OPINIA EUROPEJSKIEGO INSPEKTORA OCHRONY DANYCH

W sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych (COM(2004)835 wersja ostateczna)

(2005/C 181/06)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

uwzględniając Kartę Praw Podstawowych Unii Europejskiej, w szczególności jej art. 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych,

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, w szczególności jego art. 41,

uwzględniając wniosek w sprawie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 otrzymany od Komisji w dniu 25 stycznia 2005 r.;

WYDAJE NASTĘPUJĄCĄ OPINIĘ:

1. **WSTĘP**

1.1. **Uwagi wstępne**

Utworzenie Systemu Informacji Wizowej (VIS) stanowi ważną część wspólnej polityki wizowej UE, jak również jest objęte wieloma powiązanymi instrumentami.

— W kwietniu 2003 r. na zlecenie Komisji zostało opracowane studium wykonalności [1] w odniesieniu do VIS.

— We wrześniu 2003 r. Komisja zaproponowała wprowadzenie zmiany [2] do poprzedniego rozporządzenia ustalającego jednolity format wiz. Zasadniczym celem było wprowadzenie do nowego formatu wizy danych biometrycznych (zdjęcie twarzy i dwa odciski palców). Dane biometryczne miałyby być przechowywane w mikrochipie.

---

[1] System Informacji Wizowej, sprawozdanie w wersji ostatecznej, zlecone przez WE i przeprowadzone przez *Trasys* kwiecień 2003 r.

[2] COM(2003)558 wersja ostateczna oraz 2003/0217 (CNS) i 2003/0218 (CNS)

— W czerwcu 2004 r. decyzją Rady ([1]) został rozpoczęty proces tworzenia Systemu Informacji Wizowej poprzez zapewnienie podstawy prawnej do włączenia do budżetu UE środków na rozwój VIS. W decyzji tej zaproponowano utworzenie centralnej bazy danych złożonej z informacji związanych z wnioskami o wydanie wiz i uruchomienie procedury „komitologii" w celu opracowania rozwiązań technicznych stosowanych do VIS.

W grudniu 2004 r. Komisja przyjęła wniosek dotyczący rozporządzenia w sprawie VIS oraz wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych ([2]) (zwany dalej:„wnioskiem") będący przedmiotem niniejszej opinii. Analiza rozszerzonej oceny wpływu ([3]) jest dołączona do wniosku.

Jednakże, jak to zostało wyjaśnione w uzasadnieniu, w celu uzupełnienia rozporządzenia konieczne jest przedsięwzięcie kolejnych instrumentów prawnych, w tym:

— poprawienie Wspólnych Instrukcji Konsularnych w sprawie wiz dla misji dyplomatycznych i urzędów konsularnych Stron Umawiających się do Konwencji z Schengen (zwanych dalej „Wspólnymi Instrukcjami Konsularnymi"), związane z wprowadzeniem do procedur danych biometrycznych;

— opracowanie nowych mechanizmów wymiany danych z Irlandią i Zjednoczonym Królestwem;

— wymiana danych dotyczących wiz długoterminowych.

Zgodnie z decyzją podjętą przez Radę ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniach 5 — 6 czerwca 2003 r. i opisaną w art. 1 ust. 2 wyżej wspomnianej decyzji Rady z czerwca 2004 r., VIS będzie opierał się na scentralizowanym systemie składającym się z baz danych, w których będą przechowywane wnioski o wydanie wizy: Centralnego Systemu Informacji Wizowej (CS-VIS) i Krajowego Interfejsu (NI-VIS) znajdującego się w Państwach Członkowskich. Państwa Członkowskie wyznaczą ([4]) krajowy organ centralny połączony z Krajowym Interfejsem, za pośrednictwem którego ich odpowiednie właściwe organy będą mieć dostęp do CS-VIS.

1.2. **Główne elementy wniosku z perspektywy ochrony danych**

Celem wniosku jest usprawnienie wspólnej polityki wizowej poprzez ułatwienie wymiany danych pomiędzy Państwami Członkowskimi dzięki utworzonej centralnej bazie danych. Rozporządzenie przewiduje wprowadzanie danych biometrycznych (fotografia i odcisk palca) do procedury składania wniosków oraz przechowywanie tych danych w centralnej bazie danych.

Dane biometryczne mogą być również wykorzystywane na naklejce wizowej, zgodnie z rozporządzeniem zmieniającym zaproponowanym przez Komisję dotyczącym jednolitego formatu wiz i przewidującym wprowadzenie fotografii i odcisku palca, przechowywanych w mikrochipie (oczekuje się nadal na decyzję Rady opierającą się na wynikach prowadzonych analiz).

Wniosek dokładnie opisuje różne operacje przeprowadzane na danych (wprowadzanie, poprawianie, usuwanie i konsultowanie) oraz różne dane, które powinny być dodane do VIS zależnie od etapu rozpatrywania wniosku (wydanie, odmowa wydania itd.)

Wniosek przewiduje pięcioletni okres przechowywania danych dotyczących każdego wniosku.

Wniosek zawiera zamknięty wykaz właściwych organów innych niż organy odpowiedzialne za wydawanie wiz dysponujących dostępem do VIS oraz określa prawa, które mają im przysługiwać w zakresie dostępu:

— organy właściwe do przeprowadzania kontroli wizowych na granicach zewnętrznych i w obrębie terytorium Państwa Członkowskiego,

— właściwe organy imigracyjne,

([1]) 2004/512/WE, Dz.U. L 213, z 15.6.2004, str. 5.
([2]) COM(2004)835 wersja ostateczna oraz 2004/0287 (COD)
([3]) Analiza rozszerzonej oceny wpływu systemu informacji wizowej, sprawozdanie EPEC (*European Policy Evaluation Consortium* - Europejskie Konsorcjum ds. Oceny Polityki Europejskiej) w wersji ostatecznej grudzień 2004 r.
([4]) Art. 24 ust. 2 wniosku.

— właściwe organy zajmujące się sprawami azylu.

W odniesieniu do opisu operacji w ramach VIS i związanej z nimi odpowiedzialności, podkreślono we wniosku, że Komisja przetwarza dane zawarte w VIS w imieniu Państw Członkowskich. Wniosek podkreśla potrzebę wykorzystywania rejestrów dotyczących przetwarzania danych celem zapewnienia bezpieczeństwa danych oraz wyszczególnia właściwe obowiązki zapewniające ten poziom bezpieczeństwa.

Wniosek zawiera rozdział poświęcony ochronie danych, w którym zostaje szczegółowo opisana zarówno rola organów krajowych, jak również Europejskiego Inspektora Ochrony Danych (zwanego dalej: EIOD).

Wniosek powierza wdrożenie VIS pod względem technicznym oraz wybór odpowiednich technologii komitetowi ustanowionemu na mocy art. 5 ust. 1 rozporządzenia (WE) nr 2424/2001 w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II).

Rozszerzona ocena wpływu VIS, zlecona przez Komisję i przeprowadzona przez EPEC, znajduje się w załączniku do wniosku. Zgodnie z tą opinią opcja przewidująca zastosowanie VIS przy jednoczesnym wykorzystywaniu danych biometrycznych stanowi najlepsze dostępne rozwiązanie dla usprawnienia wspólnej polityki wizowej.

2. **STOSOWNE RAMY**

Wniosek będzie miał znaczący wpływ na prawo do prywatności i inne podstawowe prawa jednostek; należy go zatem przeanalizować pod względem uwzględnienia zasad dotyczących ochrony danych. Główne punkty odniesienia naszej analizy są następujące.

— W Europie poszanowanie życia prywatnego jest zapewnione od momentu przyjęcia w 1950 r. Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (zwanej dalej: „Konwencją o Ochronie Praw Człowieka") przez Radę Europy. Art. 8 tej konwencji ustanawia „prawo do poszanowania życia prywatnego i rodzinnego".

  Zgodnie z art. 8 ust. 2 jakakolwiek ingerencja władzy publicznej w korzystanie z tego prawa jest dozwolona wyłącznie, jeżeli jest „przewidziana przez ustawę" oraz „konieczna w demokratycznym społeczeństwie" z uwagi na ochronę ważnych interesów. Według orzecznictwa Europejskiego Trybunału Praw Człowieka warunki te spowodowały konieczność ustanowienia dodatkowych wymogów, takich jak: rodzaj podstawy prawnej dla ingerencji, proporcjonalność środków i konieczność odpowiedniego zabezpieczenia przed nadużyciami.

  Podstawowe zasady w dziedzinie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych zostały zawarte w Konwencji o Ochronie Danych, opracowanej przez Radę Europy i przyjętej w 1981 r.

— Prawo do poszanowania życia prywatnego i ochrona danych osobowych zostały niedawno ustanowione również w art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej, która została włączona do części II nowej Konstytucji UE.

  Zgodnie z art. 52 Karty przewiduje się możliwość ograniczenia tych praw, o ile są spełnione warunki podobne do tych, które przewiduje art. 8 Konwencji o Ochronie Praw Człowieka. Warunki te muszą zostać każdorazowo uwzględnione przy ocenie wniosku w sprawie ewentualnej ingerencji.

W chwili obecnej podstawowe zasady prawodawstwa UE dotyczące ochrony danych są zawarte w:

— dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz.U. L 281, str. 31) Dyrektywa ta będzie dalej nazywana „dyrektywą 95/46/WE". Dyrektywa określa szczegółowe zasady według których wniosek będzie sprawdzany w zakresie, w jakim ma ona mieć zastosowanie do Państw Członkowskich. Ma to duże znaczenie, zważywszy, że wniosek będzie stosowany łącznie z ustawodawstwem krajowym nadając dyrektywie moc obowiązującą. Skuteczność proponowanych przepisów i zabezpieczeń będzie zatem zależeć od skuteczności tej kombinacji w każdym pojedynczym przypadku.

— rozporządzeniu (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8, str. 1). Rozporządzenie to będzie dalej nazywane „rozporządzeniem 45/2001". Ustanawia ono zasady podobne do zasad przewidzianych przez dyrektywę 95/46/WE i ma znaczenie w tym kontekście w zakresie, w jakim wniosek ma mieć zastosowanie do działań Komisji, zgodnie z przepisami rozporządzenia. Zatem należy zwrócić uwagę również i na tę kombinację .

Dyrektywa 95/46/WE i rozporządzenie 45/2001 muszą być interpretowane w połączeniu z innymi instrumentami. Innymi słowami, dyrektywa i rozporządzenie, w zakresie w jakim dotyczą przetwarzania danych osobowych mogącego prowadzić do naruszeń podstawowych wolności, a zwłaszcza prawa do prywatności, muszą być interpretowane w świetle praw podstawowych. Powyższe wynika również z orzecznictwa Europejskiego Trybunału Sprawiedliwości ([1]).

— Na koniec EIOD załączy również do swojej analizy opinię nr 7/2004 z dnia 11 sierpnia 2004 r. Zespołu Roboczego ds. Ochrony Danych art. 29 ([2]), „w sprawie wprowadzenia elementów biometrycznych do pozwoleń na pobyt i wiz, przy uwzględnieniu utworzenia europejskiego Sytemu Informacji Wizowej (VIS)". W swojej opinii Zespół Roboczy wyraził obawy odnośnie kilku elementów wniosku. EIOD zamierza sprawdzić, czy i w jaki sposób wniosek uwzględnił te obawy.

3. **ANALIZA WNIOSKU**

3.1. **Analiza ogólna**

EIOD przyznaje, że dalszy rozwój wspólnej polityki wizowej wymaga skutecznej wymiany odpowiednich danych. VIS jest jednym z mechanizmów, który może zapewnić niezakłócony przepływ informacji. Jednakże ten nowy instrument powinien ograniczać się do gromadzenia i wymiany danych, pod warunkiem, że gromadzenie i wymiana są konieczne do rozwoju wspólnej polityki wizowej oraz są proporcjonalne do tego celu.

Utworzenie VIS może mieć pozytywne konsekwencje dla innego uzasadnionego interesu publicznego, ale nie może zmieniać to celu VIS. Ograniczony cel systemu odgrywa zasadniczą rolę w określaniu właściwej zawartości i wykorzystania systemu zgodnie z prawem, a zatem również w udzielaniu prawa dostępu do VIS (lub części jego danych) organom Państw Członkowskich dla uzasadnionego interesu publicznego.

Ponadto wniosek przewiduje wykorzystywanie w VIS danych biometrycznych. EIOD uznaje korzyści płynące z wykorzystania danych biometrycznych, ale jednocześnie podkreśla poważne konsekwencje wynikające z ich wykorzystania oraz sugeruje wprowadzenie surowych ograniczeń w tym zakresie.

Opinię należy interpretować w świetle wyżej wymienionych głównych uwag. Zauważa się, że niniejsza opinia powinna być uwzględniona w preambule rozporządzenia przed motywami („uwzględniając opinię ....").

([1]) W tym kontekście należy zrobić odniesienie do wyroku Trybunału Sprawiedliwości w sprawie Österreichischer Rundfunk i inni (sprawy połączone C-465/00, C-138/01 oraz C-139/01, wyrok z dnia 20 maja 2003 r., sąd w pełnym składzie, (2003) ECR I-4989). Trybunał zajął się austriacką ustawą dotyczącą transferu informacji o wynagrodzeniu w sektorze publicznym do austriackiego sądu obrachunkowego i ich późniejszą publikacją. W wyroku Trybunał ustala kryteria, opracowane na podstawie art. 8 Europejskiej Konwencji o Prawach Człowieka, do których należy się odwoływać przy stosowaniu dyrektywy 95/46/WE w takim zakresie, w jakim dyrektywa ta pozwala na pewne ograniczenia prawa do prywatności.

([2]) Jest to niezależny zespół doradczy, składający się z przedstawicieli organów z Państw Członkowskich zajmujących się ochroną danych, EIOD i Komisji, ustanowiony przepisami dyrektywy 95/46/WE.

3.2. **Cel**

Cel VIS ma kluczowe znaczenie, zarówno w świetle art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka, jak i szerszym kontekście ochrony danych. Zgodnie z ar. 6 dyrektywy 95/46/WE dane osobowe muszą być „gromadzone do określonych, wyraźnych i legalnych celów oraz nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z tymi celami". Tylko precyzyjne określenie celów pozwoli na właściwą ocenę proporcjonalności i adekwatności przetwarzania danych osobowych, która jest niezwykle istotna z powodu charakteru danych (w tym danych biometrycznych) i skali przewidzianej operacji przetwarzania.

Cel VIS jest jasno określony w art. 1 ust. 2 wniosku:

> „VIS powinien przyczynić się do poprawy zarządzania wspólną polityką wizową, współpracy konsularnej oraz procesu konsultacji pomiędzy centralnymi władzami konsularnymi poprzez ułatwienie wymiany danych pomiędzy Państwami Członkowskimi w związku z wnioskami oraz podejmowaniem odnośnych decyzji".

Zatem wszystkie elementy składające się na VIS muszą być koniecznymi i proporcjonalnymi instrumentami służącymi osiągnięciu tego celu w interesie wspólnej polityki wizowej.

Art. 1 ust. 2 wniosku przedstawia wykaz dodatkowych korzyści płynących z usprawnienia polityki wizowej, takich jak:

a) zapobieganie zagrożeniom bezpieczeństwa wewnętrznego,

b) usprawnienie walki z oszustwami,

c) ułatwienie odpraw na przejściach granicznych znajdujących się na granicach zewnętrznych.

EIOD uważa powyższe elementy nie za cele same w sobie, lecz za przykłady pozytywnych konsekwencji utworzenia VIS oraz usprawnienia wspólnej polityki wizowej.

Powyższe powoduje dwie główne konsekwencje na tym etapie:

— EIOD jest świadomy, że organy ścigania są zainteresowane w otrzymaniu dostępu do VIS; W tym zakresie zostały przyjęte konkluzje Rady w dniu 7 marca 2005 r. Zważywszy że celem VIS jest usprawnienie wspólnej polityki wizowej, należy odnotować, że stały dostęp organów ścigania nie byłby zgodny z tym celem. Chociaż zgodnie z art. 13 dyrektywy 95/46/WE dostęp taki może być udzielany *ad hoc*, w określonych okolicznościach i przy zastosowaniu odpowiednich zabezpieczeń, to jednak nie może być zapewniony dostęp stały.

  Ogólnie mówiąc, przy podejmowaniu w przyszłości decyzji o udzieleniu lub nie dostępu do VIS innym organom niezbędna jest ocena proporcjonalności i konieczności. Zadania, dla których udzielany jest dostęp, muszą być zgodne z celami VIS.

— Wyraźne określenie zawarte w lit. a):„zapobieganie zagrożeniom dla bezpieczeństwa wewnętrznego każdego z Państw Członkowskich nie jest określeniem najlepszym. Główną korzyścią płynącą z VIS będzie zapobieganie oszustwom i handlowi wizami (walka z oszustwami jest również podstawowym powodem włączenia danych biometrycznych do systemu) ([1]). Zapobieganie zagrożeniom dla bezpieczeństwa powinno zatem być postrzegane jako korzyść „drugorzędna", chociaż również pożądana.

  EIOD zaleca wprowadzenie wyraźniejszego rozróżnienia pomiędzy „celem" a „korzyściami" w art. 1 ust. 2, na przykład w następującej postaci:

  „VIS ma na celu usprawnienie zarządzania wspólną polityką wizową, współpracy konsularnej oraz procesu konsultacji pomiędzy centralnymi władzami konsularnymi poprzez ułatwienie wymiany danych pomiędzy Państwami Członkowskimi w związku z wnioskami oraz podejmowaniem odnośnych decyzji. Mając to na uwadze, powinien również przyczynić się ...".

([1]) W rozszerzonej ocenie wpływu zostaje stwierdzone jednoznacznie (str. 6, §2.7).: „*brak skuteczności w zwalczaniu handlu wizami, oszustw i w przeprowadzaniu odpraw pociąga za sobą również brak skuteczności w odniesieniu do bezpieczeństwa wewnętrznego Państw Członkowskich*". To oznacza, że zagrożenia dla bezpieczeństwa częściowo wynikają z nieskutecznej polityki wizowej. Pierwszą rzeczą do zrobienia w tej sprawie jest usprawnienie polityki wizowej, głównie poprzez zwalczanie oszustw i skuteczniejsze przeprowadzanie odpraw. Poprawa stanu bezpieczeństwa będzie wynikiem usprawnienia polityki wizowej.

W odniesieniu do powyższego warto również zauważyć, że „Wytyczne do wprowadzenia wspólnego systemu wymiany danych wizowych" przyjęte przez Radę ds. WSiSW w dniu 13 czerwca 2002 r. ([1]) umieszczają zapobieganie zagrożeniom dla bezpieczeństwa wewnętrznego na końcu listy. Takie rozwiązanie byłoby również możliwe oraz jednocześnie w większym stopniu byłaby spójna z celem VIS.

3.3. **Jakość danych**

Zgodnie z art. 6 dyrektywy 95/46/WE dane osobowe muszą również być „stosowne, istotne i nie wykraczające poza konieczne w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone". Powyższe odnosi się do proporcjonalności samego VIS, ale również do danych, które mają być gromadzone i przechowywane w VIS oraz do ich dalszego wykorzystania, jak również do dodatkowych zabezpieczeń mających zastosowanie w tym kontekście. Elementy te są w równym stopniu istotne dla oceny wniosku w świetle art. 8 Konwencji o Ochronie Praw Człowieka.

Utworzenie VIS stanowi niewątpliwie ważną ingerencję w prawo do prywatności ze względu na jego skalę i kategorie przetwarzanych danych osobowych. W związku z powyższym Zespół Roboczy art. 29 w opinii nr 7/2004 zadała pytanie: „jakie badania nad skalą i znaczeniem tych zjawisk wskazały na niepodważalne argumenty w zakresie bezpieczeństwa lub porządku publicznego, które stanowiłyby uzasadnienie takiego podejścia".

EIOD przyjął do wiadomości argumentację zawartą w poszerzonej ocenie wpływu. Chociaż argumentacja ta nie jest w pełni jednoznaczna, wydaje się że istnieją wystarczające powody uzasadniające utworzenie VIS w celu usprawnienia wspólnej polityki wizowej.

W tym kontekście wydaje się, że podjęcie decyzji o utworzeniu VIS jako instrumentu poprawiającego warunki wydawania wiz przez Państwa Członkowskie pozostaje w zakresie właściwości władzy ustawodawczej. Taki system mógłby się dobrze dopasować i umacniać stopniowe ustanawianie przestrzeni wolności, bezpieczeństwa i sprawiedliwości przewidziane Traktatem WE.

Jednakże utworzenie VIS i korzystanie z niego w żadnym wypadku nie może doprowadzić do sytuacji, w której nie można by dłużej zapewnić wysokiego poziomu ochrony danych osobowych w tej dziedzinie. Do zadań EIOD jako organu doradczego należy zbadanie, w jakim zakresie VIS wpłynie na istniejący poziom ochrony danych osób, których te dane dotyczą.

W oparciu o te przesłanki EIOD w niniejszej opinii skoncentruje się na następujących kwestiach:

— proporcjonalność i adekwatność danych i ich wykorzystywanie (np. kategorie danych, dostęp do danych dla zainteresowanych organów, okres przechowywania);

— korzystanie z systemu (np. zakres odpowiedzialności i bezpieczeństwo);

— prawa osób, których dane dotyczą (np. informacje, możliwość zmian lub usunięcia niedokładnych lub nieistotnych danych);

— monitorowanie i nadzór systemu.

Wniosek nie stanowi, poza kolejnymi ustępami, podstaw do istotnych uwag dotyczących kategorii danych, które mają być wprowadzone do VIS i ich wykorzystania. Odpowiednie przepisy zostały starannie opracowane i wydają się być w całości spójne i adekwatne.

([1]) „Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (2002/475/WSiSW)", *Dz.U.* L 164 z 22.6.2002, str. 3

3.4. **Biometria**

3.4.1. *Wpływ zastosowania biometrii*

Zastosowanie biometrii w systemach informatycznych nie jest wyborem bez znaczenia, zwłaszcza w sytuacji, w której system obejmuje tak wielką liczbę podmiotów. Biometria to nie tylko jedna z technologii informatycznych. Zmienia ona w sposób nieodwracalny stosunek pomiędzy ciałem a tożsamością: cechy ciała ludzkiego stają się przedmiotem odczytu maszynowego i mogą być dalej wykorzystywane. Nawet jeżeli cechy biometryczne nie są rozpoznawalne dla ludzkiego oka, to można je zawsze odczytać i wykorzystać przy zastosowaniu odpowiednich narzędzi, bez względu na miejsce przebywania danej osoby.

Bez względu na to, w jak dużym stopniu biometria może być przydatna do niektórych celów, jej rozpowszechnienie będzie miało znaczny wpływ na społeczeństwo i z tego powodu powinno stać się przedmiotem szerokiej i otwartej dyskusji. EIOD stwierdza, że taka dyskusja w rzeczywistości nie miała miejsca przed opracowaniem wniosku. To podkreśla w jeszcze większym stopniu potrzebę wprowadzenia rygorystycznych zabezpieczeń w odniesieniu do wykorzystania danych biometrycznych oraz dokładnego zastanowienia się i przeprowadzenia dyskusji w trakcie procesu legislacyjnego.

3.4.2. *Specyficzny charakter biometrii*

Jak to już zostało podkreślone w kilku opiniach Zespołu Roboczego art. 29 ([1]) wprowadzaniu i przetwarzaniu danych biometrycznych na potrzeby dokumentów tożsamości muszą towarzyszyć szczególnie spójne i poważne zabezpieczenia. Ze względu na niektóre swoje cechy specyficzne dane biometryczne są szczególnie wrażliwe.

Prawdą jest, że, w przeciwieństwie do hasła lub klucza, utrata przez daną osobę danych biometrycznych jest prawie niemożliwa. Gwarantują one *prawie absolutnie pewne rozróżnienie*, tj. każda osoba posiada niepowtarzalne dane biometryczne. Prawie nigdy nie ulegają zmianie na przestrzeni całego życia, co zapewnia *trwałość* tych cech. Każda osoba posiada takie same „elementy" fizyczne, co nadaje danym biometrycznym wymiar *uniwersalny*.

Jednakże usunięcie danych biometrycznych jest prawie niemożliwe: trudno zmienić palec lub twarz. Ten, z niejednego punktu widzenia pozytywny aspekt, w przypadku *kradzieży tożsamości* stanowi dużą wadę: przechowywanie odcisków palców i fotografii w bazie danych w powiązaniu ze skradzionym dowodem tożsamości może prowadzić do poważnych i trwałych problemów dla prawdziwego posiadacza danej tożsamości. Ponadto dane biometryczne ze swojej natury *nie stanowią tajemnicy* i mogą nawet *zostawiać ślady* (odciski palców, DNA), które pozwalają na gromadzenie tych danych *bez wiedzy ich posiadacza*.

Ze względu na opisane ryzyko, jakie niesie za sobą wykorzystywanie danych biometrycznych, należy wprowadzić w życie istotne zabezpieczenia (zwłaszcza w odniesieniu do zasady ograniczonego celu, ograniczeń dostępu i środków bezpieczeństwa).

3.4.3. *Niedoskonałoœci techniczne w odniesieniu do odcisków palców*

Opisane powyżej główne korzyści płynące z wykorzystania danych biometrycznych (uniwersalność, rozróżnienie, trwałość, łatwość wykorzystania itd.) nie są nigdy bezwzględne. Mają one bezpośredni wpływ na skuteczność wpisu danych biometrycznych i procedury sprawdzające przewidziane w rozporządzeniu.

Szacuje się ([2]), że do 5 % osób nie może zostać wpisanych (ponieważ nie mają one czytelnych odcisków palców lub nie mają w ogóle odcisków palców). Rozszerzona ocena wpływu załączona do wniosku przewiduje około 20 milionów wniosków wizowych w 2007 r., co oznacza, że do 1 miliona osób nie będzie mogło być objęte standardową procedurą wpisywania, co pociągnie za sobą oczywiste skutki dla wniosków wizowych i podczas odprawy granicznej.

([1]) Opinia 7/2004 w sprawie wprowadzenia elementów biometrycznych do pozwoleń na pobyt i wiz, przy uwzględnieniu utworzenia europejskiego Systemu Informacji Wizowej (VIS) (Markt/11487/04/EN - WP 96) oraz dokumentów roboczych dotyczących biometrii (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and Crime Prevention: Usability and Trust in Information Systems*, w „Foresight cybertrust and crime prevention project". 04/1151, 10 czerwca 2004, str.7, i Technology Assessment, „Using Biometrics for Border Security", United States General Accounting Office, GAO-03-174, listopad 2002.

Identyfikacja biometryczna jest również z definicji procesem statystycznym. Poziom błędu od 0,5 do 1 % jest poziomem normalnym ([1]), co oznacza, że system kontroli na granicach zewnętrznych będzie miał błąd fałszywego odrzucenia (FRR) pomiędzy 0,5 a 1 %. Ten poziom jest przyjęty w oparciu o próg ryzyka określany przez właściwe organy (odpowiada on równowadze między ilością osób błędnie odrzuconych i ilością osób błędnie zaakceptowanych). Zatem stwierdzenie, że technologie te zapewnią, jak to przewiduje motyw 9. wnioskowanego rozporządzenia, „dokładną identyfikację" osób, których dane dotyczą, jest przesadą.

Zgodnie z najnowszym badaniem ([2]) zleconym przez komitet LIBE Parlamentu Europejskiego powinny być dostępne *procedury awaryjne* w celu ustanowienia podstawowych zabezpieczeń dla wprowadzenia danych biometrycznych, jeżeli nie są one dostępne dla wszystkich lub nie są w pełni dokładne. Takie procedury powinny być wdrożone i wykorzystywane w celu poszanowania godności osób, które nie mogą skutecznie uczestniczyć w procesie wpisywania oraz uniknięcia obciążania ich niedoskonałościami systemu ([3]).

EIOD zatem zaleca opracowanie procedur awaryjnych i włączenie ich do wniosku. Procedury te nie powinny obniżać poziomu bezpieczeństwa polityki wizowej ani piętnować osób posiadających nieczytelne odciski palców.

3.5. **Szczególne kategorie danych**

Niektóre kategorie danych (oprócz danych biometrycznych) wymagają specjalnej uwagi: dane dotyczące podstaw odmowy wydania wizy (3.5.1) i dane związane z innymi członkami tej samej grupy podróżnych (3.5.2)

3.5.1. *Podstawy odmowy wydania wizy*

Art. 10 ust. 2 wniosku przewiduje przetwarzanie danych dotyczących podstaw odmowy w wypadku podjęcia decyzji o odmowie wydania wizy. Podstawy odmowy są w całości uregulowane przepisami prawa.

— Dwie pierwsze podstawy wymienione w lit. a) i b) są raczej natury administracyjnej: nie przedłożono ważnych dokumentów podróży lub ważnych dokumentów potwierdzających cel i warunki planowanego pobytu.

— Lit. c) dotyczy „wpisu do celów odmowy wjazdu, którego dokonano wobec osoby składającej wniosek wizowy", który zakłada sprawdzenie w bazie danych SIS.

— Lit. d) jako podstawę odmowy wydania wizy przewiduje fakt, że osoba składająca wniosek o wydanie wizy „stanowi zagrożenie dla polityki publicznej, bezpieczeństwa wewnętrznego, zdrowia publicznego lub stosunków międzynarodowych któregokolwiek z Państw Członkowskich".

([1])

Dane biometryczne	Twarz	Palec	Tęczówka
FTE % poziom braku wpisów	brak danych	4	7
FNMR % poziom odrzuceń	4	2,5	6
FMR1 % poziom błędnych akceptacji w systemach weryfikacji	10	< 0,01	< 0,001
FMR2 % poziom błędnych akceptacji w systemach identyfikacji z bazą danych > 1 mln	40	0,1	brak danych
FMR3 % poziom błędnych akceptacji w systemach screeningu z bazą danych = 500	12	< 1	brak danych

A. K. Jain et al., *Biometrics: A grand Challenge*, Proceedings of International Conference on Pattern Recognition, Cambridge, UK., sierpień 2004

([2]) *Biometrics at the frontiers: assessing the impact on Society*, luty 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, WE.

([3]) *Sprawozdanie okresowe w sprawie stosowania zasad Konwencji 108 do gromadzenia i przetwarzania danych biometrycznych*, Rada Europy, 2005 r. str. 11

Wszystkie podstawy odmowy muszą być stosowane z dużą rozwagą ze względu na konsekwencje, jakie mogą mieć dla danej osoby. Ponadto niektóre z nich — te, o których mowa w lit. c) oraz d), będą prowadzić do przetwarzania „danych wrażliwych" w rozumieniu art. 8 dyrektywy 95/46/WE.

EIOD chciałby zwrócić szczególną uwagę na warunek związany ze zdrowiem publicznym, który wydaje się wieloznaczny i prowadzi do przetwarzania danych bardzo wrażliwych. Zgodnie z komentarzem do artykułów załączonym do wniosku, odniesienie do zagrożenia dla zdrowia publicznego opiera się na „wniosku w sprawie rozporządzenia Rady ustanawiającego wspólnotowy kodeks zasad regulujących przepływ osób przez granice" (COM (2004)391 wersja ostateczna).

EIOD przyznaje, że kryterium „zdrowia publicznego" jest szeroko stosowane w ustawodawstwie Wspólnoty dotyczącym swobodnego przepływu osób oraz ściśle przestrzegane, jak pokazuje dyrektywa 2004/58/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium Państw Członkowskich. Art. 29 tej dyrektywy ustala warunki, jakie należy uwzględnić przy ocenie zagrożenia dla zdrowia publicznego: „Chorobami, które uzasadniają wprowadzenie środków ograniczających swobodę przemieszczania się, są potencjalne choroby epidemiczne określone przez odpowiednie instrumenty Światowej Organizacji Zdrowia oraz inne choroby zakaźne lub zakaźne choroby pasożytnicze, jeżeli są przedmiotem przepisów ochronnych mających zastosowanie do obywateli przyjmującego Państwa Członkowskiego."

— Jednakże należy zauważyć, że wniosek, o którym mowa wcześniej, jest w chwili obecnej tylko wnioskiem oraz że włączenie warunku mówiącego o niestanowieniu zagrożenia dla zdrowia publicznego do rozporządzenia VIS zależy od przyjęcia kodeksu Wspólnoty.

— Ponadto, jeśli zostanie on przyjęty, podstawa odmowy wjazdu powinna być interpretowana ścieśniająco. W rzeczywistości wniosek w sprawie kodeksu Wspólnoty opiera się na właśnie wspomnianej dyrektywie 2004/58/WE.

EIOD zaleca zatem włączenie odniesienia do art. 29 dyrektywy 2004/58/WE do tekstu wniosku w celu zagwarantowania, że „zagrożenie dla zdrowia publicznego" jest rozumiane w świetle tego właśnie przepisu. W każdym wypadku, uwzględniając wrażliwość danych, powinny być one przetwarzane wyłącznie wtedy, gdy zagrożenie dla zdrowia publicznego jest rzeczywiste, obecne i wystarczająco poważne.

3.5.2. *Dane innych członków tej samej grupy podróżnych*

Art. 2 ust. 7 definiuje „członków tej samej grupy podróżnych" jako „inne osoby ubiegające się o wizę, podróżujące razem z osobą ubiegającą się o wizę, w tym współmałżonka i dzieci towarzyszące osobie ubiegającej się o wizę". Komentarz do artykułów wspomina, że definicje zawarte w art. 2 wniosku odnoszą się w zakresie polityki wizowej do Traktatu lub do dorobku Schengen, z wyjątkiem kilku terminów, w tym „członków tej samej grupy podróżnych", które są zdefiniowane specjalnie do celów tego rozporządzenia. Można zatem założyć, że ta definicja nie odnosi się do definicji „wizy grupowej" zawartej w art. 2.1.4 Wspólnych Instrukcji Konsularnych. Komentarz do artykułów odnosi się do „osób ubiegających się o wizę, podróżujących w grupie razem z innymi osobami ubiegającymi się o wizę, np. w ramach umowy ADS (*Approved Destination Status*) lub razem z członkami rodziny".

EIOD podkreśla, że rozporządzenie powinno zawierać dokładną i zrozumiałą definicję „członków tej samej grupy podróżnych". EIOD stwierdza, że we wniosku w obecnej formie definicja ta jest zbyt nieprecyzyjna ze względu na brak konkretnego odniesienia do Traktatu lub dorobku Schengen. Według istniejącego określenia „członkowie tej samej grupy podróżnych" mogą obejmować współpracowników, innych klientów tego samego biura podróży biorących udział w wyjeździe zorganizowanym itp. Konsekwencje są niezwykle istotne:

zgodnie z art. 5 projektu rozporządzenia plik danych dotyczących wniosku wizowego osoby ubiegającej się o wizę będzie powiązany z plikami danych dotyczących wniosku wizowego pozostałych członków tej samej grupy podróżnych.

3.6. **Przechowywanie danych**

Art. 20 projektu rozporządzenia przewiduje pięcioletni okres przechowywania danych dla każdego pliku danych dotyczących wniosku wizowego. Ustawodawca Wspólnoty w ramach swojej polityki powinien określić rozsądne ramy czasowe.

Nie ma żadnych dowodów — zwłaszcza w świetle powodów przedstawionych w komentarzu do artykułów — wskazujących na brak zasadności przedstawionych we wniosku ram czasowych lub na konsekwencje niemożliwe do zaakceptowania pod warunkiem, że zostaną zastosowane wszystkie właściwe mechanizmy korygujące. Oznacza to konieczność zagwarantowania poprawienia lub usunięcia danych, które nie są już dokładne, zwłaszcza w sytuacja, w której osoba uzyskała obywatelstwo Państwa Członkowskiego albo status, który nie wymaga włączenia jej do systemu.

Ponadto, jeżeli dane znajdują się nadal w systemie, to nie mogą one w żaden sposób wpływać na nową decyzję. Niektóre podstawy odmowy (zwłaszcza wpis do celów odmowy wjazdu odnoszący się do osoby ubiegającej się o wydanie wizy, zagrożenie dla zdrowia publicznego) mają ograniczoną ważność w czasie. To, że stanowiły one ważną podstawę do odmówienia wjazdu w danym momencie, nie powinno wpływać na nową decyzję. Sytuacja musi być w całości poddana ponownej ocenie w przypadku każdego nowego wniosku o wydanie wizy, co powinno być wyraźnie stwierdzone w stosownej części rozporządzenia.

3.7. **Dostęp do danych i ich wykorzystywanie**

3.7.1. *Uwagi wstępne*

Na wstępie EIOD chciałby zaznaczyć, że docenia wysiłki włożone w opracowanie systemów regulujących dostęp do danych i ich wykorzystywanie. Każdy organ ma dostęp do różnych danych do różnych celów. Jest to słuszne podejście, które EIOD zdecydowanie popiera. Znajdujące się poniżej uwagi mają przyczynić się do zapewnienia zastosowania tego podejścia w jak najszerszym ujęciu.

3.7.2. *Kontrola wiz na przejœciach granicznych znajdujących siê na granicy zewnêtrznej oraz na terytorium danego pañstwa*

W przypadku kontroli wizowej na granicach zewnętrznych, art. 16 wnioskowanego rozporządzenia przewiduje w sposób jednoznaczny dwa jasno określone cele:

— „sprawdzenie tożsamości osoby", które oznacza według podanej definicji porównanie „indywidualne",

— „sprawdzenie autentyczności wizy". Zgodnie ze normami Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO) mikrochip znajdujący się na wizie może korzystać z publicznego/prywatnego „systemu klucza" (PKI — *Public Key Infrastructure*) w celu sprawdzenia autentyczności wizy.

Powyższe dwa cele mogą zostać osiągnięte we właściwy sposób, tylko jeżeli dostęp do chronionego mikrochipu mają wyłącznie organy właściwe do przeprowadzania kontroli wiz. Dostęp do centralnej bazy danych VIS byłby zatem nieproporcjonalny w tym konkretnym przypadku. Ta ostatnia opcja przewiduje większą liczbę organów posiadających połączenie z VIS, co może zwiększyć ryzyko nadużyć. Opcja ta mogłaby być również rozwiązaniem droższym, zważywszy, że pociągnie za sobą znaczny wzrost liczby bezpiecznych i kontrolowanych dostępów do VIS oraz zapotrzebowania na szkolenia dotyczące takiego dostępu.

Ponadto powstały wątpliwości w odniesieniu do adekwatności dostępu do danych przewidzianego w art. 16 ust. 2. Ust. 2 lit. a) przewiduje, że jeżeli po pierwszym zapytaniu okaże się, iż dane osoby ubiegającej się o wizę znajdują się w VIS (co powinno być regułą), właściwy organ może mieć dostęp do pozostałych danych, nadal w celu sprawdzenia tożsamości. Dane te dotyczą wszystkich informacji związanych z wnioskiem, fotografiami, odciskami palców, jak również z każdą uprzednio wydaną, anulowaną, cofniętą lub przedłużoną wizą.

Jeżeli sprawdzenie tożsamości powiodło się, nie jest jasne z jakiego powodu potrzebne miałyby być nadal pozostałe dane. Powinny być one udostępniane wyłącznie pod ściśle określonymi warunkami, w sytuacji, w której sprawdzenie tożsamości nie powiodło się. W takiej sytuacji dane, o których mowa w art. 16 ust. 2 będą wykorzystane w procedurze awaryjnej mającej na celu pomoc w ustaleniu tożsamości danej osoby. Zatem nie powinny być one dostępne dla wszystkich funkcjonariuszy przejścia granicznego, a tylko w sposób bardziej restryktywny dla funkcjonariuszy prowadzących trudne sprawy.

Na koniec należy stwierdzić, że definicja dotycząca organów posiadających dostęp (do danych) powinna być dokładniejsza. W szczególności nie jest jasne jakich organów dotyczy określenie „organy właściwe do przeprowadzania kontroli na terytorium Państwa Członkowskiego". EIOD zakłada, że dotyczy ono organów właściwych do przeprowadzania kontroli *wiz*, w związku z czym art. 16 powinien być pod tym kątem poprawiony.

3.7.3. *Wykorzystywanie danych do identyfikacji i deportacji nielegalnych imigrantów oraz do procedur azylowych*

W wypadkach opisanych w art. 17, 18 i 19 (deportacja nielegalnych imigrantów i procedury azylowe), VIS jest wykorzystywany do celów identyfikacji. Pomiędzy danymi, które mogą być użyte do celów identyfikacji znajdują się również fotografie. Jednakże przy obecnym poziomie technologii związanej z automatycznym rozpoznawaniem twarzy dla systemów informatycznych o tak dużej skali, fotografie nie mogą być używane do identyfikacji (jeden z wielu); nie mogą zapewnić wiarygodnego wyniku. Zatem nie należy traktować ich za dane adekwatne do celów identyfikacyjnych.

W konsekwencji EIOD zdecydowanie zaleca usunięcie słowa „fotografie" z pierwszej części tych artykułów i pozostawienie go w części drugiej (fotografie mogą być wykorzystywane jako narzędzie do sprawdzania czyjejś tożsamości, ale nie do identyfikowania w bazie danych o szerokim zasięgu).

Inną opcję stanowi poprawienie art. 36, tak aby zasady funkcjonowania dotyczące przetwarzania fotografii do celów identyfikacji były wprowadzane w życie tylko wtedy, gdy technologia ta jest uważana za wiarygodną (jeśli jest to możliwe, po uprzednim zasięgnięciu opinii komitetu ds. technologii).

3.7.4. *Publikacja wykazu organów posiadających dostêp (do danych)*

Art. 4 projektu rozporządzenia przewiduje publikację w *Dzienniku Urzędowym Unii Europejskiej* wykazu właściwych organów posiadających dostęp do VIS wyznaczonych przez każde Państwo Członkowskie. Wykazy te należy publikować regularnie (co roku), w celu informowania o zmianie sytuacji w poszczególnych krajach. EIOD podkreśla znaczenie takiej publikacji stanowiącej niezbędny instrument kontroli na szczeblu europejskim, jak również krajowym i lokalnym.

3.8. **Obowiązki**

Przypomina się, że VIS będzie miał scentralizowaną strukturę, składającą się z centralnej bazy danych, w której będą przechowywane wszystkie informacje dotyczące wiz oraz krajowych interfejsów znajdujących się w Państwach Członkowskich, za pośrednictwem których właściwe organy będą mieć dostęp do systemu centralnego. Zgodnie z motywami (14) i (15) projektu rozporządzenia, dyrektywa 95/46/WE będzie mieć zastosowanie do przetwarzania danych osobowych przez Państwa Członkowskie dokonywanego w ramach stosowania rozporządzenia, a rozporządzenie 45/2001 będzie mieć zastosowanie do działań Komisji powiązanych z ochroną danych osobowych. Jak wspomniano w tych motywach, wniosek ma na celu wyjaśnienie pewnych punktów, między innymi dotyczących odpowiedzialności za wykorzystywanie danych oraz nadzoru nad ochroną danych.

Rzeczywiście wydaje się, że punkty te mogą być powiązane z niektórymi zasadniczymi elementami bez których system zabezpieczeń przewidziany przez dyrektywę 95/46/WE i rozporządzenie 45/2001 nie miałby zastosowania lub też nie byłby w pełni spójny z wnioskiem. Stosowanie prawa krajowego zgodnie z dyrektywą zazwyczaj zakłada istnienie administratora danych ustanowionego w danym Państwie Członkowskim (art. 4), natomiast stosowanie rozporządzenia zależy od przetwarzania danych osobowych przez instytucję lub organ Wspólnoty w ramach wykonywania czynności, których część lub całość jest objęta zakresem prawa wspólnotowego (art. 3).

Zgodnie z art. 23 ust. 2 projektu rozporządzenia, dane są „przetwarzane przez VIS w imieniu Państw Członkowskich". Zgodnie z art. 23 ust. 3 Państwa Członkowskie wyznaczają organy traktowane jako administratorzy danych zgodnie z art. 2 lit. d) dyrektywy 95/46/WE. Wydaje się zatem, że zakłada to, zgodnie z systemem tworzonym przez dyrektywę, iż Komisja powinna być uważana za przetwarzającego. Znajduje to potwierdzenie w wyjaśnieniach do artykułów ([1]).

Takie sformułowanie prowadzi do pomniejszenia bardzo ważnej, a w zasadzie nawet kluczowej roli, jaką Komisja odgrywa zarówno na etapie tworzenia systemu, jak i w czasie jego funkcjonowania. Trudno dokładnie połączyć rolę Komisji z pojęciem administratora danych lub przetwarzającego; albo jest ona przetwarzającym posiadającym nadzwyczajne uprawnienia (w tym również do tworzenia systemu) lub administratorem danych posiadającym ograniczone uprawnienia (zważywszy że dane są wprowadzane i wykorzystywane przez Państwa Członkowskie). W rzeczywistości zatem rola Komisji w ramach VIS jest rolą *sui generis* ([2]) i za taką musi być uznana.

Ta istotna rola powinna zostać uznana poprzez zrozumiałe opisanie zadań Komisji, a nie poprzez używanie sformułowań, które niezupełnie odpowiadają rzeczywistości, ponieważ są zbyt restrykcyjne, nie zmieniają niczego w korzystaniu z VIS, a jedynie prowadzą do nieporozumień. Jest to również istotne ze względu na spójny i skuteczny nadzór nad VIS (patrz również ust. 3.11). W związku z powyższym EIOD zaleca skreślenie art. 23 ust. 2.

EIOD chciałby również podkreślić, że kompletny opis zadań Komisji w odniesieniu do VIS jest tym bardziej istotny, jeżeli Komisja zakłada powierzenie wykonywania tych zadań innemu organowi. „Fiche Financière" załączone do wniosku przewiduje możliwość przeniesienia tych zadań na agencję ds. granic zewnętrznych. W powyższym kontekście staje się niezwykle ważne, żeby Komisja nie pozostawała w niepewności co do zakresu swoich kompetencji, dzięki czemu jej następca będzie znał ramy, w których może działać.

3.9. **Bezpieczeństwo**

Zarządzanie i przestrzeganie optymalnego poziomu bezpieczeństwa w odniesieniu do VIS stanowi warunek konieczny do zapewnienia wymaganej ochrony danych osobowych przechowywanych w bazie danych systemu. W celu osiągnięcia tego satysfakcjonującego poziomu ochrony należy wdrożyć odpowiednie zabezpieczenia, dzięki którym będzie można zarządzać potencjalnym ryzykiem związanym z infrastrukturą systemu i z osobami go obsługującymi. Temat ten jest poruszany w niektórych częściach wniosku i wymaga wprowadzenia pewnych ulepszeń.

Art. 25 i 26 wniosku zawierają różne środki odnoszące się do bezpieczeństwa danych i wyszczególniają rodzaje nadużyć, którym należy zapobiegać. Jednakże te przepisy mogłyby być z pożytkiem uzupełnione o środki przewidujące systematyczne monitorowanie i sprawozdania na temat skuteczności środków bezpieczeństwa, które zostały wcześniej wspomniane. EIOD zaleca w szczególności uzupełnienie tych artykułów o przepisy dotyczące systematycznego (auto)kontroli środków bezpieczeństwa.

Powyższe powiązane jest z art. 40 wniosku, mówiącym o monitorowaniu i ocenie. Przepisy te nie powinny dotyczyć wyłącznie aspektów takich jak wydajność, opłacalność i jakość usług, ale również zgodności z wymogami stawianymi przez prawo, zwłaszcza w dziedzinie ochrony danych. EIOD zaleca zatem rozszerzenie zakresu art. 40 o monitorowanie zgodności z prawem przetwarzania danych oraz sprawozdań na ten temat.

Ponadto, w uzupełnieniu do art. 24 ust. 4 lit. c) oraz art. 26 ust. 2 lit. e) dotyczących personelu upoważnionego do dostępu do danych, należy dodać, że Państwa Członkowskie powinny zapewnić dostępność dokładnych profilów użytkowników (które należy przechowywać do dyspozycji krajowych organów nadzorczych w celu przeprowadzania kontroli). Poza wspomnianymi profilami użytkowników, Państwa Członkowskie muszą również opracować i stale uaktualniać kompletny spis tożsamości użytkowników. Powyższe ma zastosowanie do Komisji: art. 25 ust. 2 lit. b) należy zatem analogicznie uzupełnić.

([1]) Patrz str. 37 wniosku.

([2]) Chociaż definicja administratora danych zawarta w dyrektywie 95/46/WE i w rozporządzeniu 45/2001 przewiduje również możliwość istnienia większej liczby administratorów danych posiadających różny zakres obowiązków.

Powyższe środki bezpieczeństwa są uzupełniane poprzez monitorowanie i zabezpieczenia organizacyjne. Art. 28 wniosku opisuje warunki, w jakich należy przechowywać rejestry wszystkich operacji przetwarzania danych oraz cele takiego przechowywania. Rejestry te powinny być przechowywane nie tylko do celu monitorowania ochrony danych i zapewniania ich bezpieczeństwa, ale również dla przeprowadzania regularnej autokontroli w odniesieniu do VIS. Sprawozdania z takiej autokontroli przyczynią się do skutecznego wykonywania zadań przez organy nadzorcze, które będą w stanie znaleźć najsłabsze punkty i skoncentrować się na nich podczas przeprowadzania własnych procedur kontrolnych.

3.10. **Prawa osób, których dane dotyczą**

3.10.1. *Informowanie osób, których dane dotyczą*

Dostarczanie informacji osobom, których dane dotyczą, w celu zapewnienia rzetelnego przetwarzania danych ma olbrzymie znaczenie. Stanowi niezbędne zabezpieczenie praw jednostki. Art. 30 wniosku w chwili obecnej w zasadzie powtarza treść art. 10 dyrektywy 95/46/WE w tym zakresie.

Do przepisu tego można by jednak wprowadzić kilka zmian celem skuteczniejszego wpisania go w ramy VIS. W rzeczy samej dyrektywa przewiduje obowiązek udzielenia niektórych informacji, ale w większości przypadków zakłada udzielanie informacji, jeśli jest to konieczne ([1]). W konsekwencji należy zmienić art. 30, uzupełniając go o następujące punkty:

— Osoby, których dane dotyczą, powinny być również informowane o okresie przechowywania mającym zastosowanie do ich danych.

— Art. 30 ust. 1 lit. e) dotyczy „prawa dostępu do danych oraz prawa ich poprawiania". Stosowniejszym rozwiązaniem byłoby określenie „prawo dostępu do danych oraz prawo *złożenia wniosku* o ich poprawienie lub *usunięcie*". Odnośnie do tej kwestii osoby, których dane dotyczą, powinny być informowane o możliwości zwracania się o radę lub pomoc do odpowiednich organów nadzorczych.

— Na koniec art. 30 ust. 1 lit. a) mówi o informacjach na temat tożsamości administratora danych oraz jego przedstawiciela, jeżeli taki przedstawiciel istnieje. Zważywszy, że administrator danych znajduje się zawsze na terytorium Unii Europejskiej, nie ma potrzeby zakładania drugiej możliwości.

3.10.2. *Prawa do dostêpu, poprawiania i usuwania*

Ostatnie zdanie art. 31 ust. 1 mówi, że „taki dostęp do danych może być przyznany jedynie przez Państwo Członkowskie". Można założyć, że oznacza to, iż dostęp do danych (lub ich przekazywanie) nie może być przyznany przez jednostkę centralną, a wyłącznie przez Państwo Członkowskie. EIOD zaleca wyraźne stwierdzenie, że o takie przekazanie można wystąpić w każdym z Państw Członkowskich.

Ponadto wydaje się, że projekt tego przepisu zakłada brak możliwości odmówienia takiego dostępu oraz że będzie zapewniony bez zgody odpowiedzialnego Państwa Członkowskiego. To wyjaśniałoby, dlaczego organy krajowe muszą współpracować w celu zwiększenia uprawnień zawartych w art. 31 ust. 2, 3 i ust. 4, ale nie tych przewidzianych w art. 31 ust. 1 ([2]).

3.10.3. *Pomoc organów nadzorczych*

Art. 33 ust. 2 zobowiązuje krajowe organy nadzorcze do świadczenia pomocy i udzielania rad osobie zainteresowanej przez cały czas trwania postępowania (przed sądem). Sens tego ustępu nie jest jasny. Krajowe organy nadzorcze mają różne podejście odnośnie do swojej roli w czasie postępowania sądowego. Wydaje się, że w rozumieniu tego ustępu organy krajowe miałyby odgrywać przed sądem rolę adwokata strony powodowej, co w wielu krajach nie jest możliwe.

([1]) Artykuł ten stwierdza: „o ile takie dalsze informacje będą potrzebne, biorąc pod uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą".

([2]) W konsekwencji art. 31 ust. 3 dotyczący współpracy pomiędzy organami krajowymi w wykonywaniu prawa do poprawienia lub usunięcia danych mógłby dla większej przejrzystości zostać zmieniony w następujący sposób: „jeżeli wniosek, *o którym mowa w art. 31 ust. 2*" Wnioski, o których mowa w art. 31 ust. 1 (dostęp) nie wymagają współpracy pomiędzy organami.

3.11. **Nadzór**

Wniosek rozdziela zadania nadzoru pomiędzy krajowe organy nadzorcze oraz EIOD. Jest to zgodne z reprezentowanym we wniosku podejściem do prawa stosowanego i odpowiedzialności za funkcjonowanie i korzystanie z VIS oraz z potrzebą istnienia skutecznego nadzoru. Dlatego EIOD z zadowoleniem przyjmuje to podejście, wyrażone w art. 34 i 35.

Krajowe organy nadzorcze monitorują zgodność z prawem przetwarzania danych osobowych przez Państwa Członkowskie, *w tym przesyłanie tych danych do i z VIS*. EIOD monitoruje działania Komisji *(…) w tym zapewnienie tego, by dane osobowe przesyłane były w sposób zgodny z prawem pomiędzy interfejsami krajowymi i Centralnym Systemem Informacji Wizowej*. To może skutkować pokrywaniem się kompetencji, jako że zarówno krajowy organ nadzorczy jak i EIOD w tym samym czasie są odpowiedzialni za monitorowanie zgodności z prawem przesyłania danych pomiędzy interfejsami krajowymi i Centralnym Systemem Informacji Wizowej.

EIOD sugeruje zatem zmianę art. 34 w celu wyjaśnienia, że krajowe organy nadzorcze monitorują zgodność z prawem przetwarzania danych osobowych przez Państwo Członkowskie, w tym przesyłania ich do i z krajowego interfejsu VIS.

W odniesieniu natomiast do VIS istotne jest podkreślenie, że działania w zakresie nadzoru prowadzone przez krajowe organy nadzorcze i EIOD powinny być do pewnego stopnia skoordynowane celem zapewnienia wystarczającego poziomu spójności i ogólnej skuteczności. W rzeczywistości istnieje potrzeba ujednoliconego wprowadzania w życie rozporządzenia oraz działania w kierunku wypracowania wspólnego podejścia do wspólnych problemów. Ponadto w odniesieniu do bezpieczeństwa można dodać, że poziom bezpieczeństwa VIS zostanie — w sposób definitywny — określony przez poziom bezpieczeństwa jego najsłabszego ogniwa. W tej kwestii należy również nawiązać i umocnić współpracę pomiędzy EIOD i organami krajowymi. Art. 35 powinien zatem zawierać odpowiedni przepis stanowiący, że EIOD zwołuje przynajmniej raz do roku zebranie wszystkich krajowych organów nadzorczych.

3.12. **Realizacja**

Art. 36 ust. 2 wniosku postanawia: *„Środki konieczne do technicznej realizacji zasad funkcjonowania, o których mowa w ust. 1, przyjmuje się zgodnie z procedurą określoną w art. 39 ust. 2."* Art. 39 odnosi się do komitetu wspierającego Komisję, utworzonego w 2001 r ([1]). i którego pomoc była wykorzystywana przez różne instrumenty.

Techniczna realizacja zasad funkcjonowania VIS (interakcja/współdziałanie z właściwymi organami i jednolity format wiz) może w wielu aspektach wywrzeć negatywny wpływ na ochronę danych. Na przykład, wybór dotyczący umieszczenia lub nie na wizie mikrochipu, który będzie miał wpływ na sposób korzystania z centralnej bazy danych, jak również wzór formatu, jaki będzie użyty do wymiany danych biometrycznych wpłynie na politykę ochrony danych ([2]).

Ten wybór technologii będzie miał decydujące znaczenie dla właściwej realizacji zasad odnoszących się do celu i proporcjonalności i w związku z tym powinien być nadzorowany. Zatem wybór odnośnie do technologii, ze względu na fakt, że ma znaczący wpływ na ochronę danych, powinien zostać uregulowany rozporządzeniem, zgodnie z procedurą współdecydowania. Dopiero wtedy będzie mogła być zapewniona konieczna kontrola polityczna. We wszystkich innych kwestiach mających wpływ na ochronę danych, EIOD powinien mieć możliwość udzielania rad w sprawie wyborów dokonywanych przez komitet.

3.13. **Interoperacyjność**

Interoperacyjność stanowi kluczowy i zasadniczy warunek konieczny wydajności systemów informatycznych o dużym zasięgu takich jak VIS. Oferuje możliwość obniżenia w sposób spójny kosztów ogólnych oraz uniknięcia naturalnego nadmiaru elementów niejednolitych. Interoperacyjność może również wnieść wkład do wspólnej polityki wizowej poprzez zastosowanie tych samych norm proceduralnych do wszystkich jej elementów składowych. Jednakże istotne jest wprowadzenie rozróżnienia pomiędzy dwoma poziomami interoperacyjności:

— wysoce pożądana jest interoperacyjność pomiędzy Państwami Członkowskimi UE; w rzeczy samej wnioski o wydanie wizy wysłane przez organy jednego z Państw Członkowskich muszą być interoperacyjne z wnioskami wysłanymi przez organy innych Państw Członkowskich.

([1]) Rozporządzenie Rady nr 2424/2001 z dnia 6 grudnia 2001 r. w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II).

([2]) Wniosek w sprawie rozporządzenia Rady zmieniającego (WE) 1683/95 (jednolity format dla WIZ) we wrześniu 2003 r. zawierał również artykuł o podobnej treści.

— natomiast interoperacyjność pomiędzy systemami utworzonymi do innych celów lub z systemami państw trzecich budzi dużo większe wątpliwości .

Wśród dostępnych zabezpieczeń wykorzystywanych do ograniczenia celu systemu i zapobieżenia „zakłóceniom działania", znajduje się również możliwość wykorzystania różnych standardów technologicznych. Ponadto każda forma interakcji pomiędzy dwoma różnymi systemami powinna być rzetelnie udokumentowana. Interoperacyjność nigdy nie powinna prowadzić do sytuacji, w której organ nie upoważniony do dostępu lub wykorzystania pewnych danych mógłby uzyskać ten dostęp poprzez inny system.

W tym kontekście EIOD chciałby odwołać się do Deklaracji Rady z dnia 25 marca 2004 r. w sprawie zwalczania terroryzmu, w której Komisja jest proszona o przedstawienie wniosków mających za cel zwiększenie interoperacyjności i współdziałania pomiędzy systemami informacyjnymi (SIS, VIS i Eurodac).

Chciałby również odwołać się do toczącej się dyskusji zajmującej się kwestią, któremu organowi należy powierzyć w przyszłości zarządzanie różnymi systemami o dużym zasięgu (patrz również punkt 3.8 niniejszej opinii).

EIOD chciałby ponownie podkreślić, że wdrażanie interoperacyjności systemów nie może prowadzić do naruszenia zasady ograniczonego celu, oraz zaznacza, że każdy wniosek dotyczący tej kwestii powinien być mu przekazywany.

4. **WNIOSKI**

4.1. **Punkty ogólne**

1. EIOD przyznaje, że dalszy rozwój wspólnej polityki wizowej wymaga skutecznej wymiany odpowiednich danych. VIS jest jednym z mechanizmów, który może zapewnić niezakłócony przepływ informacji. EIOD zapoznał się dokładnie z argumentacją przedstawioną w rozszerzonej ocenie wpływu. Chociaż argumentacja ta nie jest w pełni jednoznaczna, wydaje się że istnieją wystarczające powody uzasadniające utworzenie VIS w celu usprawnienia wspólnej polityki wizowej.

   Jednakże ten nowy instrument powinien ograniczać się do gromadzenia i wymiany danych pod warunkiem, że gromadzenie i wymiana są konieczne do rozwoju wspólnej polityki wizowej oraz są proporcjonalne do tego celu.

2. Utworzenie VIS może mieć pozytywne konsekwencje dla uzasadnionego interesu publicznego, ale nie może to zmieniać celu VIS. Zatem wszystkie elementy składające się na VIS muszą być koniecznymi i proporcjonalnymi instrumentami służącymi osiągnięciu wspomnianego wyżej celu. Ponadto:

   — stały dostęp organów ścigania nie byłby zgodny z tym celem,

   — EIOD zaleca wprowadzenie wyraźniejszego rozróżnienia pomiędzy „celem" a „korzyściami" w tekście art. 1 ust. 2,

   — wdrażanie interoperacyjności z innymi systemami nie może prowadzić do naruszenia zasady ograniczonego celu.

3. EIOD uznaje korzyści płynące z wykorzystania danych biometrycznych, ale jednocześnie podkreśla poważne konsekwencje wynikające z ich wykorzystania oraz sugeruje wprowadzenie rygorystycznych ograniczeń w tym zakresie. Ponadto niedoskonałości techniczne w odniesieniu do odcisków palców wymagają ustanowienia procedur awaryjnych i włączenia ich do wniosku.

4. Niniejsza opinia powinna zostać uwzględniona w preambule rozporządzenia przed motywami („uwzględniając opinię ...").

4.2. **Pozostałe punkty**

5. W odniesieniu do podstaw odmowy wydania wizy: należy włączyć odniesienie do art. 29 dyrektywy 2004/58/WE do tekstu wniosku w celu zagwarantowania, że „zagrożenie dla zdrowia publicznego" jest rozumiane w świetle tego właśnie przepisu.

6. Dane dotyczące członków tej samej grupy podróżnych mają szczególne znaczenie dla wniosku: należy zatem zdefiniować „członków tej samej grupy podróżnych" w sposób dokładny i zrozumiały.

7. Nie ma żadnych dowodów wskazujących na brak zasadności przedstawionych we wniosku ram czasowych lub na konsekwencje niemożliwe do zaakceptowania pod warunkiem, że zostaną zastosowane wszystkie właściwe mechanizmy korygujące.

   Ponadto wniosek powinien wyraźnie określać, że dane osobowe muszą być w całości poddane ponownej ocenie w przypadku każdego nowego wniosku o wydanie wizy.

8. W odniesieniu do kontroli wizowej na granicach zewnętrznych: art. 16 wniosku powinien zostać zmieniony z uwagi na fakt, iż dostęp do centralnej bazy dany VIS byłby w opisanych przypadkach nieproporcjonalny. Wystarczającym rozwiązaniem jest zapewnienie dostępu do chronionego mikrochipu wyłącznie organom właściwym do przeprowadzania kontroli wizowej.

   Co więcej, jeżeli sprawdzenie tożsamości powiodło się, nie jest jasne, z jakiego powodu nadal potrzebne miałyby być pozostałe dane.

9. W odniesieniu do wykorzystywania danych do identyfikacji i deportacji nielegalnych imigrantów oraz do procedur azylowych: słowo „fotografie" powinno zostać usunięte z pierwszej części art. 17, 18 i 19 i pozostawione w części drugiej.

10. W odniesieniu do obowiązków Komisji i Państw Członkowskich: należy skreślić artykuł 23 ust. 2.

11. Wniosek należy uzupełnić o przepisy dotyczące systematycznej (auto)kontroli środków bezpieczeństwa. Należy rozszerzyć zakres art. 40 o monitorowanie zgodności z prawem przetwarzania danych oraz sprawozdań na ten temat. Ponadto:

   — Państwa Członkowskie muszą również opracować kompletny i stale uaktualniany spis tożsamości użytkowników. Powyższe ma zastosowanie do Komisji: art. 25 ust. 2 lit. b) należy zatem uzupełnić analogicznie.

   — Art. 28 wniosku opisuje warunki, w jakich należy przechowywać rejestry wszystkich operacji przetwarzania danych oraz cele takiego przechowywania. Rejestry te powinny być przechowywane nie tylko do celu monitorowania ochrony danych i zapewniania ich bezpieczeństwa, ale również dla przeprowadzania regularnej (auto)kontroli w odniesieniu do VIS.

12. W odniesieniu do praw osób, których dane dotyczą:

   — art. 30 powinien zostać zmieniony celem zapewnienia, aby osoby, których dane dotyczą, były również informowane o okresie przechowywania mającym zastosowanie do ich danych,

   — art. 30 ust. 1 lit. e) powinien brzmieć: „prawo dostępu do danych oraz prawo złożenia wniosku o ich poprawienie lub usunięcie",

   — art. 31 ust. 1 musi wyraźnie stwierdzać, że o niektóre przekazania/uzyskania danych można wystąpić w każdym z Państw Członkowskich.

13. W odniesieniu do nadzoru:

— art. 34 należy zmienić w celu wyjaśnienia, że krajowe organy nadzorcze monitorują zgodność z prawem przetwarzania danych osobowych przez Państwo Członkowskie, w tym przesyłanie ich do i z krajowego interfejsu VIS,

— art. 35 powinien zatem zawierać odpowiedni przepis stanowiący, że EIOD zwołuje przynajmniej raz w roku zebranie wszystkich krajowych organów nadzorczych.

14. W odniesieniu do realizacji:

— wybór odnośnie do technologii, ze względu na fakt, że ma wpływ na ochronę danych, powinien zostać uregulowany, jeśli jest to możliwe, rozporządzeniem, zgodnie z procedurą współdecydowania,

— - we wszystkich innych kwestiach EIOD powinien mieć możliwość udzielania rad w sprawie wyborów dokonywanych przez komitet, o którym mowa we wniosku.

Sporządzono w Brukseli, dnia 23 marca 2005 r.

Peter HUSTINX

Europejski inspektor ochrony danych