EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego wspólne instrukcje konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczące wiz w związku z wprowadzeniem technologii biometrycznych, łącznie z przepisami dotyczącymi organizacji przyjmowania i rozpatrywania wniosków wizowych (COM (2006) 269 wersja ostateczna) — 2006/0088 (COD)

(2006/C 321/14)

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 o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 otrzymany od Komisji w dniu 19 czerwca 2006 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1. **WSTĘP**

Proponowane rozporządzenie ma dwa główne cele, obydwa związane z wdrożeniem wizowego systemu informacyjnego:

— zapewnić państwom członkowskim podstawę prawną umożliwiającą obowiązkowe pobieranie identyfikatorów biometrycznych od osób ubiegających się o wizę;

— zapewnić ramy prawne organizacji urzędów konsularnych państw członkowskich, w szczególności poprzez organizowanie ewentualnej współpracy pomiędzy państwami członkowskimi w celu rozpatrywania wniosków wizowych.

Te dwa cele wiążą się z różnymi zagadnieniami dotyczącymi ochrony danych i dlatego, choć stanowią części tego samego wniosku, zostaną omówione w osobnych punktach.

Omawiany wniosek ma na celu zmianę wspólnych instrukcji konsularnych (WIK). Instrukcje te zostały przyjęte przez Komitet Wykonawczy ustanowiony na mocy konwencji wykonawczej do układu z Schengen z dnia 14 czerwca 1985 r. Jako część dorobku prawnego Schengen instrukcje te zostały włączone do prawa UE na mocy protokołu załączonego do traktatu amsterdamskiego i od tego czasu zostały kilkakrotnie zmienione. Choć pewna liczba zmian pozostaje poufna, WIK zostały opublikowane w 2000 r. Odnośnie do treści, stanowią one zasadniczo podręcznik zawierający praktyczne zasady wydawania wiz krótkoterminowych. Obejmują one przepisy dotyczące rozpatrywania wniosków wizowych, procedury decyzyjnej, sposobu wypełniania naklejek wizowych, itd.

2. GROMADZENIE IDENTYFIKATORÓW BIOMETRYCZNYCH

2.1. Uwaga wstępna: specyfika danych biometrycznych

Zgodnie z wnioskiem w sprawie VIS ([1]) przedstawionym przez Komisję dnia 28 grudnia 2004 r. państwa członkowskie wprowadzają do VIS odciski palców i fotografie jako identyfikatory biometryczne do celów weryfikacji i (lub) identyfikacji. Omawiany wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego WIK ma na celu zapewnienie podstawy prawnej gromadzenia identyfikatorów biometrycznych.

Dnia 23 marca 2005 r. EIOD wydał opinię dotyczącą wniosku w sprawie VIS ([2]). W opinii tej podkreślił znaczenie zastosowania podczas przetwarzania danych biometrycznych wszystkich koniecznych zabezpieczeń ze względu na specyfikę tych danych ([3]):

> *„Zastosowanie biometrii w systemach informatycznych nie jest wyborem bez znaczenia, zwłaszcza w sytuacji, w której system obejmuje tak wielką liczbę podmiotów. Biometria (…) zmienia 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."*

Zgodnie z opinią EIOD ten wrażliwy charakter danych biometrycznych wymaga, by wprowadzenie obowiązku stosowania tych danych miało miejsce wyłącznie po przeprowadzeniu dogłębnej analizy związanego z nim ryzyka i odbyło się zgodnie z procedurą umożliwiającą pełną demokratyczną kontrolę. Uwagi te stanowią podstawę przeprowadzonej przez EIOD analizy omawianego wniosku.

2.2. Kontekst wniosku

Kontekst, jakiego dotyczy omawiany wniosek, czyni go jeszcze bardziej wrażliwym. Proponowane rozporządzenie nie może być rozpatrywane niezależnie od rozwoju wielkoskalowych systemów informatycznych i generalnej tendencji do zwiększania interoperacyjności pomiędzy systemami informacyjnymi. O tendencji tej jest mowa między innymi w komunikacie Komisji z dnia 24 listopada 2005 r. w sprawie zwiększenia skuteczności, interoperacyjności i efektu synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych ([4]).

Dlatego decyzja podjęta w danym kontekście i mająca na względzie realizację danego celu prawdopodobnie wywrze skutki na rozwój i eksploatację innych systemów mających służyć innym celom. W szczególności dane biometryczne — prawdopodobnie obejmujące dane gromadzone w celu realizacji polityki wizowej — po ich udostępnieniu mogą być wykorzystywane w różnych kontekstach. Może to dotyczyć nie tylko ram SIS, ale z całym prawdopodobieństwem także Europolu i Fronteksu.

2.3. Obowiązek złożenia odcisków palców

W uzasadnieniu omawianego wniosku stwierdzono: „Ponieważ pobieranie identyfikatorów biometrycznych stanowić będzie element procedury ubiegania się o wizę, należy zmienić wspólne instrukcje konsularne, aby stworzyć podstawę prawną tego środka".

EIOD ma zastrzeżenia co do poczynionego przez prawodawcę wyboru, by włączyć do WIK zamiast do samego rozporządzenia w sprawie VIS przepisy dotyczące ewentualnego zwolnienia niektórych osób lub grup osób z obowiązku złożenia odcisków palców. Po pierwsze, przepisy te mają znaczny wpływ na prywatność dużej liczby osób i powinny zostać zawarte raczej w legislacji zasadniczej niż w instrukcjach o przeważająco technicznym charakterze. Po drugie, ze względu na jasność systemu prawnego korzystniejsze byłoby zajęcie się tą kwestią w tym samym akcie, który ustanawia wspomniany system informacyjny.

([1]) Wniosek dotyczący 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), przedstawiony przez Komisję dnia 28 grudnia 2004 r.

([2]) Opinia z dnia 23 marca 2005 r. 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, Dz.U. C 181 z 23.7.2005, str. 13.

([3]) „[Dane biometryczne] gwarantują […] 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.", ibid.

([4]) COM (2005) 597 wersja ostateczna.

a) Przede wszystkim, stworzenie podstawy prawnej dla obowiązkowego pobierania odcisków palców i innych identyfikatorów biometrycznych stanowi o wiele więcej, niż tylko kwestię techniczną; ma ono znaczny wpływ na prywatność osób, których dotyczy. Zwłaszcza określenie minimalnego lub maksymalnego wieku osób, od których mają być pobierane odciski palców stanowi decyzję polityczną, a nie tylko techniczną. EIOD zaleca zatem zajęcie się tą kwestią, a zwłaszcza jej nie tylko technicznymi aspektami, w tekście podstawowym (we wniosku w sprawie VIS), nie zaś w podręczniku zawierającym instrukcje dotyczące głównie technicznych i praktycznych aspektów procedury wizowej ([1]).

   W tym względzie pożyteczne jest także przypomnienie wymogów Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności (ECHR) i związanego z nią orzecznictwa. Zgodnie z art. 8 ust. 2 ECHR jakakolwiek ingerencja władzy publicznej w korzystanie z prawa do prywatności 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 (musi ona pochodzić z dostępnych aktów prawnych i być przewidywalna), proporcjonalność środków i konieczność odpowiedniego zabezpieczenia przed nadużyciami.

   Prócz faktu, że opisane tutaj niespójne podejście do legislacji nie wspomaga jasności i dostępności uregulowań, należy się zastanowić, czy same WIK można zaklasyfikować jako jasne i dostępne. Można też postawić pewne pytania dotyczące procedury (ewentualnych) przyszłych zmian omawianego tekstu. W jakimkolwiek przypadku należy zagwarantować, że tak ważna decyzja nie będzie mogła zostać zmieniona bez zastosowania procedury zapewniającej właściwą przejrzystość procesu i demokratyczną konsultację.

b) Druga kwestia dotyczy jasności systemu prawnego. W uzasadnieniu wniosku nie jest jasne, dlaczego do gromadzenia identyfikatorów biometrycznych i do ich przetwarzania konieczne są różne podstawy prawne. Stwierdza się w nim, że „wniosek dotyczy gromadzenia danych biometrycznych, podczas gdy wniosek w sprawie VIS obejmuje przekazywanie i wymianę danych" ([2]). Jednak z punktu widzenia ochrony danych przetwarzanie danych osobowych obejmuje ich gromadzenie. Regulacja działań, które są ze sobą powiązane, za pomocą różnych tekstów prawnych może być ze szkodą dla jasności systemu. Stanowi to problem dla osób, których dotyczą dane (na które ma wpływ omawiany wniosek) oraz dla demokratycznej kontroli systemu. Coraz trudniejsze staje się zbudowanie pełnego obrazu w tej dziedzinie, w której różne akty legislacyjne regulują zasadniczo ten sam proces przetwarzania danych.

2.4. **Zwolnienia z obowiązku składania odcisków palców**

Bardzo dobrą ilustracją powyższych obaw jest kwestia kategorii osób zwolnionych z obowiązku składania odcisków palców, w szczególności małych dzieci.

Dopuszczalność pobierania odcisków palców małych dzieci należy omówić w świetle celu samego VIS. Innymi słowy, nałożenie obowiązku pobierania identyfikatorów biometrycznych na pewne kategorie osób lub zwolnienie ich z tego obowiązku musi stanowić środek proporcjonalny w ramach polityki wizowej i związanych z nią celów określonych we wniosku w sprawie VIS. Proporcjonalność ta powinna zostać oceniona w ramach demokratycznej procedury.

Należy również przeprowadzić jej ocenę w świetle planowanego wykorzystania tych odcisków palców, opisanego we wniosku w sprawie VIS. Dane biometryczne będą wykorzystywane do celów weryfikacji lub identyfikacji: dany identyfikator biometryczny mógłby zostać uznany za odpowiedni technicznie tylko do jednego z tych celów. Przetwarzanie odcisków palców dzieci poniżej wieku 14 lat zwykle uznaje się za wystarczająco wiarygodne jedynie do celów weryfikacji. Powinno to wpłynąć na analizę omawianego wniosku, lecz niezbędnych elementów (co do których nie podjęto dotąd decyzji) znowu należy szukać we wniosku w sprawie VIS.

Podsumowując, EIOD zdecydowanie zaleca — dla zachowania jasności i spójności — ścisłe uregulowanie w rozporządzeniu w sprawie VIS zwolnień z obowiązku składania identyfikatorów biometrycznych. Uregulowanie gromadzenia identyfikatorów biometrycznych, a zwłaszcza odcisków palców w tym przypadku powinno być postrzegane jako dodatek do głównego aktu prawnego i dlatego powinno zostać ujęte w samym dokumencie głównym.

([1]) Fakt, że różni się podstawa prawna — art. 62 ust. 2 lit. b) pkt (ii) dla WIK, art. 66 dla wniosku w sprawie VIS — nie uniemożliwia prawodawcy zajęcia się tą kwestią w jednym akcie.

([2]) Uzasadnienie wniosku, str. 5.

2.5. **Wiek osób ubiegających się o wizę**

We wniosku określono, że jedynie dzieci poniżej 6 roku życia są zwolnione z obowiązku składania odcisków palców. Wiąże się to z licznymi pytaniami (niezależnie od tego, czy kwestia ta zostanie ujęta we wniosku w sprawie VIS lub WIK).

Po pierwsze, EIOD jest zdania, że powszechne pobieranie odcisków palców dzieci nie może być postrzegane wyłącznie jako wymóg techniczny i powinno wiązać się z poważną demokratyczną debatą na forum właściwych instytucji. Decyzja taka powinna się zasadzać nie tylko na technicznej wykonalności, lecz także co najmniej na korzyściach, jakie przyniosłaby wdrożeniu VIS. Wydaje się jednak, że kwestia ta nie jest obecnie przedmiotem debaty publicznej (z wyjątkiem nielicznych państw członkowskim), co jest godne ubolewania.

Należy również przypomnieć, że VIS ustanowiono zasadniczo w celu ułatwienia procedur wizowych dla osób podróżujących w dobrej wierze (większości podróżnych). Dlatego należy uwzględnić takie aspekty jak wygoda i ergonomiczność ([1]). Wykorzystanie identyfikatorów biometrycznych podczas procedury ubiegania się o wizę lub w czasie kontroli granicznej nie powinno zbytnio utrudniać wypełnienia wymogów procedury wizowej dla dzieci.

Ponadto należy przypomnieć, że żaden system identyfikacji biometrycznej nie jest pozbawiony niedociągnięć technicznych. Literatura naukowa nie zawiera jednoznacznych dowodów na to, by pobieranie odcisków palców od dzieci poniżej 14 roku życia mogło umożliwić wiarygodne ustalenie tożsamości. Jedyne doświadczenia przeprowadzone jak dotąd na dużej populacji pochodzą z systemów Eurodac i US-Visit. Co ciekawe, obydwa te systemy wykorzystują jednak odciski palców dzieci powyżej 14 roku życia. Pobieranie odcisków palców od młodszych dzieci powinno zostać poparte badaniami dowodzącymi ich dokładności i przydatności w kontekście tak wielkiej bazy danych jak VIS.

W jakimkolwiek przypadku byłoby wskazane wykorzystanie odcisków palców młodszych dzieci raczej do porównań indywidualnych (kontrola „jeden do jednego") niż do porównań w oparciu o wielorakie zestawy danych (kontrola „jeden do wielu"). Tę kwestię należy jednoznacznie uregulować.

Większość poczynionych tutaj uwag dotyczy nie tylko dzieci, lecz także osób starszych. Dokładność odcisków palców i możliwość ich wykorzystania zmniejszają się wraz z wiekiem osoby, do której należą ([2]), i kwestie wygody i ergonomii stają się szczególnie istotne.

2.6. **Fotografie**

To samo można powiedzieć o fotografiach, dla których ani w omawianym wniosku, ani we wniosku w sprawie VIS nie przewidziano limitu wieku. Można jednak postawić pytanie, czy zdjęcia dzieci, zanim nabędą dorosłych rysów twarzy, są rzeczywiście przydatne do celów identyfikacji, a nawet weryfikacji.

Rozpoznawanie rysów twarzy dzieci (zarówno automatyczne, w przyszłości, jak dokonywane przez inne osoby) na podstawie obrazów sprzed kilku lat prawdopodobnie będzie prowadzić do problemów. Nawet jeżeli technika rozpoznawania rysów twarzy poczyni znaczne postępy, jest wysoce nieprawdopodobne, by oprogramowanie było w stanie w bliskiej przyszłości skompensować wywołane wiekiem zmiany w twarzach dzieci. Zatem w rozporządzeniu w sprawie VIS należy wyjaśnić, że fotografie mogą być wykorzystywane wyłącznie jako element dodatkowy służący weryfikacji tożsamości lub identyfikacji osób, dopóki technika rozpoznawania rysów twarzy nie będzie wystarczająco wiarygodna, z uwzględnieniem faktu, że dzieci może to dotyczyć w bardziej odległej przyszłości.

Ogólnie rzecz biorąc, dla obydwu identyfikatorów biometrycznych EIOD zaleca poważne zastanowienie się nad kwestią, czy korzyści (walka z nielegalną imigracją i przemytem dzieci) przewyższają opisane powyżej wady.

2.7. **Inne zwolnienia**

We wniosku określono, że osoby ubiegające się o wizę, „od których pobranie odcisków palców jest fizycznie niemożliwe" są zwolnione z obowiązku ich składania.

([1]) Jak podkreślono w studium zleconym przez rząd holenderski, w. J.E. DEN HARTOGH et al., *How do you measure a child? A study into the use of biometrics in children*, 2005, TNO. (Jak zmierzyć dziecko? Studium wykorzystania danych biometrycznych pochodzących od dzieci)

([2]) Zob. e.g. A. HICKLIN and R. KHANNA, *The Role of Data Quality in Biometric Systems (Rola jakości danych w systemach biometrycznych)*, MTS, 9 lutego 2006 r.

EIOD podkreślił już w opinii na temat wniosku w sprawie VIS, że dotyczy to znacznej liczby osób: twierdzi się, że w stosunku do 5 % populacji nie jest możliwe wprowadzenie odpowiednich danych. W odniesieniu do bazy danych, do której wprowadza się 20 000 000 rekordów rocznie, oznacza to, że rocznie może być do 1 000 000 przypadków trudności z wprowadzeniem danych. Podczas analizy omawianego wniosku należy brać to pod uwagę. Ponadto EIOD podkreślił potrzebę skutecznych procedur awaryjnych:

„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."

Proponowane rozporządzenie przewiduje wprowadzenie do VIS w tych przypadkach adnotacji „nie dotyczy". Co oczywiste, EIOD przyjmuje to z zadowoleniem. Można jednak obawiać się, że niezdolność do podania danych mogłaby prowadzić do częstszych odmów przyznania wizy. Jest nie do przyjęcia, by w bardzo dużej części przypadków niezdolność do podania danych prowadziła do odmowy wydania wizy.

Należy zatem dodać do rozporządzenia w sprawie VIS przepis określający, że niezdolność do podania danych nie prowadzi automatycznie do negatywnej opinii w sprawie wydania wizy. Ponadto w sprawozdaniach przewidzianych w rozporządzeniu w sprawie VIS należy zwrócić szczególną uwagę na fakt, by monitorować wysoką liczbę odmów wydania wizy w połączeniu z fizyczną niemożnością podania danych.

3. ZLECANIE PRZYJMOWANIA WNIOSKÓW WIZOWYCH

Aby zmniejszyć obciążenie nałożone na każde państwo członkowskie (związane m.in. z kosztami zakupu i utrzymania sprzętu), wniosek umożliwia zastosowanie kilku mechanizmów współpracy:

— wspólna placówka: personel należący do co najmniej jednego państwa członkowskiego rozpatruje złożony mu wniosek wizowy (w tym identyfikatory biometryczne) w misji dyplomatycznej lub urzędzie konsularnym innego państwa członkowskiego, wykorzystując sprzęt należący do tego państwa członkowskiego;

— wspólne ośrodki składania wniosków wizowych: personel misji dyplomatycznych co najmniej jednego państwa członkowskiego jest zebrany w jednym budynku w celu przyjmowania składanych mu wniosków wizowych (w tym identyfikatorów biometrycznych);

— ponadto wniosek przewiduje, że przyjmowanie formularzy wniosku wizowego i pobieranie identyfikatorów biometrycznych mogłoby być przeprowadzane przez zewnętrznego usługodawcę (ta opcja zdaje się ostatnim możliwym rozwiązaniem dla państw członkowskich, które nie są w stanie skorzystać z żadnej z powyższych dwu możliwości, choć nie jest to zupełnie jasne).

We wniosku usilnie starano się zagwarantować, że wybierani będą wyłącznie wiarygodni usługodawcy zewnętrzni i że muszą oni być w stanie przedsięwziąć wszystkie konieczne środki ochrony danych „przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub udostępnieniem (…)" (art. 1.B.2 wniosku).

Przepis ten został opracowany bardzo starannie i ze zwróceniem szczególnej uwagi na kwestie ochrony danych, co EIOD przyjmuje z zadowoleniem. Rozpatrywanie wniosków wizowych przez usługodawcę zewnętrznego w państwie trzecim ma jednak pewne konsekwencje co do ochrony (czasami bardzo wrażliwych) danych gromadzonych do celów wydawani wiz.

EIOD podkreśla zwłaszcza, że:

— może okazać się bardzo trudne, a być może wręcz niemożliwe przeprowadzenie sprawdzeń dotyczących pracowników ze względu na prawodawstwo lub praktyki danego państwa trzeciego;

— podobnie nie jest pewna możliwość nałożenia kar na pracowników usługodawcy zewnętrznego za naruszenie prawa w zakresie prywatności (nawet jeżeli do głównego wykonawcy można zastosować kary umowne);

— na przedsiębiorstwo prywatne może wywierać wpływ niestabilna sytuacja polityczna lub jej zmiany i może ono przez to nie być w stanie wypełniać swych zobowiązań w odniesieniu do bezpieczeństwa przetwarzania danych;

— trudne byłoby wprowadzenie skutecznego nadzoru, choć biorąc pod uwagę partnerów zewnętrznych byłby on jeszcze bardziej uzasadniony.

Jakikolwiek kontrakt z usługodawcami zewnętrznymi powinien zatem zawierać konieczne gwarancje zapewniające spełnienie wymogów ochrony danych, w tym audytów zewnętrznych, regularne kontrole na miejscu, sprawozdania, mechanizmy zapewniające odpowiedzialność usługodawcy w przypadku naruszenia prawa dotyczącego prywatności, w tym zobowiązanie do odszkodowania na rzecz osób poszkodowanych w wyniku działania usługodawcy.

Co może okazać się nawet bardziej istotne, poza tymi obawami należy mieć świadomość, że państwa członkowskie nie będą w stanie zagwarantować ochrony przetwarzania danych powierzonego usługodawcom zewnętrznym (lub przetwarzania danych we wspólnym ośrodku składania wniosków wizowych, jeżeli znajduje się on w budynku poza terenem misji dyplomatycznej) przed ewentualną interwencją (np. przeszukaniem lub zajęciem) ze strony organów władzy publicznej państwa, z którego pochodzą osoby ubiegające się o wizę ([1]).

Zewnętrzni usługodawcy, pomimo wszystkich postanowień umowy, będą związani prawem krajowym państwa trzeciego, w którym mają siedzibę. Niedawne wydarzenia dotyczące dostępu organów państwa trzeciego do danych finansowych przetwarzanych przez przedsiębiorstwo z UE pokazują, że niebezpieczeństwo to bynajmniej nie jest wyłącznie teoretyczne. Ponadto mogłoby to oznaczać zwiększenie ryzyka dla osób ubiegających się o wizę w niektórych państwach trzecich, których organom zależy (do celów politycznej kontroli oponentów i dysydentów) na informacji, którzy obywatele starają się o wizę. Personel prywatnego przedsiębiorstwa, w większości wypadków prawdopodobnie zatrudniony na miejscu, nie byłby w stanie przeciwstawić się naciskom rządów lub organów ochrony porządku publicznego państw, z których pochodzą osoby ubiegające się o wizę, jeżeli te rządy lub organy wymagałyby od nich udostępnienia danych.

Stanowi to poważną wadę systemu w porównaniu z sytuacją, w której dane są przetwarzane w obrębie urzędu konsularnego lub misji dyplomatycznej. W takim przypadku dane byłyby chronione na mocy konwencji wiedeńskiej z dnia 18 kwietnia 1961 r. o stosunkach dyplomatycznych. Art. 21 tej konwencji stwierdza, że:

> *„Pomieszczenia misji są nietykalne. Funkcjonariusze państwa przyjmującego nie mogą do nich wkraczać, chyba że uzyskają na to zgodę szefa misji. (…) Pomieszczenia misji, ich urządzenia i inne przedmioty, które się w nich znajdują, oraz środki transportu misji nie podlegają rewizji, rekwizycji, zajęciu lub egzekucji”.*

Ponadto, zgodnie z art. 4 ust. 1 lit. b) dyrektywy 95/46/WE przepisy krajowe wdrażające dyrektywę miałyby również bezpośrednie zastosowanie do takiego przetwarzania danych osobowych, wzmacniając ich ochronę.

Wydaje się więc oczywiste, że jedynym skutecznym sposobem ochrony danych dotyczących osób ubiegających się o wizę oraz osób pokrywających koszty ich pobytu (obywateli UE lub przedsiębiorstw z UE) jest zapewnienie im ochrony zagwarantowanej w konwencji wiedeńskiej. Oznacza to, że dane powinny być przetwarzane w obiektach znajdujących się pod ochroną dyplomatyczną. Nie uniemożliwiłoby to państwom członkowskim zlecania przetwarzania wniosków wizowych, o ile wykonawca zewnętrzny jest w stanie prowadzić swoją działalność w obrębie misji dyplomatycznej. Odnosi się to również do wspólnych ośrodków składania wniosków wizowych.

EIOD zatem zdecydowanie odradza zlecanie usługodawcom zewnętrznym przewidziane na str. 15 wniosku, w nowym punkcie 1.B.1 b). Możliwe do przyjęcia są następujące rozwiązania:

— zlecanie przetwarzanie wniosków wizowych przedsiębiorstwom prywatnym, o ile działają w miejscu o statusie dyplomatycznym;

— zlecanie wyłącznie udzielania informacji telefonicznemu centrum obsługi klienta, zgodnie z proponowanym punktem 1.B.1.a).

4. **PODSUMOWANIE**

EIOD z zadowoleniem przyjmuje fakt, że wniosek dotyczący zmiany wspólnych instrukcji konsularnych ma zostać przyjęty w ramach procedury współdecyzji, co zwiększa możliwość demokratycznej kontroli dziedziny, która z pewnością tego wymaga.

([1]) Problem ten już istnieje i jest związany z przetwarzaniem wniosków wizowych przez biura podróży;staje się jednak jeszcze poważniejszy od chwili zastosowania danych biometrycznych oraz dlatego, że zasadniczo korzystanie z usług biura podróży nie jest obowiązkowe.

Co do treści EIOD zaleca:

— w celu zapewnienia jasności i spójności systemu ujęcie w rozporządzeniu w sprawie VIS, nie zaś WIK, zwolnień z obowiązku składania odcisków palców;

— dogłębne rozważenie limitów wiekowych pobierania odcisków palców i fotografii z uwzględnieniem wykonalności, a także etyki, wygody i dokładności;

— by nie uznawać fotografii za samodzielną metodę identyfikacji, lecz jedynie za jej pomocniczy element;

— by dopuszczać zlecanie przetwarzania wniosków wizowych przedsiębiorstwom prywatnym tylko jeżeli odbywa się ono w miejscu cieszącym się ochroną dyplomatyczną i na podstawie klauzul umownych zapewniających skuteczny nadzór oraz odpowiedzialność wykonawcy.

Sporządzono w Brukseli, dnia 27 października 2006 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych