EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego decyzji Rady w sprawie wglądu do danych Systemu Informacji Wizowej (VIS) dla organów Państw Członkowskich odpowiedzialnych za bezpieczeństwo wewnętrzne oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw (COM(2005) 600 wersja ostateczna)

(2006/C 97/03)

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 29 listopada 2005 r.;

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1. WSTĘP

1.1. Uwaga wstępna

Wniosek dotyczący decyzji Rady w sprawie wglądu do danych Systemu Informacji Wizowej dla organów Państw Członkowskich odpowiedzialnych za bezpieczeństwo wewnętrzne oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw (zwany dalej „wnioskiem") zostały skierowany do Europejskiego Inspektora Ochrony Danych (EIOD) za pośrednictwem pisma wysłanego przez Komisję w dniu 24 listopada 2005 r. EIOD przyjmuje, że pismo to stanowi prośbę o opinię dla instytucji i organów wspólnotowych, zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. EIOD uważa, że należy uwzględnić niniejszą opinię w preambule do decyzji.

EIOD podkreśla znaczenie wydania opinii dotyczącej tego delikatnego tematu, ponieważ omawiany wniosek związany jest bezpośrednio z ustanowieniem systemu VIS, który on sam będzie nadzorował, i w sprawie którego wydał już opinię w dniu 23 marca 2005 r. ([1]) Wspomniana opinia przewiduje możliwość dostępu przez organy ochrony porządku publicznego (patrz poniżej); wprowadzenie nowych praw dostępu do VIS będzie miało — w odniesieniu do ochrony danych — decydujący wpływ na ten system. Wydanie opinii w sprawie omawianego wniosku jest zatem niezbędne jako uzupełnienie pierwszej opinii.

1.2. Znaczenie wniosku

a) *Kontekst*

Omawiany wniosek ma duże znaczenie nie tylko z uwagi na zawarte w nim zagadnienia merytoryczne, ale również ze względu na fakt, że wpisuje się w ogólną tendencję udzielania organom ochrony porządku publicznego dostępu do wielu systemów informacyjnych i identyfikacyjnych o dużym zasięgu. O tendencji tej jest mowa między innymi w komunikacie Komisji z dnia 24 listopada 2005 r. w sprawie w sprawie zwiększenia skuteczności, interoperacyjności i efektu synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych ([2]), a w szczególności w pkt 4.6 tego komunikatu: „*W kontekście walki z terroryzmem i przestępczością Rada uznaje obecnie, że brak dostępu organów odpowiedzialnych za bezpieczeństwo wewnętrzne do danych VIS stanowi niedociągnięcie. Takie samo stwierdzenie można także sformułować w odniesieniu do wszystkich danych SIS II dotyczących imigracji oraz danych EURODAC.*"

Omawiany wniosek mógłby więc być postrzegany jako prekursor instrumentów prawnych tego rodzaju mających zastosowanie do innych baz danych; kluczową kwestią staje się określenie od samego początku przypadków, w których dostęp taki byłby dopuszczalny.

([1]) 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).

([2]) KOM(2005) 597 wersja ostateczna.

b) *Skutki rozszerzenia dostępu do VIS*

EIOD przyznaje, że niewątpliwie istnieje potrzeba zapewnienia organom ochrony porządku *publicznego* możliwości korzystania z najlepszych dostępnych narzędzi mających pomóc w identyfikacji sprawców aktów terrorystycznych lub innych poważnych przestępstw. Jest on również świadomy, że w niektórych sytuacjach dane zawarte w VIS mogą stanowić podstawowe źródło informacji dla tych organów.

Niemniej jednak nie można pomniejszać znaczenie udzielenia organom ochrony porządku publicznego dostępu do baz danych pierwszego filaru, bez względu na to, w jak dużym stopniu dostęp ten miałby być uzasadniony walką z terroryzmem. Nie wolno zapominać, że VIS jest systemem informacyjnym mającym służyć realizacji europejskiej polityki wizowej, a nie narzędziem służącym ochronie porządku publicznego. Stały dostęp w rzeczy samej stanowiłby poważne naruszenie zasady ograniczenia celu. Oznaczałby on nieuzasadnione naruszenie prawa do prywatności przysługującego podróżnym, którzy w celu otrzymania wizy zgodzili się na przetwarzanie swoich danych, i którzy spodziewają się, że ich dane będą zbierane, konsultowane i przekazywane tylko do tego celu.

Jako że systemy informacyjne są tworzone w określonym celu, który determinuje ochronę, bezpieczeństwo i warunki dostępu do nich, udzielenie stałego dostępu w celu różniącym się od celu pierwotnego nie tylko naruszyłoby zasadę ograniczenia celu, ale również mogłoby spowodować, że wymienione elementy stałyby się nieadekwatne lub niewystarczające.

Zgodnie z tym tokiem rozumowania, tak istotna zmiana systemu mogłaby zniweczyć rezultaty badania oceny skutków (które dotyczyło wyłącznie wykorzystania systemu do celu pierwotnego). To samo ma zastosowanie do opinii organów ochrony danych. Można by twierdzić, że nowy wniosek zmienia przesłanki analiz zgodności przeprowadzonych przez te organy.

c) *Ścisłe ograniczenie dostępu*

W świetle poczynionych powyżej uwag EIOD chciałby podkreślić, że dostęp organów ochrony porządku publicznego do VIS może być udzielony wyłącznie w określonych sytuacjach, indywidualnie dla każdego przypadku oraz muszą mu towarzyszyć restrykcyjne zabezpieczenia. Innymi słowy możliwość wglądu przez organy ochrony porządku publicznego musi zostać ograniczona — za pomocą właściwych środków technicznych i prawnych — do określonych przypadków.

EIOD zwrócił uwagę na ten problem już w opinii w sprawie VIS: „*EIOD jest świadomy, że organy ochrony porządku publicznego są zainteresowane uzyskaniem 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.*”

Podstawowe wymogi można podsumować w następujący sposób:

— Nie należy udzielać stałego dostępu: decyzja musi zagwarantować każdorazowe rozpatrzenie konieczności i proporcjonalności dostępu organów trzeciego filaru indywidualnie dla każdego przypadku. W związku z tym kwestią o najwyższym znaczeniu staje się precyzyjne sformułowanie przepisów prawnych nie zostawiające miejsca na szeroką interpretację, która prowadziłaby do udzielenia stałego dostępu.

— W razie udzielenia dostępu należy przyjąć właściwe zabezpieczenia i zapewnić odpowiednie warunki, obejmujące ogólny system ochrony danych w krajowym wykorzystaniu danych, uwzględniający wrażliwy charakter takiego dostępu.

1.3 **Uwagi wstępne**

EIOD uznaje, że w proponowanym akcie prawnym ochronie danych została poświęcona znaczna uwaga, przede wszystkim poprzez ograniczenie dostępu do VIS do konkretnych przypadków i tylko w ramach walki z poważnymi przestępstwami ([1]).

Spośród pozostałych pozytywnych rozwiązań EIOD chciałby również wspomnieć w szczególności:

— ograniczenie do niektórych rodzajów przestępstw, zgodnie z konwencją o Europolu;

— obowiązek państw członkowskich sporządzenia wykazu organów posiadających dostęp do VIS i podanie takich wykazów do publicznej wiadomości;

— istnienie centralnego punktu kontaktowego w każdym państwie członkowskim (oraz wyspecjalizowanej jednostki w ramach Europolu), ułatwiającego sprawne rozpatrywanie wniosków o dostęp oraz pozwalające na skuteczniejszy nadzór;

— precyzyjne zasady dotyczące dalszego transferu danych, zgodnie z art. 8 ust. 5 wniosku;

— obowiązek państw członkowskich i Europolu prowadzenia rejestru osób odpowiedzialnych za wgląd do danych.

2. **ANALIZA WNIOSKU**

2.1. **Uwaga wstępna**

W celu udzielenia dostępu organom w ramach trzeciego filaru, podstawowy wniosek w sprawie VIS dotyczący pierwszego filaru powinien zawierać klauzulę pomostową, która określiłaby w sposób zasadniczy dopuszczalną treść aktu prawnego — takiego jak omawiany wniosek — dotyczącego trzeciego filaru. W momencie wydania przez EIOD opinii w sprawie VIS klauzula taka nie została jeszcze wprowadzona, i tym samym EIOD nie mógł zgłosić do niej uwag. Wszystkie uwagi znajdujące się poniżej zostały zatem poczynione z zastrzeżeniem odnoszącym się do treści klauzuli pomostowej.

([1]) Takie rozwiązanie jest również spójne z konkluzjami Rady z marca i czerwca 2005 roku, w których stwierdzono, że dostęp do VIS powinien być udzielany organom odpowiedzialnym za bezpieczeństwo wewnętrzne „*w ścisłej zgodności z przepisami dotyczącymi ochrony danych osobowych*”.

2.2 **Cel dostępu**

Wyraźne zdefiniowanie warunków udzielenia dostępu do VIS staje się szczególnie istotne w odniesieniu do kwestii skutecznego ograniczenia dostępu. Zadowolenie budzi fakt, że nie tylko sama proponowana decyzja, ale również poprzedzające ją uzasadnienie i motywy (patrz zwłaszcza motyw 7.) w sposób wyraźny wskazują, że celem wniosku jest zapewnienie dostępu wyłącznie na zasadzie indywidualnego rozpatrywania każdego przypadku.

Art. 5 można opatrzyć komentarzem, który powinny pomóc w jego właściwej interpretacji.

W artykule tym dostęp zostaje ograniczony następującymi zasadniczymi warunkami:

b) wgląd do danych zgromadzonych w systemie musi być konieczny w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom lub w celu ich wykrywania i ścigania;

c) wgląd do danych zgromadzonych w systemie musi być konieczny w danym szczególnym przypadku (…), oraz

d) muszą istnieć uzasadnione powody, oparte na materiale faktycznym, aby uznać, że wgląd do danych zgromadzonych w VIS przyczyni się do zapobiegania wszelkim wspomnianym przestępstwom lub do ich wykrywania i ścigania.

Warunki te muszą wystąpić łącznie; warunek zawarty w lit. b) stanowi raczej definicję zakresu *ratione materiae*. Praktycznie rzecz ujmując oznacza to, że organ starający się o uzyskanie dostępu musi mieć do czynienia z poważnym przestępstwem, o którym mowa w lit. b) wniosku; musi być to dany szczególny przypadek, o którym mowa w lit. c). Ponadto organ musi być w stanie udowodnić, że w danym szczególnym przypadku wgląd do danych zawartych w VIS przyczyni się do zapobiegania temu przestępstwu lub do jego wykrywania albo ścigania, zgodnie z lit. d).

Nawet przy takiej interpretacji art. 5. EIOD jest zaniepokojony elastycznym sformułowaniem lit. d): określenie „przyczyni się do" jest pojęciem szerokim. W wielu przypadkach dane zawarte w VIS mogłyby „przyczynić się do" zapobiegania poważnym przestępstwom lub ich ścigania. Według opinii EIOD, aby uzasadnić dostęp do danych zawartych w VIS przy uchyleniu zasady ograniczenia celu, dostęp ten powinien „przyczyniać się w znacznym stopniu do" zapobiegania poważnym przestępstwom, ich wykrywania lub ścigania; w związku z czym EIOD proponuje odpowiednią zmianę art. 5.

Art. 10 przewiduje, że w rejestrze powinien zostać odnotowany dokładny cel wglądu do danych.„Dokładny cel" powinien obejmować elementy, które sprawiły, że wgląd do VIS był niezbędny zgodnie z art. 5 lit. d). Takie rozwiązanie pomogłoby w zagwarantowaniu, że każdy wgląd do VIS jest oceniany pod względem niezbędności oraz zmniejszyłoby ryzyko stałego dostępu.

2.3. **Kryteria wyszukiwania w bazie danych VIS**

Art. 5 ust. 2 i 3 przewiduje dwustopniowy dostęp do danych zawartych w VIS, zakładający, że pewien zestaw danych będzie dostępny tylko, jeżeli uzyskano wcześniej pozytywny wynik w przeszukiwaniu pierwszego zestawu danych. Jest to słuszne podejście. Niemniej jednak pierwszy zestaw danych wydaje się bardzo obszerny. W szczególności można zakwestionować słuszność umieszczenia w pierwszym zestawie danych wymienionych w art. 5 ust. 2 lit. e) i i):

— „Cel podróży" wydaje się być kryterium o znacznym stopniu ogólności, uniemożliwiającym skuteczne przeszukiwanie systemu. Ponadto pociąga ono za sobą ryzyko przeprowadzania podziałów podróżnych na kategorie na podstawie tego elementu.

— W odniesieniu do „fotografii" — możliwość przeszukiwania tak dużej bazy danych na podstawie fotografii jest ograniczona; wyniki takiego wyszukiwania zawierają, na obecnym etapie rozwoju technologicznego, zbyt wysoki odsetek błędnych trafień. Konsekwencje płynące z błędnej identyfikacji są bardzo poważne dla zainteresowanej osoby.

EIOD wnioskuje zatem, aby dane wymienione w art. 5 ust. 2 lit. e) i i) zostały uznane za informacje dodatkowe dostępne tylko, jeżeli pierwszy wgląd do systemu pokaże, że w systemie znajdują się już przedmiotowe dane oraz aby dane te przenieść do art. 5 ust. 3.

Rozwiązaniem alternatywnym mogłoby być uzależnienie możliwości przeszukiwania bazy danych na podstawie fotografii od oceny przez komitet doradczy zasadności stosowania takiej techniki; możliwość taka mogłaby zostać wprowadzona dopiero wtedy, gdy technika osiągnie stopień zaawansowania gwarantujący wystarczający stopień niezawodności.

2.4. **Zastosowanie do państw członkowskich, do których nie ma zastosowania rozporządzenie w sprawie VIS**

Organy państw członkowskich nie objętych systemem VIS odpowiedzialne za bezpieczeństwo wewnętrzne mogą mieć dostęp do tego systemu w celu wglądu. Konsultacja taka musi odbywać się za pośrednictwem państwa członkowskiego uczestniczącego w VIS, przy odpowiednim poszanowaniu warunków przewidzianych w art. 5 ust. 1 lit. b)-d) (czyli przy indywidualnym rozpatrzeniu każdego przypadku) i poprzedzona jest złożeniem właściwie uzasadnionego wniosku w formie pisemnej.

EIOD chciałby podkreślić konieczność nałożenia pewnych warunków na przetwarzanie danych wykraczające poza wgląd. Zasada mająca zastosowanie do państw członkowskich uczestniczących w VIS stanowi, że dane, po ich pobraniu z VIS, muszą być przetwarzane zgodnie z decyzją ramową w sprawie ochrony danych w trzecim filarze (patrz poniżej). Ten sam warunek powinien stosować się do państw członkowskich, do których nie ma zastosowania rozporządzenie w sprawie VIS, ale które mają wgląd do danych zawartych w tym systemie. Ten sam tok rozumowania należy zastosować w odniesieniu do przechowywania rejestrów do celów przyszłego nadzoru. EIOD zaleca zatem dodanie w art. 6 wniosku ustępu, zgodnie z którym art. 8 i 10 decyzji ma zastosowanie również do państw członkowskich, do których nie ma zastosowania rozporządzenie w sprawie VIS.

2.5. **System ochrony danych**

a) *Stosowanie decyzji ramowej w sprawie ochrony danych w trzecim filarze*

Jako że dostęp organów odpowiedzialnych za bezpieczeństwo wewnętrzne stanowi wyjątek nieobjęty celem VIS, powinien on podlegać spójnemu systemowi ochrony danych zapewniającemu wysoki stopień ochrony danym pobranym z VIS i przetwarzanym przez organy krajowe lub Europol.

Art. 8 wniosku stanowi, że decyzja ramowa Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (zwana dalej „decyzją ramową") ma zastosowanie do przetwarzania danych zgodnie z proponowaną decyzją. W odniesieniu do ochrony danych omawiany wniosek powinien zatem być postrzegany jako przepisy szczególne uzupełniające przepisy ogólne (tj. decyzję ramową) lub je precyzujące. Na przykład zawarte w omawianym wniosku zasady dotyczące dalszego transferu danych są bardziej restrykcyjne i powinny być stosowane. To samo ma zastosowanie do podstaw dostępu do danych.

b) *Zakres stosowania*

EIOD z zadowoleniem przyjmuje fakt, że system ochrony danych przewidziany w decyzji ramowej ma zastosowanie do każdego rodzaju przetwarzania danych osobowych zgodnie z proponowaną decyzją. Oznacza to, że poziom ochrony danych jest taki sam, bez względu na to, jakie organy mają wgląd od danych znajdujących się w VIS.

Ponieważ art. 2 w celu określenia tych organów stosuje kryteria funkcjonalne („organy państw członkowskich, które są odpowiedzialne za zapobieganie przestępstwom terrorystycznym i innym poważnym przestępstwom oraz za ich wykrywanie i ściganie"), definicją tą mogłyby zostać objęte zarówno służby wywiadowcze, jak i organy ochrony porządku publicznego. Służby wywiadowcze mające wgląd do danych w VIS są zatem zasadniczo objęte takimi samymi obowiązkami dotyczącym ochrony danych, co niewątpliwie jest rozwiązaniem pozytywnym.

Zważywszy jednak na fakt, że mogą powstać pewne wątpliwości co do interpretacji kwestii stosowania decyzji ramowej do służb wywiadowczych, w przypadkach, w których mają one dostęp do danych zawartych w VIS, EIOD proponuje alternatywne sformułowanie o następującej treści:

„W przypadkach, w których decyzja ramowa (…) nie ma zastosowania, państwa członkowskie zapewniają poziom ochrony danych co najmniej równy poziomowi ochrony zapewnianemu przez decyzję ramową".

c) *Nadzór*

W odniesieniu do brzmienia art. 8 należałoby wyraźnie stwierdzić, że ust. 1 dotyczy przetwarzania danych na terytorium państw członkowskich. W ust. 2 i 3 jasno został określony ich zakres stosowania (przetwarzanie danych przez Europol i Komisję), w związku z czym należy wyraźnie stwierdzić, że ust. 1 dotyczy innej sytuacji.

Podział uprawnień związanych z nadzorem w zależności od odpowiednich działań różnych podmiotów stanowi właściwe rozwiązanie. Brakuje jednak jednego elementu: potrzeby skoordynowanego podejścia do nadzoru. Zgodnie z wcześniejszą opinią EIOD dotyczącą 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. W rzeczywistości istnieje potrzeba ujednoliconego wprowadzania w życie rozporządzenia oraz działania w kierunku wypracowania wspólnego podejścia do wspólnych problemów.

Art. 35 [wniosku w sprawie VIS] powinien zatem zawierać odpowiedni przepis stanowiący, że EIOD zwołuje przynajmniej raz do roku spotkanie wszystkich krajowych organów nadzorczych."

To samo rozwiązanie ma zastosowanie do omawianego wykorzystania systemu VIS (przy jednoczesnym zaangażowaniu w tym przypadku również wspólnego organu nadzorczego Europolu). Nadzór powinien być całkowicie spójny z nadzorem przewidzianym w „VIS w pierwszym filarze", ponieważ jest to ten sam system. Co więcej, zwoływane przez EIOD spotkania koordynacyjne, w których uczestniczą wszystkie strony biorące udział w nadzorze, stanowią rozwiązanie stosowane również w odniesieniu do nadzoru pozostałych systemów informacyjnych o dużym zasięgu, takich jak EURODAC.

EIOD jest świadom, że w ograniczonym zakresie koordynacja została przewidziana przez wniosek, w którym została zaakcentowana rola mającej powstać Grupy Roboczej ds. Ochrony Osób w zakresie Przetwarzania Danych Osobowych ustanowionej w art. 31 proponowanej decyzji ramowej. Jednakże należy powtórzyć, że zadania tego organu doradczego nie obejmują nadzoru jako takiego.

EIOD proponuje dodanie przepisu, zgodnie z którym zwoływane przez niego spotkania koordynujące w ramach nadzoru „VIS w pierwszym filarze" powinny również mieć uprawnienie w odniesieniu do danych przetwarzanych zgodnie z omawianym wnioskiem; w tym celu reprezentowany powinien być wspólny organ nadzorczy Europolu.

2.6. **Kontrola wewnętrzna**

Art. 12 wniosku przewiduje wprowadzenie systemów monitorujących funkcjonowanie VIS. W opinii EIOD takie monitorowanie nie powinno ograniczać się tylko do aspektów dotyczących wydajności, opłacalności i jakości usług, ale powinno również objąć ocenę zgodności z wymogami stawianymi przez prawo, zwłaszcza w dziedzinie ochrony danych. W związku z czym art. 12 należy odpowiednio zmienić.

Aby umożliwić przeprowadzanie kontroli wewnętrznych oceniających zgodność przetwarzania danych z prawem, Komisja powinna mieć możliwość korzystania z rejestrów prowadzonych zgodnie z art. 10 wniosku. Art. 10 powinien zatem przewidywać możliwość przechowywania tych rejestrów nie tylko do celów monitorowania ochrony danych i zapewniania ich bezpieczeństwa, ale również do celów przeprowadzania regularnych kontroli wewnętrznych VIS. Sprawozdania z kontroli wewnętrznych pomogą EIOD przy wykonywaniu jego zadań związanych z nadzorem, a innym organom nadzorującym ułatwią określenie najważniejszych obszarów, które mają zostać objęte nadzorem.

3. **WNIOSEK**

W świetle powyższych uwag EIOD podkreśla kluczowe znaczenie udzielenia dostępu do VIS organom odpowiedzialnym za bezpieczeństwo wewnętrzne i Europolowi wyłącznie przy zastosowaniu zasady indywidualnego rozpatrywania każdego przypadku i przestrzegając restrykcyjnych zabezpieczeń. Wniosek osiąga ten cel w stopniu ogólnie zadowalającym, chociaż można wprowadzić do niego pewne zmiany, zgodnie z propozycjami zawartymi w niniejszej opinii:

— Warunkiem dostępu do VIS zgodnie z art. 5 powinno być przyczynienie się tego dostępu „w znacznym stopniu" do zapobiegania poważnym przestępstwom, ich wykrywania lub ścigania, a rejestry o których mowa art. 10, powinny umożliwiać ocenę spełnienia tego warunku w każdym indywidualnie rozpatrywanym przypadku.

— Należy ponownie zastanowić się nad dwoma spośród wymienionych w art. 5 ust. 2 kryteriami dostępu do VIS, tj. „celem podróży" i „fotografiami" — powinny one być dostępne jako informacje dodatkowe w przypadku wcześniejszego uzyskania pozytywnego wyniku przy wyszukiwaniu.

— Poziom ochrony danych mający zastosowanie do sytuacji innych niż dostęp w celu wglądu powinien być taki sam, bez względu na to, jakie organy mają wgląd do VIS. Art. 8 i 10 powinien mieć zastosowanie również do państw członkowskich, do których rozporządzenie w sprawie VIS nie ma zastosowania.

— Należy zapewnić skoordynowane podejście do nadzoru, także w odniesieniu do dostępu do VIS przewidzianego w omawianym wniosku.

— Przepisy regulujące systemy monitorujące powinny również zapewniać wewnętrzną kontrolę zgodności z wymogami dotyczącymi ochrony danych.

Sporządzono w Brukseli, dnia 20 stycznia 2006 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych