystanie z routera w celu kwerendy w danych Europolu nie jest technicznie możliwe z powodu awarii infrastruktury Europolu, Europol automatycznie powiadamia o tym fakcie państwa członkowskie, Komisję i eu-LISA. Europol niezwłocznie podejmuje odpowiednie działania mające na celu usunięcie braku technicznej możliwości korzystania z routera.

Sekcja 2

EPRIS

Artykuł 42

EPRIS

1. Niniejszym ustanawia się europejski system przekazywania informacji z rejestrów policyjnych (EPRIS). Do celów zautomatyzowanego przeszukania indeksów krajowego rejestru policyjnego, o których mowa w art. 26, państwa członkowskie i Europol korzystają z EPRIS.

2. W skład EPRIS wchodzi:

- a) zdecentralizowana infrastruktura w państwach członkowskich, obejmująca narzędzie do przeszukania umożliwiające jednoczesną kwerendę w indeksach krajowego rejestru policyjnego, na podstawie krajowych baz danych;

- b) infrastruktura centralna, wspierająca narzędzie do przeszukania umożliwiające jednoczesną kwerendę w indeksach krajowego rejestru policyjnego;
- c) bezpieczny kanał komunikacji między infrastrukturą centralną, państwami członkowskimi i Europolem.

Artykuł 43

Użytkowanie EPRIS

1. Do celów przeszukania indeksów krajowego rejestru policyjnego za pośrednictwem EPRIS wykorzystuje się co najmniej dwa spośród następujących zbiorów danych:
 - a) imię lub imiona;
 - b) nazwisko lub nazwiska;
 - c) datę urodzenia.
2. Można również wykorzystywać następujące zbiory danych, jeśli są dostępne:
 - a) alias lub alias-y oraz poprzednio używane imię i nazwisko lub imiona i nazwiska;
 - b) obywatelstwo lub obywatelstwa;
 - c) państwo urodzenia;
 - d) płeć.
3. Dane, o których mowa w ust. 1 lit. a) i b) oraz w ust. 2 lit. a), muszą być spseudonimizowane.

Artykuł 44

Przetwarzanie

1. W przypadku gdy państwo członkowskie lub Europol składa zapytanie w celu kwerendy, przesyła dane, o których mowa w art. 43.

EPRIS przesyła zapytanie w celu kwerendy do indeksów krajowego rejestru policyjnego państw członkowskich wraz z danymi przekazanymi przez pytające państwo członkowskie lub Europol i zgodnie z niniejszym rozporządzeniem.

2. Po otrzymaniu od EPRIS zapytania w celu kwerendy każde odpytywane państwo członkowskie w sposób zautomatyzowany i bezzwłocznie uruchamia kwerendę w indeksie krajowego rejestru policyjnego.
3. Wszelkie dopasowania wynikające z kwerend, o których mowa w ust. 1, w indeksach rejestrów policyjnych każdego z odpytywanych państw członkowskich są w sposób zautomatyzowany odsyłane do EPRIS.
4. EPRIS w sposób zautomatyzowany zwraca pytającemu państwu członkowskiemu lub Europolowi listę dopasowań. Lista dopasowań zawiera informacje o jakości dopasowania oraz o państwie członkowskiemu lub państwach członkowskich, których indeksy rejestru policyjnego zawierają dane wykazujące dopasowanie lub dopasowania.
5. Po otrzymaniu listy dopasowań pytające państwo członkowskie podejmuje decyzję o tym, które dopasowania wymagają działań następczych, i za pośrednictwem aplikacji SIENA przesyła odpytywanemu państwu członkowskiemu lub odpytywanym państwom członkowskim uzasadnione zapytanie o działania następcze zawierający dane, o których mowa w art. 25 i 27, oraz wszelkie dodatkowe istotne informacje. Odpytywane państwo członkowskie lub odpytywane państwa członkowskie niezwłocznie przetwarzają takie zapytania, aby podjąć decyzję o ewentualnym udostępnieniu danych przechowywanych w ich bazie danych.
6. Komisja przyjmuje akty wykonawcze określające procedurę techniczną, zgodnie z którą EPRIS dokonuje kwerendy w indeksach krajowego rejestru policyjnego państw członkowskich, oraz formatu i maksymalnej liczby odpowiedzi. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

*Artykuł 45***Prowadzenie rejestrów**

1. Każde uczestniczące państwo członkowskie i Europol prowadzą rejestry wszystkich operacji przetwarzania danych w EPRIS. Rejestry te obejmują:
 - a) informację czy zapytania w celu kwerendy dokonało państwo członkowskie czy Europol; w przypadku gdy zapytania w celu kwerendy dokonało państwo członkowskie – nazwa danego państwa członkowskiego;
 - b) datę i godzinę zapytania;
 - c) datę i godzinę odpowiedzi;
 - d) krajowe bazy danych, do których przesłano zapytanie w celu kwerendy;
 - e) krajowe bazy danych, z których otrzymano odpowiedź.
2. Każde uczestniczące państwo członkowskie prowadzi rejestry zapytań w celu kwerendy dokonywanych przez personel jego właściwych organów należycie upoważniony do korzystania z EPRIS. Europol prowadzi rejestry zapytań w celu kwerendy dokonywanych przez jej należycie upoważniony personel.
3. Rejestry, o których mowa w ust. 1 i 2, wykorzystuje się wyłącznie w celu zbierania danych statystycznych, monitorowania ochrony danych, w tym sprawdzania dopuszczalności kwerendy 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 trzy lata po utworzeniu. Jeżeli jednak są konieczne do prowadzenia już rozpoczętych procedur monitorowania, są one usuwane, gdy tylko przestają być konieczne do celu tych procedur.
4. Na potrzeby monitorowania ochrony danych, w tym sprawdzania dopuszczalności kwerendy i zgodności przetwarzania danych z prawem, administratorzy danych mają dostęp do rejestrów w celu monitorowania własnej działalności, o którym mowa w art. 55.

*Artykuł 46***Procedury powiadamiania w przypadku braku technicznej możliwości korzystania z EPRIS**

1. Jeśli korzystanie z EPRIS w celu kwerendy w indeksie lub indeksach krajowego rejestru policyjnego nie jest technicznie możliwe z powodu awarii infrastruktury Europolu, Europol automatycznie powiadamia o tym fakcie państwa członkowskie. Europol niezwłocznie podejmuje działania mające na celu usunięcie braku technicznej możliwości korzystania z EPRIS.
2. Jeśli korzystanie z EPRIS w celu kwerendy w indeksie lub indeksach krajowego rejestru policyjnego nie jest technicznie możliwe z powodu awarii infrastruktury krajowej w jednym z państw członkowskich, to państwo członkowskie automatycznie powiadamia o tym fakcie pozostałe państwa członkowskie, Komisję i Europol. Państwo członkowskie niezwłocznie podejmuje działania mające na celu usunięcie braku technicznej możliwości korzystania z EPRIS.

ROZDZIAŁ 4

Wymiana danych po stwierdzeniu dopasowania*Artykuł 47***Wymiana danych podstawowych**

1. Zbiór danych podstawowych jest odsyłany za pośrednictwem routera w ciągu 48 godzin od spełnienia wszystkich następujących warunków:
 - a) w wyniku procedur, o których mowa w art. 6, 11 lub 20, stwierdzono dopasowanie między danymi wykorzystanymi do przeszukania i danymi przechowywanymi w bazie danych odpytywanego państwa członkowskiego lub odpytywanych państw członkowskich;

- b) dopasowanie, o którym mowa w lit. a) niniejszego ustępu, zostało ręcznie potwierdzone przez wykwalifikowanego pracownika pytającego państwa członkowskiego, o czym mowa w art. 6 ust. 6, art. 11 ust. 2 i art. 20 ust. 2, lub, w przypadku profili DNA, o których mowa w art. 6 ust. 7 – odpytywanego państwa członkowskiego;
- c) przekazano opis faktów i wskazanie przestępstwa leżącego u jego podstaw, przy użyciu wspólnej tabeli kategorii przestępstw określonej w akcie wykonawczym, który ma zostać przyjęty zgodnie z art. 11b ust. 1 lit. a) decyzji ramowej 2009/315/WSiSW, przez pytające państwo członkowskie, lub – w przypadku profili DNA, o których mowa w art. 6 ust. 7 – przez odpytywane państwo członkowskie, w celu oceny proporcjonalności zapytania, w tym wagi przestępstwa, w odniesieniu do którego przeprowadzono wyszukiwanie, zgodnie z prawem krajowym państwa członkowskiego dostarczającego zbiór danych podstawowych.

2. W przypadku gdy na podstawie prawa krajowego dane państwo członkowskie może dostarczyć konkretny zbiór danych podstawowych dopiero po uzyskaniu zgody organu sądowego, to państwo członkowskie może odstąpić od terminu określonego w ust. 1, o ile jest to konieczne do uzyskania takiej zgody.

3. Zbiór danych podstawowych, o których mowa w ust. 1 niniejszego artykułu, jest odsyłany przez odpytywane państwo członkowskie lub – przypadku profili DNA, o których mowa w art. 6 ust. 7 – przez pytające państwo członkowskie.

4. W przypadku gdy potwierdzone dopasowanie dotyczy zidentyfikowanych danych osoby, zbiór danych podstawowych, o którym mowa w ust. 1, zawiera następujące dane, o ile są one dostępne:

- a) imię lub imiona;
- b) nazwisko lub nazwiska;
- c) alias lub alias-y oraz poprzednio używane imię i nazwisko lub imiona i nazwiska;
- d) datę urodzenia;
- e) obywatelstwo lub obywatelstwa;
- f) miejsce i państwo urodzenia;
- g) płeć;
- h) datę i miejsce pozyskania danych biometrycznych;
- i) przestępstwo, w związku z którym pozyskano dane biometryczne;
- j) sygnaturę sprawy karnej;
- k) właściwy organ odpowiedzialny za sprawę karną.

5. Jeżeli potwierdzone dopasowanie dotyczy niezidentyfikowanych danych lub śladów, zbiór danych podstawowych, o którym mowa w ust. 1, zawiera następujące dane, o ile są one dostępne:

- a) datę i miejsce pozyskania danych biometrycznych;
- b) przestępstwo, w związku z którym pozyskano dane biometryczne;
- c) sygnaturę sprawy karnej;
- d) właściwy organ odpowiedzialny za sprawę karną.

6. Odesłanie podstawowych danych przez odpytywane państwo członkowskie lub, w sprawie dotyczącej profili DNA, o której mowa w art. 6 ust. 7, przez pytające państwo członkowskie, jest uzależnione od decyzji podjętej przez człowieka.

ROZDZIAŁ 5

Europol

Artykuł 48

Dostęp państw członkowskich do danych biometrycznych przekazanych przez państwa trzecie i przechowywanych przez Europol

1. Zgodnie z rozporządzeniem (UE) 2016/794 państwa członkowskie mają dostęp do danych biometrycznych, które państwa trzecie przekazały Europolowi do celów określonych w art. 18 ust. 2 lit. a), b) i c) rozporządzenia (UE) 2016/794, oraz mogą przeszukać te dane za pośrednictwem routera.
2. Jeżeli w wyniku przeszukania, o którym mowa w ust. 1, stwierdzono dopasowanie między danymi wykorzystanymi do przeszukania a przekazanymi przez państwo trzecie danymi przechowywanymi przez Europol, podejmuje się działania następcze zgodnie z rozporządzeniem (UE) 2016/794.

Artykuł 49

Dostęp Europolu do danych przechowywanych w bazach danych państw członkowskich, przy użyciu danych przekazanych przez państwa trzecie

1. W przypadku gdy jest to konieczne do osiągnięcia celów wyznaczonych art. 3 rozporządzenia (UE) 2016/794, zgodnie z tym rozporządzeniem oraz z niniejszym rozporządzeniem Europol ma dostęp do danych, które są przechowywane przez państwa członkowskie w ich krajowych bazach danych i indeksach rejestru policyjnego.
2. Kwerendy Europolu wykorzystujące dane biometryczne jako kryterium przeszukania przeprowadza się z wykorzystaniem routera.
3. Kwerendy Europolu wykorzystujące dane rejestracyjne pojazdów jako kryterium przeszukania przeprowadza się z wykorzystaniem EUCARIS.
4. Kwerendy Europolu wykorzystujące jako kryterium przeszukania dane biograficzne osób podejrzanych i osób skazanych, o których mowa w art. 25, przeprowadza się z wykorzystaniem EPRIS.
5. Europol przeprowadza przeszukania przy użyciu danych przekazanych przez państwa trzecie zgodnie z ust. 1–4 niniejszego artykułu wyłącznie wtedy, gdy jest to konieczne do wykonywania jego zadań do celów art. 18 ust. 2 lit. a) i c) rozporządzenia (UE) 2016/794.
6. Jeżeli w wyniku procedur, o których mowa w art. 6, 11 lub 20, stwierdzono dopasowanie między danymi wykorzystanymi do przeszukania a danymi przechowywanymi w krajowej bazie danych odpytywanego państwa członkowskiego lub odpytywanych państw członkowskich Europol informuje o tym wyłącznie zaangażowane państwo członkowskie lub państwa członkowskie.

Odpytywane państwo członkowskie podejmuje decyzję o ewentualnym odesłaniu za pośrednictwem routera zbioru danych podstawowych w ciągu 48 godzin od spełnienia wszystkich następujących warunków:

- a) dopasowanie, o którym mowa w akapicie pierwszy, zostało ręcznie potwierdzone przez wykwalifikowanego członka personelu Europolu;
- b) przekazano opis faktów i wskazanie przestępstwa będącego podstawą zapytania, przy użyciu wspólnej tabeli kategorii przestępstw określonej w akcie wykonawczym, który ma zostać przyjęty na podstawie art. 11b ust. 1 lit. a) decyzji ramowej 2009/315/WSiSW przez Europol, w celu oceny proporcjonalności zapytania, w tym wagi przestępstwa, w odniesieniu do którego przeprowadzono wyszukiwanie, zgodnie z prawem krajowym państwa członkowskiego, które dostarcza zbiór danych podstawowych;
- c) przekazano nazwę państwa trzeciego, które przedstawiło dane;

W przypadku gdy na podstawie prawa krajowego państwo członkowskie może przedstawić konkretny zbiór danych podstawowych dopiero po uzyskaniu zgody organu sądowego, to państwo członkowskie może odstąpić od terminów określonych w akapicie drugim, o ile jest to konieczne do uzyskania takiej zgody.

Jeżeli potwierdzone dopasowanie dotyczy zidentyfikowanych danych osoby, zbior danych podstawowych, o którym mowa w akapicie drugim, w miarę dostępności zawiera następujące dane:

- a) imię lub imiona;
- b) nazwisko lub nazwiska;
- c) alias lub alias-y oraz poprzednio używane imię i nazwisko lub imiona i nazwiska;
- d) datę urodzenia;
- e) obywatelstwo lub obywatelstwa;
- f) miejsce i państwo urodzenia;
- g) płeć;
- h) datę i miejsce pozyskania danych biometrycznych;
- i) przestępstwo, w związku z którym pozyskano dane biometryczne;
- j) sygnaturę sprawy karnej;
- k) właściwy organ odpowiedzialny za sprawę karną.

Jeżeli potwierdzone dopasowanie dotyczy niezidentyfikowanych danych lub śladów, zbior danych podstawowych, o którym mowa w akapicie drugim, w miarę dostępności zawiera następujące dane:

- a) datę i miejsce pozyskania danych biometrycznych;
- b) przestępstwo, w związku z którym pozyskano dane biometryczne;
- c) sygnaturę sprawy karnej;
- d) właściwy organ odpowiedzialny za sprawę karną.

Odesłanie podstawowych danych przez odpytywane państwo członkowskie jest uzależnione od decyzji podjętej przez człowieka.

7. Wykorzystanie przez Europol informacji uzyskanych w wyniku kwerendy dokonanej zgodnie z niniejszym artykułem oraz w wyniku wymiany zbioru danych podstawowych zgodnie z ust. 6 wymaga zgody państwa członkowskiego, w którego bazie danych stwierdzono dopasowanie. W przypadku gdy to państwo członkowskie zezwoli na wykorzystanie takich informacji, posługiwanie się nimi przez Europol regulowane jest rozporządzeniem (UE) 2016/794.

ROZDZIAŁ 6

Ochrona danych

Artykuł 50

Cel przetwarzania danych

1. Przetwarzanie danych osobowych otrzymanych przez państwo członkowskie lub Europol jest dopuszczalne wyłącznie do celów, do których dane zostały dostarczone przez państwo członkowskie, które przekazało dane, zgodnie z niniejszym rozporządzeniem. Przetwarzanie w innych celach jest dopuszczalne wyłącznie za uprzednią zgodą państwa członkowskiego, które przekazało dane.

2. Przetwarzanie danych dostarczonych przez państwo członkowskie lub Europol zgodnie z art. 6, 11, 16, 20 lub 26 jest dopuszczalne wyłącznie, gdy jest to konieczne w celu:

- a) ustalenia, czy występuje dopasowanie między porównywanymi profilami DNA, danymi daktyloskopijnymi, danymi rejestracyjnymi pojazdów, wizerunkami twarzy lub z rejestrami policyjnymi;
- b) wymiany zbiorów danych podstawowych zgodnie z art. 47;
- c) w przypadku stwierdzenia dopasowania tych danych – przygotowania i złożenia wniosku policyjnego lub sądowego o pomoc prawną;
- d) prowadzenia rejestru zgodnie z art. 18, 40 i 45.

3. Po uzyskaniu zautomatyzowanych wyników przeszukania dane otrzymane przez państwo członkowskie lub Europol usuwa się niezwłocznie, chyba że konieczne jest dalsze ich przetwarzanie do celów, o których mowa w ust. 2, lub gdy jest ono dozwolone zgodnie z ust. 1.

4. Przed połączeniem krajowych baz danych z routerem lub EPRIS państwa członkowskie przeprowadzają ocenę skutków dla ochrony danych, o której mowa w art. 27 dyrektywy (UE) 2016/680, i w stosownych przypadkach konsultują się z organem nadzorczym określonym w art. 28 tej dyrektywy. Organ nadzorczy może skorzystać z każdego z uprawnień, którymi dysponuje na mocy art. 47 tej dyrektywy, zgodnie z art. 28 ust. 5 tej dyrektywy.

Artykuł 51

Prawidłowość, stosowność i zatrzymywanie danych

1. Państwa członkowskie i Europol zapewniają poprawność i stosowność danych osobowych przetwarzanych na podstawie niniejszego rozporządzenia. W przypadku gdy odpytywane państwo członkowskie lub Europol uzyskają wiedzę, że dostarczono danych, które są nieścisłe lub nieaktualne, lub danych, których nie należało dostarczyć, bez zbędnej zwłoki powiadamiają o tym państwo członkowskie, które otrzymało dane, lub Europol. Wszystkie zainteresowane państwa członkowskie lub Europol odpowiednio korygują lub usuwają dane bez zbędnej zwłoki. W przypadku gdy państwo członkowskie, które otrzymało dane, lub Europol mają podstawy, by przypuszczać, że otrzymane dane są nieścisłe lub powinny zostać usunięte, informują o tym bez zbędnej zwłoki państwo członkowskie, które przekazało dane.

2. Państwa członkowskie i Europol wprowadzają odpowiednie środki służące aktualizacji danych istotnych do celów niniejszego rozporządzenia.

3. Jeżeli osoba, której dane dotyczą, kwestionuje prawidłowość danych będących w posiadaniu państwa członkowskiego lub Europolu, której prawidłowości dane państwo członkowskie lub Europol nie jest w stanie wiarygodnie ustalić, oraz jeżeli zażąda tego osoba, której dane dotyczą, dane te oznacza się znacznikiem. Wprowadzony znacznik może zostać usunięty przez państwa członkowskie lub Europol jedynie za zgodą osoby, której dane dotyczą, lub na podstawie decyzji właściwego sądu, organu nadzorczego lub Europejskiego Inspektora Ochrony Danych, w zależności od przypadku.

4. Dane, których nie należało dostarczać ani przyjmować, usuwa się. Dane dostarczone i przyjęte zgodnie z prawem usuwa się:

- a) jeżeli nie są lub przestały być niezbędne do celu, w którym zostały dostarczone;
- b) po upływie maksymalnego okresu przechowywania danych określonego na podstawie prawa krajowego państwa członkowskiego, które przekazało dane, w przypadku gdy w chwili dostarczania danych państwo członkowskie poinformowało państwo członkowskie, które otrzymało dane, lub Europol o takim maksymalnym okresie; lub
- c) po upływie maksymalnego okresu przechowywania danych określonego w rozporządzeniu (UE) 2016/794.

W przypadku gdy są podstawy do przypuszczenia, że usunięcie danych spowodowałoby uszczerbek dla interesów osoby, której dane dotyczą, dane nie są usuwane, lecz ogranicza się ich przetwarzanie. W przypadku gdy ograniczono przetwarzanie danych, przetwarza się je jedynie do celu, z uwagi na który zaniechano ich usunięcia.

*Artykuł 52***Przetwarzający dane**

1. eu-LISA jest podmiotem przetwarzającym w rozumieniu art. 3 pkt 12 rozporządzenia (UE) 2018/1725 na potrzeby przetwarzania danych osobowych za pośrednictwem routera.
2. Europol jest podmiotem przetwarzającym w rozumieniu art. 3 pkt 12 rozporządzenia (UE) 2018/1725 na potrzeby przetwarzania danych osobowych za pośrednictwem EPRIS.

*Artykuł 53***Bezpieczeństwo przetwarzania danych**

1. Właściwe organy państw członkowskich, eu-LISA i Europol zapewniają bezpieczeństwo przetwarzania danych osobowych na podstawie niniejszego rozporządzenia. Właściwe organy państw członkowskich, eu-LISA i Europol współpracują w zakresie zadań związanych z bezpieczeństwem.
2. Nie naruszając przepisów art. 33 rozporządzenia (UE) 2018/1725 i art. 32 rozporządzenia (UE) 2016/794, eu-LISA i Europol stosują środki niezbędne do zapewnienia bezpieczeństwa routera i EPRIS odpowiednio, oraz powiązanej z nimi infrastruktury łączności.
3. eu-LISA przyjmuje konieczne środki dotyczące routera, zaś Europol przyjmuje konieczne środki dotyczące EPRIS, 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 – wyłącznie za pomocą niepowtarzalnych identyfikatorów użytkownika oraz poufnych haseł – aby osoby upoważnione do dostępu do routera lub EPRIS miały dostęp jedynie do danych objętych ich upoważnieniem dostępu;
 - h) zapewnienia możliwości sprawdzenia i ustalenia, którym organom można dostarczać dane osobowe przy użyciu sprzętu do przekazywania danych;
 - i) zapewnienia możliwości sprawdzenia i ustalenia, które dane zostały przetworzone w, odpowiednio, routerze lub EPRIS oraz kiedy, przez kogo i w jakim celu zostały one przetworzone;
 - j) uniemożliwienia nieuprawnionego odczytu, kopiowania, modyfikowania lub usuwania danych osobowych w trakcie przekazywania danych osobowych do lub z odpowiednio routera lub EPRIS 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 poprzez zadbanie o właściwe zgłaszanie wszelkich błędów w funkcjonowaniu odpowiednio routera lub EPRIS;
 - 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.

Niezbędne środki, o których mowa w akapicie pierwszym, obejmują plan bezpieczeństwa, plan ciągłości działania i plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej.

Artykuł 54

Incydenty bezpieczeństwa

1. Zdarzenie, które ma lub może mieć wpływ na bezpieczeństwo routera lub EPRIS i może spowodować uszkodzenie lub utratę danych przechowywanych w routerze lub EPRIS, 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. W przypadku incydentu bezpieczeństwa dotyczącego routera eu-LISA i zainteresowane państwa członkowskie lub, w stosownych przypadkach, Europol współpracują ze sobą w celu zapewnienia szybkiego, skutecznego i właściwego reagowania.
3. W przypadku incydentu bezpieczeństwa dotyczącego EPRIS zainteresowane państwa członkowskie i Europol współpracują ze sobą w celu zapewnienia szybkiego, skutecznego i właściwego reagowania.
4. Państwa członkowskie bez zbędnej zwłoki powiadamiają swoje właściwe organy o wszelkich incydentach bezpieczeństwa.

Z zastrzeżeniem art. 92 rozporządzenia (UE) 2018/1725 w przypadku incydentu bezpieczeństwa dotyczącego infrastruktury centralnej routera eu-LISA powiadamia Służbę ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii (CERT-UE) o znaczących cyberzagrożeniach, znaczących podatnościach i znaczących incydentach bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny po uzyskaniu o nich wiedzy. Odpowiednie szczegóły techniczne dotyczące cyberzagrożeń, podatności i incydentów, na podstawie których można podjąć działania i które umożliwiają prewencyjne wykrywanie, reagowanie na incydenty lub stosowanie środków łagodzących, ujawnia się CERT-UE bez zbędnej zwłoki.

Z zastrzeżeniem art. 34 rozporządzenia (UE) 2016/794 i art. 92 rozporządzenia (UE) 2018/1725 w przypadku incydentu bezpieczeństwa dotyczącego infrastruktury centralnej EPRIS Europol powiadamia CERT-UE o znaczących cyberzagrożeniach, znaczących podatnościach i znaczących incydentach bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny po uzyskaniu o nich wiedzy. Odpowiednie szczegóły techniczne dotyczące cyberzagrożeń, podatności i incydentów, na podstawie których można podjąć działania i które umożliwiają prewencyjne wykrywanie, reagowanie na incydenty lub stosowanie środków łagodzących, ujawnia się CERT-UE bez zbędnej zwłoki.

5. Informacja o incydencie bezpieczeństwa, który ma lub może mieć wpływ na funkcjonowanie routera lub na dostępność, integralność i poufność danych, zostaje niezwłocznie przekazana przez odpowiednie państwa członkowskie i agencje unijne pozostałym państwom członkowskim oraz Europolowi i zgłoszona zgodnie z zapewnionym przez eu-LISA planem zarządzania incydentami.
6. Informacja o incydencie bezpieczeństwa, który ma lub może mieć wpływ na funkcjonowanie EPRIS lub na dostępność, integralność i poufność danych, zostaje niezwłocznie przekazana przez odpowiednie państwa członkowskie i agencje unijne pozostałym państwom członkowskim i zgłoszona zgodnie z zapewnionym przez Europol planem zarządzania incydentami.

Artykuł 55

Monitorowanie własnej działalności

1. Państwa członkowskie zapewniają, aby każdy organ uprawniony do użytkowania ram z Prüm II podejmował środki niezbędne do monitorowania własnego przestrzegania przepisów niniejszego rozporządzenia oraz aby w razie potrzeby współpracował z organem nadzorczym. Europol stosuje środki niezbędne do monitorowania własnego przestrzegania niniejszego rozporządzenia oraz, w razie potrzeby, współpracuje z Europejskim Inspektorem Ochrony Danych.

2. Administratorzy danych wprowadzają konieczne środki, aby skutecznie monitorować zgodność przetwarzania danych z niniejszym rozporządzeniem, w tym poprzez częstą weryfikację zapisów w rejestrach, o których mowa w art. 18, 40 i 45. W razie potrzeby i w stosownych przypadkach, współpracują oni z organami nadzorczymi lub z Europejskim Inspektorem Ochrony Danych.

Artykuł 56

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 57

Odpowiedzialność

Jeżeli państwo członkowskie lub – podczas przeprowadzania kwerend zgodnie z art. 49 – Europol nie dopełnią obowiązków spoczywających na nich zgodnie z niniejszym rozporządzeniem i spowoduje to szkodę w routerze lub EPRIS, wówczas to państwo członkowskie lub Europol ponoszą odpowiedzialność za tę szkodę, chyba że – i w zakresie, w jakim – eu-LISA, Europol lub inne państwo członkowskie związane niniejszym rozporządzeniem nie wprowadziły uzasadnionych środków zapobiegających wystąpieniu takiej szkody lub ograniczających jej skutki.

Artykuł 58

Kontrole ze strony Europejskiego Inspektora Ochrony Danych

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

2. eu-LISA 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. 40 i 45, oraz umożliwiają mu uzyskanie dostępu do wszystkich swoich pomieszczeń w dowolnym momencie. Niniejszy ustęp nie narusza uprawnień Europejskiego Inspektora Ochrony Danych na mocy art. 58 rozporządzenia (UE) 2018/1725, a w odniesieniu do Europolu – na mocy art. 43 ust. 3 rozporządzenia (UE) 2016/794.

Artykuł 59

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, aby zapewnić skoordynowany nadzór nad stosowaniem 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 ram z Prüm II.

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 od rozpoczęcia funkcjonowania routera i EPRIS, a następnie co dwa lata, Europejska Rada Ochrony Danych przesyła sprawozdanie ze swojej działalności na podstawie niniejszego artykułu Parlamentowi Europejskiemu, Radzie, Komisji, eu-LISA i Europolowi. W sprawozdaniu tym każdemu państwu członkowskiemu poświęcony jest osobny rozdział przygotowany przez organ nadzorczy danego państwa członkowskiego.

*Artykuł 60***Przekazywanie danych osobowych państwom trzecim i organizacjom międzynarodowym**

Państwo członkowskie przekazuje dane osobowe uzyskane na mocy niniejszego rozporządzenia państwu trzeciemu lub organizacji międzynarodowej wyłącznie zgodnie z rozdziałem V dyrektywy (UE) 2016/680 i w przypadku gdy odpytywane państwo członkowskie udzieliło zgody przed przekazaniem.

Europol przekazuje dane osobowe uzyskane na mocy niniejszego rozporządzenia państwu trzeciemu lub organizacji międzynarodowej wyłącznie w przypadku gdy spełnione są warunki określone w art. 25 rozporządzenia (UE) 2016/794 i gdy odpytywane państwo członkowskie udzieliło zgody przed przekazaniem.

*Artykuł 61***Związek z innymi aktami prawnymi dotyczącymi ochrony danych**

Wszelkie przetwarzanie danych osobowych do celów niniejszego rozporządzenia odbywa się zgodnie z niniejszym rozdziałem oraz z dyrektywą (UE) 2016/680 lub rozporządzeniem (UE) 2018/1725, (UE) 2016/794 lub (UE) 2016/679, stosownie do przypadku.

ROZDZIAŁ 7

Obowiązki*Artykuł 62***Odpowiedzialność za zachowanie należytej staranności**

Państwa członkowskie i Europol z należytą starannością oceniają, czy zautomatyzowana wymiana danych jest objęta celem ram z Prüm II określonym w art. 2 i czy spełnia ona warunki określone w tym artykule, w szczególności w odniesieniu do praw podstawowych.

*Artykuł 63***Szkolenia**

Upoważnionym właściwym organom krajowym państw członkowskich, organom nadzorczym państw członkowskich i Europolu, zapewnia się, stosownie do przypadku, odpowiednie zasoby i szkolenia, w tym w zakresie ochrony danych i prawidłowego przeglądu dopasowań, w celu wykonywania zadań wynikających z niniejszego rozporządzenia.

*Artykuł 64***Obowiązki państw członkowskich**

1. Każde państwo członkowskie odpowiada za:
 - a) podłączenie do infrastruktury routera;
 - b) integrację swoich istniejących krajowych systemów i infrastruktury z routerem;
 - c) organizację swojej istniejącej infrastruktury krajowej, zarządzanie nią, jej funkcjonowanie i utrzymanie oraz jej podłączenie do routera;
 - d) podłączenie do infrastruktury EPRIS;
 - e) integrację swoich istniejących krajowych systemów i infrastruktury z EPRIS;

- f) organizację swojej istniejącej infrastruktury krajowej, zarządzanie nią, jej funkcjonowanie i utrzymanie oraz jej podłączenie do EPRIS;
 - g) zarządzanie dostępem odpowiednio upoważnionego personelu właściwych organów do routera oraz ustalenia dotyczące tego dostępu, zgodnie z niniejszym rozporządzeniem, a także sporządzenie listy takich członków personelu wraz z ich profilami i jej regularną aktualizację;
 - h) zarządzanie dostępem odpowiednio upoważnionego personelu właściwych organów do EPRIS oraz ustalenia dotyczące tego dostępu, zgodnie z niniejszym rozporządzeniem, a także sporządzenie listy takich członków personelu wraz z ich profilami i jej regularną aktualizację;
 - i) zarządzanie dostępem odpowiednio upoważnionego personelu właściwych organów do EUCARIS oraz ustalenia dotyczące tego dostępu, zgodnie z niniejszym rozporządzeniem, a także sporządzenie listy takich członków personelu wraz z ich profilami i jej regularną aktualizację;
 - j) ręczne potwierdzenie przez wykwalifikowany personel dopasowania o którym mowa w art. 6 ust. 6, art. 6 ust. 7, art. 11 ust. 2 i art. 20 ust. 2;
 - k) zapewnienie dostępności danych niezbędnych do wymiany danych zgodnie z art. 5, 10, 16, 19 i 25;
 - l) wymianę informacji zgodnie z art. 6, 11, 16, 20 i 26;
 - m) skorygowanie, aktualizację lub usunięcie wszelkich danych otrzymanych od odpytywanego państwa członkowskiego w terminie 48 godzin od powiadomienia przez odpytywane państwo członkowskie, że przekazane dane są nieprawidłowe, nieaktualne lub zostały przekazane w sposób niezgodny z prawem;
 - n) zgodność z wymaganiami dotyczącymi jakości danych określonymi w niniejszym rozporządzeniu.
2. Każde państwo członkowskie odpowiada za podłączenie swoich właściwych organów do routera, EPRIS i EUCARIS.

Artykuł 65

Obowiązki Europolu

1. Europol odpowiada za zarządzanie dostępem swojego należycie upoważnionego personelu do routera, EPRIS i EUCARIS oraz za ustalenia dotyczące tego dostępu zgodnie z niniejszym rozporządzeniem.
2. Europol jest odpowiedzialny za przetwarzanie kwerend w danych Europolu dokonywanych za pośrednictwem routera. Europol dostosowuje odpowiednio swoje systemy informacyjne.
3. Europol odpowiada za wszelkie techniczne dostosowania infrastruktury Europolu wymagane do ustanowienia podłączenia do routera i EUCARIS.
4. Z zastrzeżeniem przeszukań przeprowadzanych przez Europol na podstawie art. 49, Europol nie ma dostępu do żadnych danych osobowych przetwarzanych za pośrednictwem EPRIS.
5. Europol odpowiada za opracowanie EPRIS we współpracy z państwami członkowskimi. EPRIS zapewnia funkcje określone w art. 42–46.

Europol odpowiada za zarządzanie techniczne EPRIS. Zarządzanie techniczne EPRIS obejmuje wszystkie zadania i rozwiązania techniczne niezbędne do utrzymania funkcjonowania infrastruktury centralnej EPRIS i zapewniające nieprzerwane usługi państwom członkowskim 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 EPRIS, zwłaszcza jeśli chodzi o czas odpowiedzi podczas przesyłania zapytań do krajowych baz danych, zgodnie ze specyfikacją techniczną.

6. Europol zapewnia szkolenie w zakresie technicznego użytkowania EPRIS.
7. Europol odpowiada za procedury przewidziane w art. 48 i 49.

Artykuł 66

Obowiązki eu-LISA w fazie prac projektowych i rozwojowych nad routerem

1. eu-LISA zapewnia zgodnie z niniejszym rozporządzeniem użytkowanie infrastruktury centralnej routera.
2. Router jest obsługiwany przez eu-LISA w jej obiektach technicznych i zapewnia funkcje określone w niniejszym rozporządzeniu zgodnie z warunkami bezpieczeństwa, dostępności, jakości i wydajności, o których mowa w art. 67 ust. 1.
3. eu-LISA odpowiada za opracowanie routera i za wszelkie dostosowania techniczne niezbędne do jego działania.
4. eu-LISA nie ma dostępu do żadnych danych osobowych przetwarzanych za pośrednictwem routera.
5. eu-LISA określa projekt architektury fizycznej routera, w tym jego bezpiecznej infrastruktury łączności, oraz specyfikacje techniczne i ich rozwój, w odniesieniu do infrastruktury centralnej i bezpiecznej infrastruktury łączności. Zarząd eu-LISA zatwierdza projekt pod warunkiem uzyskaniu przychyłnej opinii Komisji. eu-LISA wprowadza też konieczne adaptacje do elementów interoperacyjności wynikające z ustanowienia routera, jak określono w niniejszym rozporządzeniu.
6. eu-LISA opracowuje i wdraża router tak szybko, jak to tylko możliwe, po przyjęciu przez Komisję środków, o których mowa w art. 37 ust. 6. Opracowywanie tych elementów obejmuje stworzenie i wdrożenie specyfikacji technicznych, przeprowadzenie testów oraz ogólną koordynację projektu i zarządzanie nim.
7. W fazie prac projektowych i rozwojowych regularnie odbywają się posiedzenia Komisji ds. Zarządzania Programem, o której mowa w art. 54 rozporządzenia (UE) 2019/817 i w art. 54 rozporządzenia (UE) 2019/818. Zapewnia ona odpowiednie zarządzanie fazą prac projektowych i rozwojowych nad routerem.

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.

Grupa doradcza ds. interoperacyjności, o której mowa w art. 78, spotyka się regularnie do czasu uruchomienia routera. 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 podejmuje działania następcze w odniesieniu do stanu przygotowania państw członkowskich.

Artykuł 67

Obowiązki eu-LISA po uruchomieniu routera

1. Po rozpoczęciu funkcjonowania routera eu-LISA odpowiada za zarządzanie techniczne infrastrukturą centralną routera, w tym za jej 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 niezbędną infrastrukturą łączności.

Zarządzanie techniczne routerem obejmuje wszystkie zadania i rozwiązania techniczne niezbędne do utrzymania funkcjonowania routera i zapewniające nieprzerwane usługi państwom członkowskim i Europołowi 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 routera, zwłaszcza jeśli chodzi o dostępność i czas odpowiedzi podczas przesyłania zapytań do krajowych baz danych i danych Europolu zgodnie ze specyfikacją techniczną.

Router należy opracować i zarządzać nim w taki sposób, by zapewnić szybki, sprawny, efektywny i kontrolowany dostęp, pełną i nieprzerwaną dostępność oraz czas odpowiedzi zgodny z potrzebami operacyjnymi właściwych organów państw członkowskich i Europolu.

2. Bez uszczerbku dla art. 17 regulaminu pracowniczego urzędników Unii Europejskiej, ustanowionego rozporządzeniem Rady (EWG, Euratom, EWWiS) nr 259/68 ⁽¹⁸⁾, eu-LISA stosuje właściwe przepisy dotyczące tajemnicy zawodowej lub nakłada inne równoważne obowiązki zachowania poufności na swoich pracowników zobowiązanych do pracy z danymi przechowywanymi w routerze. Zobowiązanie to stosuje się także po odejściu takiego personelu z urzędu lub z pracy lub po zakończeniu przez niego działalności.

eu-LISA nie ma dostępu do żadnych danych osobowych przetwarzanych za pośrednictwem routera.

3. eu-LISA wypełnia zadania związane z zapewnianiem szkoleń z zakresu technicznego użytkowania routera.

ROZDZIAŁ 8

Zmiany w innych obowiązujących aktach

Artykuł 68

Zmiany w decyzjach 2008/615/WSiSW i 2008/616/WSiSW

1. W decyzji 2008/615/WSiSW zastępuje się art. 1 lit. a), art. 2–6 oraz rozdział 2 sekcje 2 i 3 w odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem od dnia rozpoczęcia stosowania przepisów niniejszego rozporządzenia dotyczących routera, określonego w art. 75 ust. 1. W związku z tym uchyla się art. 1 lit. a), art. 2–6 oraz rozdział 2 sekcje 2 i 3 decyzji 2008/615/WSiSW od dnia rozpoczęcia stosowania przepisów niniejszego rozporządzenia dotyczących routera, określonego w art. 75 ust. 1.

2. W decyzji 2008/616/WSiSW zastępuje się rozdziały 2–5 oraz art. 18, 20 i 21 w odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem od dnia rozpoczęcia stosowania przepisów niniejszego rozporządzenia dotyczących routera, określonego w art. 75 ust. 1. W związku z tym uchyla się rozdziały 2–5 oraz art. 18, 20 i 21 decyzji 2008/616/WSiSW od dnia rozpoczęcia stosowania przepisów niniejszego rozporządzenia dotyczących routera, określonego w art. 75 ust. 1.

Artykuł 69

Zmiany w rozporządzeniu (UE) 2018/1726

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

1) dodaje się artykuł w brzmieniu:

„Artykuł 8d

Zadania związane z routerem Prüm II

⁽¹⁸⁾ Dz.U. L 56 z 4.3.1968, s. 1.

W odniesieniu do routera Prüm II Agencja wykonuje zadania powierzone jej na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/982 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/982 z dnia 13 marca 2024 r. w sprawie zautomatyzowanego przeszukania i zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej oraz zmieniające decyzje Rady 2008/615/WSiSW oraz 2008/616/WSiSW oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1726, (UE) 2019/817 i (UE) 2019/818 („rozporządzenie Prüm II”) (Dz.U. L, 2024/982, 5.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/982/oj>).”;

2) art. 17 ust. 3 akapit drugi otrzymuje brzmienie:

„Zadania związane z rozwojem i zarządzaniem operacyjnym, o których mowa w art. 1 ust. 4 i 5, art. 3–8 i art. 8d, 9 i 11 są wykonywane w centrum technicznym w Strasburgu we Francji.”;

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

a) dodaje się punkt w brzmieniu:

„eeb) przyjmuje sprawozdania ze stanu prac nad opracowaniem routera Prüm II zgodnie z art. 80 ust. 2 rozporządzenia (UE) 2024/982.”;

b) lit. ff) i otrzymuje brzmienie:

„ff) przyjmuje sprawozdania dotyczące następujących kwestii:

- (i) systemu SIS – 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 (**),
- (ii) systemu VIS – na podstawie art. 50 ust. 3 rozporządzenia (WE) nr 767/2008 i art. 17 ust. 3 decyzji 2008/633/WSiSW,
- (iii) systemu EES – na podstawie art. 72 ust. 4 rozporządzenia (UE) 2017/2226,
- (iv) systemu ETIAS – na podstawie art. 92 ust. 4 rozporządzenia (UE) 2018/1240,
- (v) systemu ECRIS-TCN i wzorcowej implementacji ECRIS – na podstawie art. 36 ust. 8 rozporządzenia (UE) 2019/816,
- (vi) elementów interoperacyjności – na podstawie art. 78 ust. 3 rozporządzenia (UE) 2019/817 i art. 74 ust. 3 rozporządzenia (UE) 2019/818,
- (vii) systemu e-CODEX – na podstawie art. 16 ust. 1 rozporządzenia (UE) 2022/850,
- (viii) platformy współpracy JIT na podstawie art. 26 ust. 6 rozporządzenia (UE) 2023/969;
- (ix) routera Prüm II – na podstawie art. 80 ust. 5 rozporządzenia (UE) 2024/982;

(*) 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).

(**) 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).”;

c) lit. hh) otrzymuje brzmienie:

„hh) przyjmuje oficjalne uwagi dotyczące sprawozdań Europejskiego Inspektora Ochrony Danych z audytów, na podstawie art. 56 ust. 2 rozporządzenia (UE) 2018/1861, art. 42 ust. 2 rozporządzenia (WE) nr 767/2008, 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 oraz art. 58 ust. 1 rozporządzenia (UE) 2024/982, a także zapewnia odpowiednie działania w następstwie tych audytów.”

Artykuł 70

Zmiany w rozporządzeniu (UE) 2019/817

W art. 6 ust. 2 rozporządzenia (UE) 2019/817 dodaje się literę w brzmieniu:

„d) bezpiecznej infrastruktury łączności między europejskim portalem wyszukiwania a routerem ustanowionym w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/982 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/982 z dnia 13 marca 2024 r. w sprawie zautomatyzowanego przeszukania i zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej oraz zmieniające decyzje Rady 2008/615/WSiSW i 2008/616/WSiSW oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1726, (UE) 2019/817 i (UE) 2019/818 („rozporządzenie Prüm II”) (Dz.U. L, 2024/982, 5.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/982/oj>).”

Artykuł 71

Zmiany w rozporządzeniu (UE) 2019/818

W rozporządzeniu (UE) 2019/818 wprowadza się następujące zmiany:

1) w art. 6 ust. 2 dodaje się literę w brzmieniu:

„d) bezpiecznej infrastruktury łączności między europejskim portalem wyszukiwania a routerem ustanowionym w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/982 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/982 z dnia 13 marca 2024 r. w sprawie zautomatyzowanego przeszukania i zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej („Prüm II”), zmieniające decyzje Rady 2008/615/WSiSW i 2008/616/WSiSW oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1726, (UE) 2019/817 i (UE) 2019/818 („rozporządzenie Prüm II”) (Dz.U. L, 2024/982, 5.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/982/oj>).”

2) Art. 39 ust. 1 i 2 otrzymują brzmienie:

„1. Centralne repozytorium sprawozdawczo-statystyczne ustanawia się, aby wspierać realizację celów SIS, Eurodac i ECRIS-TCN 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. Centralne repozytorium sprawozdawczo-statystyczne wspiera także osiągnięcie celów rozporządzenia (UE) 2024/982.

2. eu-LISA ustanawia, wdraża i obsługuje w swoich centrach technicznych centralne repozytorium sprawozdawczo-statystyczne zawierające dane i statystyki, o których mowa w art. 74 rozporządzenia (UE) 2018/1862 oraz art. 32 rozporządzenia (UE) 2019/816, logicznie oddzielone według systemu informacyjnego UE. eu-LISA gromadzi również dane i statystyki z routera, o którym mowa w art. 72 ust. 1 rozporządzenia (UE) 2024/982. 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. 74 rozporządzenia (UE) 2018/1862, art. 32 rozporządzenia (UE) 2019/816 oraz art. 72 ust. 1 rozporządzenia (UE) 2024/982.”

ROZDZIAŁ 9

Przepisy końcowe

Artykuł 72

Sprawozdawczość i statystyki

1. W razie potrzeby odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji, Europolu i eu-LISA ma dostęp do następujących danych związanych z routerem wyłącznie do celów sporządzania sprawozdań i statystyk:

- a) liczba kwerend przypadająca na państwo członkowskie i liczba kwerend przypadająca na Europol w podziale na kategorie danych;
- b) liczba kwerend w każdej z połączonych baz danych;
- c) liczba dopasowań w bazie danych każdego państwa członkowskiego w podziale na kategorie danych;
- d) liczba dopasowań w danych Europolu w podziale na kategorie danych;
- e) liczba potwierdzonych dopasowań w przypadkach, w których nastąpiła wymiana danych podstawowych;
- f) liczba potwierdzonych dopasowań w przypadkach, w których nie nastąpiła wymiana danych podstawowych;
- g) liczba kwerend za pośrednictwem routera we wspólnym repozytorium danych umożliwiających identyfikację; oraz
- h) liczba dopasowań według rodzaju w następujący sposób:
 - (i) dane zidentyfikowane (osoba) – dane niezidentyfikowane (ślad);
 - (ii) dane niezidentyfikowane (ślad) – dane zidentyfikowane (osoba);
 - (iii) dane niezidentyfikowane (ślad) – dane niezidentyfikowane (ślad);
 - (iv) dane zidentyfikowane (osoba) – dane zidentyfikowane (osoba).

W oparciu o dane określone w akapicie pierwszym nie może być możliwa identyfikacja poszczególnych osób.

2. Odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji i Europolu ma dostęp do następujących danych związanych z EUCARIS, wyłącznie do celów sporządzania sprawozdań i statystyk:

- a) liczba kwerend przypadająca na państwo członkowskie i liczba kwerend przypadająca na Europol;
- b) liczba kwerend w każdej z połączonych baz danych; oraz
- c) liczba dopasowań w bazie danych każdego państwa członkowskiego.

W oparciu o dane określone w akapicie pierwszym nie może być możliwa identyfikacja poszczególnych osób.

3. Odpowiednio upoważniony personel właściwych organów państw członkowskich, Komisji i Europolu ma dostęp do następujących danych związanych z EPRIS, wyłącznie do celów sporządzania sprawozdań i statystyk:

- a) liczba kwerend przypadająca na państwo członkowskie i liczba kwerend przypadająca na Europol;
- b) liczba kwerend w każdym z połączonych indeksów; oraz
- c) liczba dopasowań w bazie danych każdego państwa członkowskiego.

W oparciu o dane określone w akapicie pierwszym nie może być możliwa identyfikacja poszczególnych osób.

4. eu-LISA przechowuje dane określone w ust. 1 niniejszego artykułu w centralnym repozytorium sprawozdawczo-statystycznym ustanowionym w art. 39 rozporządzenia (UE) 2019/818. Europol przechowuje dane określone w ust. 3. Dane te umożliwiają właściwym organom państw członkowskich, Komisji, eu-LISA i Europolowi uzyskanie sprofilowanych sprawozdań i statystyk w celu zwiększenia efektywności współpracy organów ścigania.

Artykuł 73

Koszty

1. Koszty poniesione w związku z ustanowieniem i funkcjonowaniem routera i EPRIS są pokrywane z budżetu ogólnego Unii.
2. Koszty poniesione w związku z integracją istniejącej krajowej infrastruktury oraz jej podłączeniem do routera i EPRIS i w związku z ustanowieniem krajowych baz danych wizerunków twarzy oraz indeksów krajowego rejestru policyjnego do celów zapobiegania przestępczości, wykrywania przestępstw i prowadzenia postępowań przygotowawczych w sprawach karnych 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. Każde państwo członkowskie ponosi koszty powstałe w wyniku administrowania, użytkowania i konserwacji Euca-ris.
 4. Każde państwo członkowskie ponosi koszty powstałe w wyniku administrowania, użytkowania i konserwacji krajowych podłączeń do routera i EPRIS.

Artykuł 74

Powiadomienia

1. Państwa członkowskie powiadamiają eu-LISA o właściwych organach, o których mowa w art. 36. Organy te mogą korzystać z routera lub uzyskiwać do niego dostęp.
2. eu-LISA powiadamia Komisję o pomyślnym zakończeniu testów, o których mowa w art. 75 ust. 1 lit. b).
3. Europol powiadamia Komisję o pomyślnym zakończeniu testów, o których mowa w art. 75 ust. 3 lit. b).
4. Każde państwo członkowskie powiadamia pozostałe państwa członkowskie, Komisję, eu-LISA i Europol o zawartości swoich krajowych baz danych DNA oraz o warunkach zautomatyzowanego przeszukania, do których zastosowanie mają art. 5 i 6.
5. Każde państwo członkowskie powiadamia pozostałe państwa członkowskie, Komisję, eu-LISA i Europol o zawartości swoich krajowych baz danych daktyloskopijnych oraz o warunkach zautomatyzowanego przeszukania, do których zastosowanie mają art. 10 i 11.
6. Każde państwo członkowskie powiadamia pozostałe państwa członkowskie, Komisję, eu-LISA i Europol o zawartości swoich krajowych baz danych wizerunków twarzy oraz o warunkach zautomatyzowanego przeszukania, do których zastosowanie mają art. 19 i 20.

7. Państwa członkowskie uczestniczące w zautomatyzowanej wymianie informacji z rejestrów policyjnych na podstawie art. 25 i 26 powiadamiają pozostałe państwa członkowskie, Komisję i Europol o zawartości swoich indeksów krajowego rejestru policyjnego, krajowych baz danych wykorzystywanych do tworzenia tych indeksów oraz o warunkach zautomatyzowanego przeszukania.

8. Państwa członkowskie powiadamiają Komisję, eu-LISA i Europol o swoich krajowych punktach kontaktowych wyznaczonych na podstawie art. 30. Komisja sporządza wykaz krajowych punktów kontaktowych, o których została powiadomiona, i udostępnia go wszystkim państwom członkowskim.

Artykuł 75

Uruchomienie systemu

1. Komisja określa w drodze aktu wykonawczego datę, od której państwa członkowskie i Europol mogą rozpocząć korzystanie z routera, gdy zostaną spełnione następujące warunki:

- a) przyjęto środki, o których mowa w art. 5 ust. 3, art. 8 ust. 2 i 3, art. 13 ust. 2 i 3, art. 17 ust. 3, art. 22 ust. 2 i 3, art. 31 oraz art. 37 ust. 6;
- b) eu-LISA oświadczyła, że pomyślnie ukończono wszechstronny test routera, który przeprowadziła we współpracy z właściwymi organami państw członkowskich i z Europolem.

Komisja określa w drodze aktu wykonawczego, o którym mowa w akapicie pierwszym, datę, od której państwa członkowskie i Europol mają rozpocząć korzystanie z routera. Data ta przypada rok od daty określonej zgodnie z akapitem pierwszym.

Komisja może przesunąć datę, od której państwa członkowskie i Europol mają rozpocząć korzystanie z routera, maksymalnie o jeden rok, jeżeli ocena wdrożenia routera wykaże, że takie przesunięcie jest konieczne.

2. Dwa lata po rozpoczęciu działania routera państwa członkowskie zapewniają dostępność wizerunków twarzy, zgodnie z art. 19, do celów zautomatyzowanego przeszukania wizerunków twarzy, o którym mowa w art. 20.

3. Komisja określa w drodze aktu wykonawczego datę, od której państwa członkowskie i Europol mają rozpocząć korzystanie z EPRIS, gdy zostaną spełnione następujące warunki:

- a) przyjęto środki, o których mowa w art. 44 ust. 6;
- b) Europol oświadczył, że pomyślnie ukończono wszechstronny test EPRIS, który przeprowadził we współpracy z właściwymi organami państw członkowskich.

4. Komisja określa w drodze aktu wykonawczego datę, od której Europol ma udostępniać państwom członkowskim dane biometryczne pochodzące od państw trzecich zgodnie z art. 48, gdy zostaną spełnione następujące warunki:

- a) router został uruchomiony;
- b) Europol oświadczył, że pomyślnie ukończono wszechstronny test jego połączenia z routerem, który przeprowadził we współpracy z właściwymi organami państw członkowskich i z eu-LISA.

5. Komisja określa w drodze aktu wykonawczego datę, od której Europol otrzymuje dostęp do danych przechowywanych w bazach danych państw członkowskich zgodnie z art. 49, gdy zostaną spełnione następujące warunki:

- a) router został uruchomiony;

- b) Europol oświadczył, że pomyślnie ukończono wszechstronny test jego połączenia z routerem, który przeprowadził we współpracy z właściwymi organami państw członkowskich i z eu-LISA.
6. Akty wykonawcze, o których mowa w niniejszym artykule, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 77 ust. 2.

Artykuł 76

Przepisy przejściowe i odstęstwa

1. Państwa członkowskie i agencje unijne rozpoczynają stosowanie art. 19–22, art. 47 i art. 49 ust. 6 od daty określonej zgodnie z art. 75 ust. 1 akapit pierwszy, z wyjątkiem państw członkowskich, które nie rozpoczęły korzystania z routera.
2. Państwa członkowskie i agencje unijne rozpoczynają stosowanie art. 25–28 i art. 49 ust. 4 od daty określonej zgodnie z art. 75 ust. 3.
3. Państwa członkowskie i agencje unijne rozpoczynają stosowanie art. 48 od daty określonej zgodnie z art. 75 ust. 4.
4. Państwa członkowskie i agencje unijne rozpoczynają stosowanie art. 49 ust. 1, 2, 3, 5 i 7 od daty określonej zgodnie z art. 75 ust. 5.

Artykuł 77

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

Artykuł 78

Grupa doradcza ds. interoperacyjności

Zakres obowiązków grupy doradczej ds. interoperacyjności eu-LISA, ustanowionej na podstawie art. 75 rozporządzenia (UE) 2019/817 oraz art. 71 rozporządzenia (UE) 2019/818 zostaje rozszerzony o router. Ta grupa doradcza ds. interoperacyjności zapewnia eu-LISA wiedzę fachową związaną z routerem, w szczególności w kontekście przygotowywania rocznego programu prac oraz rocznego sprawozdania z działalności.

Artykuł 79

Praktyczny podręcznik

Komisja, w ścisłej współpracy z państwami członkowskimi, eu-LISA, Europelem i Agencją Praw Podstawowych Unii Europejskiej udostępnia praktyczny podręcznik na potrzeby wdrażania niniejszego rozporządzenia i zarządzania tym rozporządzeniem. Ten praktyczny podręcznik zawiera wytyczne o charakterze technicznym i operacyjnym, zalecenia i najlepsze praktyki. Komisja przyjmuje praktyczny podręcznik w formie zalecenia przed rozpoczęciem działania zarówno routera, jak i EPRIS. Komisja regularnie i w razie potrzeby aktualizuje praktyczny podręcznik.

Artykuł 80

Monitorowanie i ocena

1. eu-LISA zapewnia istnienie procedur monitorowania tworzenia routera pod kątem realizacji celów dotyczących planowania i kosztów oraz procedur monitorowania jego funkcjonowania pod kątem realizacji celów dotyczących rezultatów technicznych, opłacalności, bezpieczeństwa i jakości usług.

Europol zapewnia istnienie procedur monitorowania tworzenia EPRIS pod kątem realizacji celów dotyczących planowania i kosztów oraz procedur monitorowania jego funkcjonowania pod kątem realizacji celów dotyczących rezultatów technicznych, opłacalności, bezpieczeństwa i jakości usług.

2. Do dnia 26 kwietnia 2025 r., a następnie co roku w trakcie fazy rozwojowej routera eu-LISA przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie z aktualnej sytuacji w zakresie opracowywania routera. Sprawozdania te zawierają szczegółowe informacje na temat poniesionych kosztów oraz informacje dotyczące wszelkich rodzajów ryzyka, które mogą mieć wpływ na ogólne koszty pokrywane z budżetu ogólnego Unii zgodnie z art. 73.

Po zakończeniu prac rozwojowych nad routerem eu-LISA przekazuje Parlamentowi Europejskiemu i Radzie sprawozdanie zawierające szczegółowe wyjaśnienia dotyczące sposobu osiągnięcia celów, w szczególności w zakresie planowania i kosztów, i zawierające uzasadnienie wszelkich rozbieżności.

3. Do dnia 26 kwietnia 2025 r., a następnie co roku w trakcie fazy rozwojowej EPRIS Europol przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie na temat stanu rozwoju EPRIS. Sprawozdania te zawierają szczegółowe informacje o poniesionych kosztach oraz informacje o wszelkich zagrożeniach, które mogą mieć wpływ na ogólne koszty pokrywane z budżetu ogólnego Unii zgodnie z art. 73.

Po zakończeniu prac rozwojowych nad EPRIS Europol przekazuje Parlamentowi Europejskiemu i Radzie sprawozdanie zawierające szczegółowe wyjaśnienia dotyczące sposobu osiągnięcia celów, w szczególności w zakresie planowania i kosztów, i zawierające uzasadnienie wszelkich rozbieżności.

4. Na potrzeby konserwacji technicznej eu-LISA ma dostęp do niezbędnych informacji związanych z operacjami przetwarzania danych przeprowadzanymi w routerze. Na potrzeby konserwacji technicznej Europol ma dostęp do niezbędnych informacji związanych z operacjami przetwarzania danych przeprowadzanymi w EPRIS.

5. Po upływie dwóch lat od uruchomienia routera, a następnie co dwa lata, eu-LISA przedkłada Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie dotyczące technicznego funkcjonowania routera, w tym jego bezpieczeństwa.

6. Po upływie dwóch lat od uruchomienia EPRIS, a następnie co dwa lata, Europol przedkłada Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie dotyczące technicznego funkcjonowania EPRIS, w tym jego bezpieczeństwa.

7. Po upływie trzech lat od uruchomienia routera i EPRIS, o których mowa w art. 75, a następnie co cztery lata Komisja sporządza sprawozdanie z ogólnej oceny ram z Prüm II.

Po upływie roku od uruchomienia routera, a następnie co dwa lata, Komisja sporządza sprawozdanie z oceny korzystania z wizerunków twarzy na podstawie niniejszego rozporządzenia.

Sprawozdania, o których mowa w akapicie pierwszym i drugim obejmują:

- a) ocenę stosowania niniejszego rozporządzenia, w tym jego stosowania przez każde państwo członkowskie i Europol;
- b) analizę osiągniętych wyników w stosunku do celów niniejszego rozporządzenia i ocenę jego wpływu na prawa podstawowe;
- c) wpływ, skuteczność i wydajność funkcjonowania ram z Prüm II i metod pracy w świetle jego celów, mandatu i zadań;

d) ocenę bezpieczeństwa ram z Prüm II;

Komisja przekazuje te sprawozdania Parlamentowi Europejskiemu, Radzie, Europejskiemu Inspektorowi Danych Osobowych i Agencji Praw Podstawowych Unii Europejskiej.

8. W sprawozdaniach, o których mowa w ust. 7 akapit pierwszy Komisja zwraca szczególną uwagę na następujące nowe kategorie danych: wizerunki twarzy i informacje z rejestrów policyjnych. Komisja uwzględni w takich sprawozdaniach korzystanie z tych nowych kategorii danych przez każde państwo członkowskie i Europol, oraz ich wpływ, skuteczność i wydajność. W sprawozdaniach, o których mowa w ust. 7 akapit drugi, Komisja zwraca szczególną uwagę na ryzyko fałszywych dopasowań i na jakość danych.

9. Państwa członkowskie i Europol dostarczają eu-LISA i Komisji informacji niezbędnych do sporządzania sprawozdań, o których mowa w ust. 2 i 5. Informacje te nie mogą stwarzać zagrożenia dla metod pracy ani ujawniać źródeł, członków personelu lub postępowań przygotowawczych prowadzonych przez właściwe organy państw członkowskich.

10. Państwa członkowskie przekazują Komisji i Europolowi informacje niezbędne do sporządzania sprawozdań, o których mowa w ust. 3 i 6. Informacje te nie mogą stwarzać zagrożenia dla metod pracy ani ujawniać źródeł, członków personelu lub postępowań przygotowawczych prowadzonych przez właściwe organy państw członkowskich.

11. Z zastrzeżeniem wymogów dotyczących poufności państwa członkowskie, eu-LISA i Europol przekazują Komisji informacje niezbędne do przeprowadzenia sprawozdań, o których mowa w ust. 7. Państwa członkowskie przekazują również Komisji liczbę potwierdzonych dopasowań w bazie danych każdego państwa członkowskiego w podziale na kategorie i rodzaj danych. Informacje te nie mogą stwarzać zagrożenia dla metod pracy ani ujawniać źródeł, członków personelu lub postępowań przygotowawczych prowadzonych przez właściwe organy państw członkowskich.

Artykuł 81

Wejście w życie i stosowanie

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

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

Sporządzono w Strasburgu dnia 13 marca 2024 r.

W imieniu Parlamentu Europejskiego
Przewodnicząca
R. METSOLA

W imieniu Rady
Przewodnicząca
H. LAHBIB