# Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie wniosków dotyczących dwóch rozporządzeń ustanawiających ramy interoperacyjności między wielkoskalowymi systemami informacyjnymi UE

*(Pełny tekst niniejszej opinii jest dostępny w wersji angielskiej, francuskiej i niemieckiej na stronie internetowej EIOD www.edps.europa.eu)*

(2018/C 233/07)

Obecne pilne wyzwania związane z bezpieczeństwem i zarządzaniem granicami wymagają inteligentniejszego wykorzystania informacji już dostępnych właściwym organom publicznym. Skłoniło to Komisję Europejską do rozpoczęcia procesu zmierzającego do osiągnięcia interoperacyjności (obecnych i przyszłych) wielkoskalowych systemów informacyjnych UE w dziedzinie migracji, azylu i bezpieczeństwa. W grudniu 2017 r. Komisja wydała dwa wnioski dotyczące rozporządzeń, które ustanawiają ramy prawne dla interoperacyjności między unijnymi wielkoskalowymi systemami informacyjnymi.

Interoperacyjność, pod warunkiem że jest wdrażana w sposób przemyślany i w pełnej zgodności z prawami podstawowymi, w tym z prawem do prywatności i ochrony danych, może być użytecznym narzędziem służącym zaspokajaniu uzasadnionych potrzeb właściwych organów korzystających z wielkoskalowych systemów informacyjnych oraz przyczynianiu się do rozwoju skutecznej i wydajnej wymiany informacji. Interoperacyjność jest nie tylko, czy przede wszystkim, wyborem technicznym, ale raczej wyborem politycznym, który może mieć poważne konsekwencje prawne i społeczne, których nie można ukryć za rzekomo technicznymi zmianami. Decyzja prawodawcy Unii o uczynieniu wielkoskalowych systemów informatycznych interoperacyjnymi miałaby nie tylko trwały i głęboki wpływ na ich strukturę i sposób działania, ale także zmieniłaby dotychczasowy sposób interpretowania zasad prawnych w tej dziedzinie, co stanowiłoby „punkt bez powrotu".

Chociaż początkowo interoperacyjność mogła być przewidziana jako narzędzie ułatwiające jedynie korzystanie z systemów, wnioski wprowadziłyby nowe możliwości dostępu do danych przechowywanych w różnych systemach i korzystania z takich danych w celu zwalczania oszustw dotyczących tożsamości, ułatwienia kontroli tożsamości, a także usprawnienia dostępu organów ścigania do nieprawnych systemów informacyjnych.

W szczególności wnioski tworzą nową scentralizowaną bazę danych, która zawierałaby informacje o milionach obywateli państw trzecich, w tym ich dane biometryczne. Ze względu na skalę i charakter danych, które mają być przechowywane w tej bazie danych, konsekwencje wszelkich naruszeń bezpieczeństwa danych mogłyby poważnie zaszkodzić potencjalnie bardzo dużej liczbie osób fizycznych. Jeżeli takie informacje kiedykolwiek znalazłyby się w niewłaściwych rękach, baza danych mogłaby stać się niebezpiecznym narzędziem wykorzystywanym przeciwko prawom podstawowym. Dlatego konieczne jest stworzenie silnych zabezpieczeń prawnych, technicznych i organizacyjnych. Szczególną czujność należy zachować zarówno w odniesieniu do celów bazy danych, jak i jej warunków i sposobów wykorzystania.

W tym kontekście EIOD podkreśla znaczenie dalszego wyjaśnienia zakresu problemu oszustw dotyczących tożsamości wśród obywateli państw trzecich, aby zapewnić, że proponowany środek jest odpowiedni i proporcjonalny. Możliwość korzystania ze scentralizowanej bazy danych w celu ułatwienia kontroli tożsamości na terytorium państw członkowskich powinna zostać ograniczona.

EIOD rozumie potrzebę korzystania przez organy ścigania z najlepszych możliwych narzędzi do szybkiej identyfikacji sprawców aktów terrorystycznych i innych poważnych przestępstw. Ułatwienie organom ścigania dostępu do systemów innych niż systemy egzekwowania prawa (tj. do informacji uzyskanych przez organy do celów innych niż egzekwowanie prawa), nawet w ograniczonym zakresie, nie jest jednak bez znaczenia z punktu widzenia praw podstawowych. Rutynowy dostęp stanowiłby poważne naruszenie zasady ograniczenia celu. EIOD wzywa zatem do utrzymania autentycznych zabezpieczeń w celu ochrony praw podstawowych obywateli państw trzecich.

Ponadto EIOD pragnie podkreślić, że zarówno pod względem prawnym, jak i technicznym, wnioski zwiększają złożoność istniejących systemów, jak również tych, które są nadal w fazie opracowywania, a ich dokładne implikacje są trudne do oceny na tym etapie. Złożoność ta będzie miała wpływ nie tylko na ochronę danych, ale również na zarządzanie systemami i nadzór nad nimi. Na obecnym etapie trudno jest w pełni ocenić dokładne konsekwencje dla praw i wolności, które stanowią podstawę projektu UE. Z tych powodów EIOD wzywa do szerszej debaty na temat przyszłości wymiany informacji w UE, zarządzania nimi oraz sposobów ochrony praw podstawowych w tym kontekście.

## 1. **WPROWADZENIE**

### 1.1. **Kontekst**

1. W kwietniu 2016 r. Komisja przyjęła komunikat „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa" ([1]), który zapoczątkował dyskusję na temat tego, w jaki sposób systemy informacyjne w Unii Europejskiej mogłyby lepiej usprawnić zarządzanie granicami i bezpieczeństwo wewnętrzne.

2. W czerwcu 2016 r., w następstwie komunikatu, Komisja powołała grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności (ang. *high-level expert group*, „HLEG"). Zadaniem tej grupy było sprostanie prawnym, technicznym i operacyjnym wyzwaniom związanym z interoperacyjnością centralnych systemów UE w zakresie granic i bezpieczeństwa ([2]).

3. Grupa ta przedstawiła zalecenia najpierw w swoim wstępnym sprawozdaniu z grudnia 2016 r. ([3]), a następnie w swoim sprawozdaniu końcowym z maja 2017 r. ([4]) EIOD został zaproszony do udziału w pracach HLEG i wydał oświadczenie na temat koncepcji interoperacyjności w dziedzinie migracji, azylu i bezpieczeństwa, które zawarto w sprawozdaniu końcowym HLEG.

4. W oparciu o komunikat z 2016 r. i zalecenia grupy ekspertów wysokiego szczebla Komisja zaproponowała nowe podejście, zgodnie z którym wszystkie scentralizowane systemy informacyjne UE w zakresie zarządzania bezpieczeństwem, granicami i migracją byłyby interoperacyjne ([5]). Komisja ogłosiła zamiar podjęcia prac nad utworzeniem europejskiego portalu wyszukiwania, wspólnego serwisu kojarzenia danych biometrycznych oraz wspólnego repozytorium tożsamości.

5. W dniu 8 czerwca 2017 r. Rada z zadowoleniem przyjęła stanowisko Komisji i proponowany sposób osiągnięcia interoperacyjności systemów informacyjnych do roku 2020 ([6]). W dniu 27 lipca 2017 r. Komisja rozpoczęła konsultacje publiczne w sprawie interoperacyjności systemów informacyjnych UE w zakresie granic i bezpieczeństwa ([7]). Konsultacjom towarzyszyła wstępna ocena skutków.

6. W dniu 17 listopada 2017 r. EIOD wydał – jako wkład dodatkowy – dokument analityczny na temat interoperacyjności systemów informacyjnych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości ([8]). W dokumencie tym uznał, że interoperacyjność, po wdrożeniu jej w przemyślany sposób oraz zgodnie z podstawowymi wymogami konieczności i proporcjonalności, może być użytecznym narzędziem służącym zaspokojeniu uzasadnionych potrzeb właściwych organów korzystających z wielkoskalowych systemów informacyjnych, w tym usprawnieniu wymiany informacji.

7. W dniu 12 grudnia 2017 r. Komisja opublikowała dwa wnioski ustawodawcze („wnioski") dotyczące:

   — rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniające decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399 i rozporządzenie (UE) 2017/2226, zwane dalej „wnioskiem w sprawie granic i wiz",

   — rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności pomiędzy systemami informacyjnymi UE (współpraca policyjna i sądowa, azyl i migracja), zwanego dalej „wnioskiem dotyczącym współpracy policyjnej i sądowej, azylu i migracji".

([1]) Komunikat Komisji do Parlamentu Europejskiego i Rady „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa", COM(2016) 205 final z 6.4.2017.

([2]) Tamże, s. 15.

([3]) Wstępne sprawozdanie przewodniczącego grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności powołanej przez Komisję Europejską, wstępne sprawozdanie przewodniczącego grupy ekspertów wysokiego szczebla, grudzień 2016 r., dostępne na stronie: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.

([4]) Sprawozdanie końcowe grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności powołanej przez Komisję Europejską, 11 maja 2017 r., dostępne na stronie internetowej: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.

([5]) Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej i Rady „Siódme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa", COM(2017) 261 final z 16.5.2017.

([6]) Konkluzje Rady w sprawie dalszych prac nad usprawnieniem wymiany informacji i zapewnieniem interoperacyjności unijnych systemów informacyjnych, 8 czerwca 2017 r.: http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/pl/pdf.

([7]) Konsultacje publiczne i ocena skutków są dostępne na stronie: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en.

([8]) https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf.

1.2. **Cele wniosków**

8. Wnioski zasadniczo mają na celu poprawę zarządzania granicami zewnętrznymi Schengen i przyczynienie się do bezpieczeństwa wewnętrznego Unii Europejskiej. W tym celu ustanawiają one ramy zapewniające interoperacyjność istniejących i przyszłych wielkoskalowych systemów informacyjnych UE w dziedzinie odprawy granicznej, azylu i imigracji, współpracy policyjnej i współpracy sądowej w sprawach karnych.

9. Elementy interoperacyjności ustanowione we wnioskach obejmowałyby:

— trzy istniejące systemy: system informacyjny Schengen (SIS), system Eurodac oraz wizowy system informacyjny (VIS),

— trzy proponowane systemy, które są nadal w przygotowaniu lub w trakcie opracowywania:

— uzgodniony niedawno przez prawodawców Unii i wymagający rozwinięcia: system wjazdu/wyjazdu (EES) ([1]), oraz

— dwa systemy, które są nadal przedmiotem negocjacji: proponowany europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) ([2]) oraz proponowany europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN) ([3]),

— bazę Interpolu zawierającą dane skradzionych lub utraconych dokumentów podróży (baza danych SLTD), oraz

— dane Europolu ([4]).

10. Interoperacyjność między tymi systemami składa się z czterech elementów:

— europejskiego portalu wyszukiwania,

— wspólnego serwisu kojarzenia danych biometrycznych,

— wspólnego repozytorium tożsamości, oraz

— modułu wykrywającego multiplikację tożsamości.

11. Europejski portal wyszukiwania działałby jako pośrednik komunikatów. Jego celem jest zapewnienie prostego interfejsu, który szybko dostarczyłby wyniki zapytań w przejrzysty sposób. Umożliwiłoby to jednoczesne wyszukiwanie danych w różnych systemach przy użyciu danych identyfikacyjnych (zarówno biograficznych, jak i biometrycznych). Innymi słowy, użytkownik końcowy mógłby przeprowadzić pojedyncze wyszukiwanie i otrzymywać wyniki ze wszystkich systemów, do których ma uprawniony dostęp, zamiast oddzielnie przeszukiwać każdy system.

12. Wspólny serwis kojarzenia danych biometrycznych byłby technicznym narzędziem ułatwiającym identyfikację osoby fizycznej, która może być zarejestrowana w różnych bazach danych. Przechowywano by w nim wzory danych biometrycznych (odciski palców i wizerunki twarzy) zawarte w scentralizowanych systemach informacyjnych UE (tj. SIS, systemie Eurodac, EES, VIS oraz ECRIS-TCN). Umożliwiłoby to z jednej strony jednoczesne wyszukiwanie danych biometrycznych przechowywanych w różnych systemach, a z drugiej strony – porównywanie tych danych.

13. Wspólne repozytorium tożsamości ułatwiłoby identyfikację osób, w tym na terytorium państw członkowskich, a także ułatwiłoby organom ścigania dostęp do systemów informacji nieprawnych. We wspólnym repozytorium tożsamości przechowywano by dane biograficzne i biometryczne zarejestrowane w VIS, ECRIS-TCN, EES, systemie Eurodac i ETIAS. Dane byłyby przechowywane – logicznie oddzielone – w zależności od systemu, z którego by pochodziły.

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

([2]) Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniającego rozporządzenia (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/794 i (UE) 2016/1624, COM(2016) 731 final z 16.11.2016.

([3]) Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego scentralizowany system identyfikacji państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców na potrzeby uzupełnienia i wsparcia europejskiego systemu przekazywania informacji z rejestrów karnych (systemu ECRIS-TCN) i zmieniającego rozporządzenie (UE) nr 1077/2011, COM(2017) 344 final z 29.6.2017.

([4]) 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).

14. Moduł wykrywający multiplikację tożsamości byłby narzędziem umożliwiającym łączenie danych identyfikacyjnych w ramach wspólnego repozytorium tożsamości i SIS oraz przechowywanie łączy między rejestrami. Przechowywałby linki dostarczające informacji w przypadku wykrycia jednej lub większej liczby konkretnych lub możliwych dopasowań lub w przypadku użycia fałszywej tożsamości. Sprawdzałby, czy zapytanie o dane lub dane wejściowe istnieją w więcej niż jednym systemie w celu wykrycia wielu tożsamości (np. te same dane biometryczne połączone z różnymi danymi biograficznymi lub te same/podobne dane biograficzne połączone z różnymi danymi biometrycznymi). W module wykrywającym multiplikację tożsamości przedstawiono by wpisy biograficzne dotyczące tożsamości, które mają połączenia w innych systemach.

15. Poprzez cztery elementy interoperacyjności wnioski mają na celu:

— zapewnienie upoważnionym użytkownikom szybkiego, bezproblemowego, systematycznego i kontrolowanego dostępu do odpowiednich systemów informacyjnych,

— ułatwianie kontroli tożsamości obywateli państw trzecich na terytorium państw członkowskich,

— wykrywanie różnych tożsamości powiązanych z tym samym zestawem danych, oraz

— usprawnienie dostępu organów ścigania do systemów informacyjnych niezwiązanych z organami ścigania.

16. Ponadto we wnioskach ustanowiono by centralne repozytorium sprawozdawczo-statystyczne, uniwersalny format wiadomości („UMF") oraz wprowadzono by mechanizmy automatycznej kontroli jakości danych.

17. Publikacja dwóch wniosków ustawodawczych zamiast jednego wynika z konieczności przestrzegania rozróżnienia między systemami, które dotyczą:

— dorobku Schengen dotyczącego granic i wiz (tj. VIS, EES, ETIAS i SIS, regulowane rozporządzeniem (WE) nr 1987/2006),

— dorobku Schengen w sprawie współpracy policyjnej lub które nie są związane z dorobkiem Schengen (system Eurodac, ECRIS-TCN oraz SIS, regulowane decyzją Rady 2007/533/WSiSW).

18. Oba wnioski są „bliźniaczymi propozycjami", które należy odczytywać razem. Numeracja artykułów jest zasadniczo podobna w obu wnioskach, podobnie jak ich treść. W związku z tym, o ile nie określono inaczej, gdy wspomina się o konkretnym artykule, artykuł ten odnosi się do tego samego w obu wnioskach.

## 5. **WNIOSKI**

142. EIOD zauważa, że interoperacyjność, po wdrożeniu jej w przemyślany sposób oraz zgodnie z podstawowymi wymogami konieczności i proporcjonalności, może być użytecznym narzędziem służącym zaspokojeniu uzasadnionych potrzeb właściwych organów korzystających z wielkoskalowych systemów informacyjnych, w tym usprawnieniu wymiany informacji.

143. Podkreśla, że interoperacyjność nie jest głównie wyborem technicznym, lecz przede wszystkim wyborem politycznym, który w nadchodzących latach będzie miał istotne konsekwencje prawne i społeczne. Na tle wyraźnej tendencji do łączenia różnych przepisów i celów politycznych UE (tj. odprawy granicznej, azylu i imigracji, współpracy policyjnej, a obecnie także współpracy sądowej w sprawach karnych), jak również przyznania organom ścigania rutynowego dostępu do baz danych niezwiązanych z bazami danych organów ścigania, decyzja prawodawcy Unii o uczynieniu wielkoskalowych systemów informatycznych interoperacyjnymi w sposób trwały i głęboki wpłynęłaby nie tylko na ich strukturę i sposób funkcjonowania, ale zmieniłaby także sposób, w jaki do tej pory interpretowano zasady prawne w tej dziedzinie, i jako taka stanowiłaby „punkt bez powrotu". Z tych powodów EIOD wzywa do szerszej debaty na temat przyszłości wymiany informacji w UE, zarządzania nimi oraz sposobów ochrony praw podstawowych w tym kontekście.

144. Chociaż przedstawione wnioski mogłyby sprawiać wrażenie interoperacyjności jako ostatecznego elementu już w pełni funkcjonujących systemów informacyjnych (lub przynajmniej systemów, których akty założycielskie są już „stabilne" i znajdują się w końcowej fazie procesu legislacyjnego), EIOD pragnie przypomnieć, że tak nie jest. W rzeczywistości obecnie nie istnieją jeszcze trzy z sześciu systemów informacyjnych UE, które mają zostać połączone zgodnie z wnioskami (ETIAS, ECRIS-TCN i EES), dwa są obecnie poddawane przeglądowi (SIS i Eurodac), a jeden ma zostać poddany przeglądowi jeszcze w tym roku (VIS). Ocena dokładnego wpływu bardzo złożonego systemu z tak dużą liczbą „ruchomych części" na prywatność i ochronę danych jest prawie niemożliwa. EIOD przypomina, jak ważne jest zapewnienie spójności między już negocjowanymi (lub przyszłymi) tekstami prawnymi a wnioskami w celu zapewnienia jednolitego otoczenia prawnego, organizacyjnego i technicznego dla wszystkich działań związanych z przetwarzaniem danych w Unii. W tym kontekście pragnie podkreślić, że niniejsza opinia pozostaje bez uszczerbku dla dalszych interwencji, które mogą nastąpić w miarę postępu procesu legislacyjnego w różnych powiązanych ze sobą instrumentach prawnych.

145. EIOD zauważa, że chociaż początkowo interoperacyjność mogła być przewidziana jako narzędzie ułatwiające jedynie korzystanie z systemów, wnioski wprowadzają nowe możliwości dostępu do danych przechowywanych w różnych systemach i ich wykorzystywania w celu zwalczania oszustw dotyczących tożsamości, ułatwiania kontroli tożsamości i usprawniania dostępu organów ścigania do systemów informacji nieprawnych.

146. Jak już zaznaczono w dokumencie analitycznym, EIOD podkreśla znaczenie dalszego wyjaśnienia zakresu problemu oszustw dotyczących tożsamości wśród obywateli państw trzecich, aby zapewnić, że proponowany środek jest odpowiedni i proporcjonalny.

147. Jeżeli chodzi o wykorzystanie danych przechowywanych w różnych systemach w celu ułatwienia kontroli tożsamości na terytoriach państw członkowskich, EIOD podkreśla, że cele takiego wykorzystania, tj. zwalczanie nielegalnej migracji i przyczynianie się do wysokiego poziomu bezpieczeństwa, zostały sformułowane zbyt szeroko i powinny zostać „ściśle ograniczone" i „precyzyjnie określone" we wnioskach, tak aby były zgodne z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej. Uważa w szczególności, że dostęp do wspólnego repozytorium tożsamości w celu ustalenia tożsamości obywatela państwa trzeciego do celów zapewnienia wysokiego poziomu bezpieczeństwa powinien być dozwolony jedynie w przypadku, gdy istnieje dostęp do podobnych krajowych baz danych w tym samym celu (np. rejestr obywateli/mieszkańców itp.) i na tych samych warunkach. Zaleca wyjaśnienie tego we wnioskach. W przeciwnym razie wydaje się, że wnioski ustanawiałyby domniemanie, że obywatele państw trzecich z definicji stanowią zagrożenie dla bezpieczeństwa. EIOD zaleca również zapewnienie dostępu do danych w celu zidentyfikowania osoby w trakcie kontroli tożsamości:

— co do zasady w obecności danej osoby, oraz

— jeżeli dana osoba nie jest w stanie współpracować i nie posiada dokumentu potwierdzającego tożsamość, lub

— odmawia współpracy lub

jeżeli istnieją uzasadnione podstawy, aby przypuszczać, że przedstawione dokumenty są nieprawdziwe lub że dana osoba nie mówi prawdy o swojej tożsamości.

148. EIOD rozumie potrzebę korzystania przez organy ścigania z najlepszych możliwych narzędzi do szybkiej identyfikacji sprawców aktów terrorystycznych i innych poważnych przestępstw. Jednakże usunięcie autentycznych zabezpieczeń wprowadzonych w celu ochrony praw podstawowych, głównie w interesie przyspieszenia procedury, byłoby nie do przyjęcia. W związku z tym zaleca dodanie do art. 22 ust. 1 wniosków warunków dotyczących istnienia uzasadnionych podstaw, wcześniejszego wyszukiwania w krajowych bazach danych oraz rozpoczęcia wyszukiwania w systemie automatycznej identyfikacji daktyloskopijnej innych państw członkowskich na mocy decyzji 2008/615/WSiSW przed rozpoczęciem jakiegokolwiek wyszukiwania we wspólnym repozytorium danych dotyczących tożsamości. Ponadto uważa on, że zgodność z warunkami dostępu nawet do ograniczonych informacji, takich jak wynik lub brak wyniku, powinna być zawsze weryfikowana, niezależnie od dalszego dostępu do danych przechowywanych w systemie, który dostarczył wyniku.

149. EIOD uważa, że należy wyraźniej wykazać konieczność i proporcjonalność wykorzystania danych przechowywanych w ECRIS-TCN w celu wykrycia multiplikacji tożsamości i ułatwienia kontroli tożsamości; EIOD wymaga również wyjaśnienia pod względem zgodności z zasadą ograniczenia celu. Zaleca zatem, by we wnioskach zapewnić dostęp do danych przechowywanych w ECRIS-TCN i ich wykorzystywanie wyłącznie do celów ECRIS TCN określonych w jej instrumencie prawnym.

150. EIOD z zadowoleniem przyjmuje fakt, że celem wniosków jest utworzenie zharmonizowanego środowiska technicznego dla systemów, które będą działać wspólnie w celu zapewnienia szybkiego, płynnego, kontrolowanego i systematycznego dostępu do informacji potrzebnych różnym zainteresowanym stronom do wykonywania ich zadań. Przypomina, że na wszystkich etapach wdrażania wniosków powinno się brać pod uwagę podstawowe zasady ochrony danych i w związku z tym zaleca włączenie do wniosków obowiązku przestrzegania przez eu-LISA i państwa członkowskie zasad ochrony danych już w fazie projektowania oraz jako opcji domyślnej.

151. Poza uwagami ogólnymi i kluczowymi kwestiami określonymi powyżej EIOD ma dodatkowe zalecenia dotyczące następujących aspektów wniosków:

— funkcjonalności europejskiego portalu wyszukiwania, wspólnego serwisu kojarzenia danych biometrycznych, wspólnego repozytorium tożsamości i modułu wykrywającego multiplikację tożsamości,

— okresów przechowywania danych we wspólnym repozytorium tożsamości i module wykrywającym multiplikację tożsamości,

— ręcznej weryfikacji linków,

— centralnego repozytorium sprawozdawczo-statystycznego,

— podziału ról i odpowiedzialności między eu-LISA a państwami członkowskimi,

— bezpieczeństwa elementów interoperacyjności,

— praw osób, których dane dotyczą,

— dostępu pracowników eu-LISA,

— okresu przejściowego,

— dzienników zdarzeń, oraz

— roli krajowych organów nadzoru i EIOD.

152. EIOD pozostaje dostępny w celu udzielenia dalszych wskazówek w sprawie wniosków, również w odniesieniu do aktu delegowanego lub wykonawczego przyjętego zgodnie z proponowanymi rozporządzeniami, który może mieć wpływ na przetwarzanie danych osobowych.

Sporządzono w Brukseli dnia 19 marca 2018 r.

Giovanni BUTTARELLI

*Europejski Inspektor Ochrony Danych*