

# EUROPEJSKI INSPEKTOR OCHRONY DANYCH

## Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności (COM (2005) 490 wersja ostateczna)

(2006/C 116/04)

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 wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (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,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

### I. UWAGI WSTĘPNE

1. Wniosek dotyczący decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności został skierowany do Europejskiego Inspektora Ochrony Danych (EIOD) za pośrednictwem pisma wysłanego przez Komisję w dniu 12 października 2005 r. EIOD przyjmuje, że pismo to stanowi prośbę o opinię dla instytucji i organów wspólnotowych, w myśl art. 28 ust. 2 rozporządzenia 45/2001/WE. EIOD uważa, że niniejsza opinia powinna zostać uwzględniona w preambule do decyzji ramowej.
2. Niniejsza opinia musi być rozpatrywana w kontekście opisanym w pkt II. Zgodnie z pkt II nie jest bynajmniej oczywiste, że omawiany wniosek — lub podejście do zasady dostępności w nim proponowane — w konsekwencji doprowadzi do przyjęcia aktu prawnego. Wiele państw członkowskich popiera inne podejścia.
3. Jest jednak oczywiste, że problem dostępności ponad granicami wewnętrznymi informacji służących organom ścigania lub, w szerszym kontekście, wymiana takich informacji, stanowi kwestię mającą duże znaczenie dla państw

członkowskich, zarówno na forum Rady, jak i poza nim, a także na forum Parlamentu Europejskiego.

4. Podobnie oczywistym jest, że temat ten ma szczególne znaczenie z punktu widzenia ochrony danych osobowych, co zostanie odzwierciedlone w niniejszej opinii. EIOD przypomina, że omawiany wniosek został przedstawiony przez Komisję w związku z wnioskiem dotyczącym decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych — w sprawie tego drugiego wniosku EIOD przedstawił opinię w dniu 19 grudnia 2005 r.
5. EIOD, korzystając z nadarzającej się okazji, przedstawi w niniejszej opinii podstawowe założenia o charakterze ogólnym dotyczące wymiany informacji służących organom ścigania oraz różnorodnych podejść do uregulowania tego tematu. EIOD ma nadzieję, że przedstawienie niniejszej opinii zapewni uwzględnienie w należyтым stopniu problematyki ochrony danych w przyszłych dyskusjach na ten temat.
6. Na późniejszym etapie prac będzie można zgłaszać do EIOD kolejne wnioski o wydanie opinii w zależności od postępów poczynionych w kolejnych stadiach procesu legislacyjnego obejmującego zarówno omawiany wniosek, jak i inne wnioski z nim powiązane.

### II. KONTEKST WNIOSKU

7. Zasada dostępności — jako nowa, mająca duże znaczenie zasada prawa — została po raz pierwszy wprowadzona w programie haskim. Zakłada ona, że przepływ ponad granicami wewnętrznymi UE informacji potrzebnych do walki z przestępczością powinien odbywać się bez utrudnień. Celem niniejszego wniosku jest wprowadzenie tej zasady do wiążącego aktu prawnego.
8. Wymiana pomiędzy różnymi państwami informacji potrzebnych policji stanowi często przedmiot zainteresowania ustawodawców, zarówno w ramach UE, jak i poza nią. Uwagę EIOD w ostatnim czasie zwróciły następujące inicjatywy.

9. Przede wszystkim, w dniu 4 czerwca 2004 r. Szwecja przedstawiła projekt decyzji ramowej w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej. Podczas posiedzenia w dniu 1 grudnia 2005 r. Rada osiągnęła porozumienie w sprawie podejścia ogólnego do tego wniosku.
10. Po drugie, w dniu 27 maja 2005 r. siedem państw członkowskich podpisało w Prüm (Niemcy) konwencję w sprawie rozszerzenia współpracy transgranicznej, szczególnie w zakresie zwalczania terroryzmu, przestępczości transgranicznej i nielegalnej migracji. Konwencja ta wprowadza między innymi rozwiązania służące usprawnieniu wymiany informacji na temat DNA i odcisków palców. Do konwencji może przystąpić każde z państw członkowskich Unii Europejskiej. Umawiające się strony postawiły sobie za cel włączenie przepisów konwencji do ram prawnych Unii Europejskiej.
11. Po trzecie, dostępność — ponad granicami wewnętrznymi Unii Europejskiej — informacji służących organom ścigania będzie nadal zwiększana dzięki innym aktom prawnym, takim jak wnioski dotyczące Systemu Informacyjnego Schengen drugiej generacji (SIS II), wniosek dotyczący dostępu do Systemu Informacji Wizowej (VIS) oraz wniosek dotyczący decyzji w sprawie organizacji wymiany informacji pochodzących z rejestrów karnych pomiędzy państwami członkowskimi oraz treści tych informacji. W tym kontekście właściwe wydaje się również przypomnienie komunikatu wydanego przez Komisję w dniu 25 listopada 2005 r. w sprawie poprawy skuteczności, sprawniejszej operacyjności i współdziałania europejskich baz danych w obszarze sprawiedliwości i spraw wewnętrznych.
12. Biorąc pod uwagę wszystkie podjęte inicjatywy wspomniane powyżej, należy stwierdzić, że omawiany wniosek dotyczący decyzji ramowej w sprawie dostępności nie powinien być analizowany w oderwaniu od proponowanych rozwiązań — trzeba również uwzględnić inne podejścia do kwestii wymiany informacji służących organom ścigania. Jest to szczególnie istotne ze względu na obecną tendencję widoczną na forum Rady, zgodnie z którą większym poparciem cieszą się podejścia do problematyki wymiany informacji i do pojęcia dostępności odbiegające od podejścia ogólnego zaproponowanego przez Komisję w omawianym wniosku. Tekst wniosku w obecnym brzmieniu może nawet nie zostać poddany pod dyskusję na forum Rady.
13. Ponadto omawiany wniosek jest ściśle powiązany z wnioskiem dotyczącym decyzji ramowej w sprawie ochrony danych osobowych. Niniejsza opinia musi być interpretowana w świetle bardziej szczegółowej opinii w sprawie tej decyzji ramowej.
14. W opinii na temat wniosku dotyczącego decyzji ramowej w sprawie ochrony danych osobowych, EIOD podkreślił znaczenie zapewnienia właściwej ochrony danych, koniecznej w przypadku przyjęcia aktu prawnego dotyczącego dostępności. Według EIOD taki akt prawny nie powinien zostać przyjęty bez uprzedniego zapewnienia podstawowych zabezpieczeń w zakresie ochrony danych.
15. Takie samo stanowisko EIOD zajmuje w odniesieniu do przyjęcia innych aktów prawnych, które miałyby ułatwić przepływ przez granice wewnętrzne UE informacji służących organom ścigania. EIOD przyjmuje zatem z zadowoleniem fakt, że zarówno Rada, jak i Parlament Europejski nadały priorytetowe znaczenie wspomnianemu wcześniej wnioskowi dotyczącemu decyzji ramowej w sprawie ochrony danych osobowych.

### III. ZASADA DOSTĘPNOŚCI

16. Zasada dostępności jako taka jest zasadą prostą. Informacje dostępne dla niektórych organów w jednym państwie członkowskim muszą być również dostępne dla równoważnych organów w pozostałych państwach członkowskich. Wymiana informacji między organami państw członkowskich musi być dokonywana w możliwie najszybszy i najprostszy sposób, najlepiej przy wykorzystaniu bezpośredniego dostępu przez Internet.
17. Trudności pojawiają się w związku z warunkami, w jakich zasada dostępności ma znaleźć zastosowanie:
- Niejednolita organizacja organów policyjnych i sądowych w państwach członkowskich, stosujących różniące się między sobą systemy kontroli i równowagi.
  - Różnego rodzaju (wrażliwe) informacje (takie jak DNA lub odciski palców).
  - Różne sposoby dostępu do stosownych informacji przewidziane dla właściwych organów nawet w obrębie poszczególnych państw członkowskich.
  - Ze względu na różnice językowe, różnice w systemach technologicznych (interoperacyjność) i w systemach prawnych trudno jest zapewnić właściwą interpretację informacji pochodzących z innego państwa członkowskiego.
  - Zasada ta musi być włączona do zarówno już istniejących, jak i dopiero tworzonych systemów przepisów prawnych, które dotyczą wymiany między państwami informacji służących organom ścigania.
18. Niezależnie od tak złożonej sytuacji, oczywistym jest, że zasada ta nie może działać w oderwaniu od innych instrumentów. Koniecznym jest przedsięwzięcie dodatkowych środków, które zagwarantują skuteczne wyszukiwanie informacji i skuteczny do nich dostęp. W każdym razie środki te muszą ułatwiać organom ścigania zdobycie wiedzy na temat posiadania potrzebnych informacji przez organy ścigania innych państw członkowskich oraz informacji na temat miejsca, w którym takie informacje można uzyskać. Takie dodatkowe środki mogłyby obejmować interfejsy umożliwiające bezpośredni dostęp do wszystkich lub poszczególnych danych posiadanych przez inne państwa członkowskie. Z tego powodu wniosek dotyczący decyzji ramowej w sprawie dostępności wprowadza „odnośniki”, czyli konkretne dane, do których można mieć bezpośredni dostęp ponad granicami.

19. Ogólnie rzecz ujmując zasada dostępności powinna ułatwić przepływ informacji między państwami członkowskimi. W związku z faktem, że granice wewnętrzne zostaną zniesione, państwa członkowskie muszą zezwolić, aby informacje dostępne dla ich organów policyjnych stopniowo były udostępniane również organom z innych państw członkowskich. Państwa członkowskie tracą uprawnienia do kontrolowania przepływu informacji, co oznacza również, że nie mogą już traktować własnego ustawodawstwa krajowego jako wystarczającego instrumentu odpowiedniej ochrony informacji.
20. Z tego właśnie powodu wniosek wymaga szczególnej uwagi z punktu widzenia ochrony danych osobowych. Po pierwsze, informacje, które zazwyczaj mają charakter poufny i które są dobrze zabezpieczone, muszą zostać udostępnione organom innych państw członkowskich. Po drugie, aby zapewnić funkcjonowanie systemu, należy utworzyć odnośniki i udostępnić je organom innych państw członkowskich. Zastosowanie tej zasady będzie w konsekwencji prowadziło do tworzenia większej liczby danych w porównaniu do danych obecnie dostępnych.
23. Wniosek nie precyzuje, czy określenie „dostępne informacje” dotyczy wyłącznie informacji już kontrolowanych przez właściwe organy, czy też obejmują one również te informacje, które mogą dopiero zostać przez te organy uzyskane. Zdaniem EIOD wniosek można jednak interpretować jako zawierający obydwa rozwiązania.
24. W rzeczy samej, podczas gdy art. 2 ust. 2 wydaje się sugerować — poprzez określenie, że decyzja ramowa „nie pociąga za sobą obowiązku gromadzenia i przechowywania informacji [...] w wyłącznym celu udostępniania ich” — wąski zakres zastosowania, art. 3 lit. a) pozwala na szerszą interpretację, stwierdzając, że „informacje” oznaczają „istniejące informacje, wymienione w załączniku II”.
25. Załącznik II wymienia co najmniej dwie kategorie danych, które w większości przypadków kontrolowane są przez organy inne niż policja. Do pierwszej kategorii należą dane rejestracyjne pojazdów. W wielu państwach członkowskich bazy danych zawierające takie dane nie są kontrolowane przez organy ścigania, chociaż są im regularnie udostępniane. Czy dane tego rodzaju powinny być objęte zakresem pojęcia „dostępnych informacji”, które, zgodnie z art. 1, są udostępniane równoważnym właściwym organom innych państw członkowskich? Druga kategoria danych wymienionych w załączniku II, którą należy wskazać, to numery telefoniczne i inne dane dotyczące połączeń: czy takie dane powinny być uważane za „dostępne” także w sytuacjach, w których są one kontrolowane przez prywatne firmy, a nie przez właściwe władze?

#### IV. GŁÓWNE ELEMENTY

##### Zakres zastosowania zasady dostępności

21. Przede wszystkim należy określić, do jakich informacji zasada dostępności będzie miała zastosowanie. Dziedzina, do której odnosi się ta zasada określona została w sposób ogólny w art. 2 wniosku, w powiązaniu z art. 1 ust. 1 i art. 3 lit. a). Zasada stosuje się do informacji:
- istniejących;
  - wymienionych w załączniku II, który definiuje sześć rodzajów informacji;
  - dostępnych właściwym organom.
- Są to trzy podstawowe elementy wyznaczające we wniosku Komisji zakres zastosowania omawianej zasady. Zakres ten zostaje dokładniej określony w art. 2. Art. 2 ust. 1 ogranicza stosowanie zasady dostępności do etapu poprzedzającego rozpoczęcie postępowania karnego, natomiast ust. 2, 3 i 4 tego samego artykułu wprowadzają ograniczenia bardziej szczegółowe.
22. Aby zrozumieć konsekwencje, jakie pociąga za sobą wniosek, konieczne jest przeprowadzenie dokładniejszej analizy trzech podstawowych, wyżej wspomnianych, elementów. Pierwsze dwa elementy określające zakres są wystarczająco jasne. Definicja „istniejących informacji” jest zawarta w art. 2 ust. 2, który mówi, że decyzja ramowa nie pociąga za sobą obowiązku gromadzenia i przechowywania informacji w wyłącznym celu udostępniania ich, natomiast interpretacja wykazu zamieszczonego w załączniku II nie budzi wątpliwości. Dalszych wyjaśnień wymaga natomiast trzeci z podstawowych elementów, zarówno sam, jak i w powiązaniu z dwoma pierwszymi elementami.
26. Ponadto w innych przepisach wniosku, w szczególności w art. 3 lit. d) i art. 4 ust. 1 lit. c), wspierany jest pogląd, zgodnie z którym „wyznaczone organy”, a nawet „wyznaczone strony” mogą kontrolować informacje, które są „dostępne” dla „właściwych organów”. Z tekstu wniosku wynika również, że „właściwy organ” państwa członkowskiego oznacza organ objęty art. 29, tiret pierwsze traktatu UE, podczas gdy każdy organ krajowy może być „organem wyznaczonym”.
27. Według EIOD zastosowanie zasady dostępności do informacji kontrolowanych przez wyznaczone organy i wyznaczone strony budzi następujące wątpliwości:
- Czy art. 30 ust. 1 lit. b) stanowi wystarczającą podstawę prawną, zważywszy, że informacje muszą być udostępniane przez wyznaczone organy i wyznaczone strony, a ponadto, że pochodzą z baz danych nie objętych trzecim filarem?
  - Czy decyzja ramowa w sprawie ochrony danych osobowych będzie miała zastosowanie, tak jak to zakłada np. art. 8 wniosku?
  - Jeżeli nie, czy przetwarzanie danych jest zgodne z obowiązkami ustanowionymi w dyrektywie 95/46/WE?

28. Zastosowanie zasady o zakresie tak szerokim jak „zasada dostępności” wymaga jasnego i precyzyjnego zdefiniowania danych, które powinny być uważane za dostępne. Wobec powyższego EIOD zaleca:

- Sprecyzowanie zakresu zastosowania.
- Pierwsza możliwość: ograniczenie zakresu zastosowania zasady dostępności do informacji kontrolowanych przez właściwe organy.
- Druga możliwość: w przypadku szerszego zakresu zastosowania, wprowadzenie wystarczających zabezpieczeń w celu ochrony danych osobowych. Należy uwzględnić kwestie poruszone w znajdującym się powyżej pkt 27.

#### **Pozostałe kwestie związane z zakresem zastosowania**

29. Zgodnie z art. 2 ust. 1 wniosku decyzja ramowa ma zastosowanie do przetwarzania informacji poprzedzającego rozpoczęcie postępowania karnego. Jej zakres zastosowania jest bardziej ograniczony niż zakres wniosku dotyczącego decyzji ramowej w sprawie ochrony danych osobowych, który w całości odnosi się do współpracy sądowej w sprawach karnych.

30. Jednak zdaniem EIOD ograniczenie takie samo w sobie nie zawęża zakresu zastosowania wniosku do współpracy policyjnej. Zakresem tym mogłaby również zostać objęta współpraca sądowa w sprawach karnych, zważywszy że w niektórych państwach członkowskich organy sądowe mają również uprawnienia w odniesieniu do dochodzeń lub śledztw prowadzonych w sprawach karnych, jeszcze przed rozpoczęciem postępowania sądowego. Niemniej jednak fakt, że podstawę wniosku stanowi wyłącznie art. 30 ust. 1 lit. b) TUE wydaje się wskazywać, że wniosek ten ma zastosowanie tylko do współpracy policyjnej. Wyjaśnienie tego aspektu zostało przyjęte z zadowoleniem.

31. Omawiany wniosek ma zastosowanie do udostępniania informacji Europolowi, podczas gdy wniosek dotyczący decyzji ramowej w sprawie ochrony danych osobowych wyłącza możliwość przetwarzania danych osobowych przez Europol. EIOD doradza ograniczenie wymiany informacji z Europolem do celów, zgodnie z którymi działa ta organizacja, wymienionych w art. 2 konwencji o Europolu i w załączniku do niej. Ponadto należy uwzględnić szczególne zasady wymiany danych z Europolem zawarte w niektórych aktach Rady.

#### **Nie dla nowych baz danych zawierających dane osobowe**

32. Punktem wyjścia wniosku jest stwierdzenie, że nie będzie on prowadził do tworzenia nowych baz danych zawierających dane osobowe. Wyraźnie zostaje to stwierdzone w art. 2 ust. 2: wniosek nie pociąga za sobą obowiązku

gromadzenia i przechowywania informacji w wyłącznym celu udostępniania ich. Z punktu widzenia ochrony danych jest to istotny, a zarazem pozytywny element wniosku. EIOD przypomina swoją opinię na temat wniosku dotyczącego dyrektywy w sprawie zatrzymywania danych przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej<sup>(1)</sup>, w której podkreślił, że obowiązki prawne prowadzące do powstania dużych baz danych skutkują powstaniem szczególnego ryzyka dla osoby, której dane dotyczą, między innymi ze względu na ryzyko związane z nieuprawnionym wykorzystaniem danych.

33. Jednakże:

- Należy zagwarantować, że wniosek nie będzie przyczyniał się do tworzenia nieograniczonych wzajemnych połączeń między bazami danych, a tym samym do tworzenia trudnej do nadzorowania sieci baz danych.

- Od zasady stanowiącej wspomniany powyżej punkt wyjścia istnieje pewien wyjątek: jest to art. 10 wniosku zapewniający dostępność odnośników przez Internet. Odnośniki mogą zawierać dane osobowe lub przynajmniej informować o istnieniu takich danych.

#### **Bezpośredni i pośredni dostęp do informacji**

34. Wniosek przewiduje bezpośredni i pośredni dostęp do informacji. Art. 9 wniosku przewiduje bezpośredni dostęp przez Internet do informacji znajdujących się w bazach danych, do których równoważne właściwe organy krajowe mają bezpośredni dostęp przez Internet. Art. 10 przewiduje dostęp pośredni. Odnośniki do informacji niedostępnych przez Internet są dostępne w drodze konsultacji przez Internet dla równoważnych właściwych organów innych państw członkowskich i Europolu. Jeżeli organ ten znajdzie odnośnik do poszukiwanych informacji, może on sporządzić wniosek o udzielenie informacji i przesłać go wyznaczonemu organowi w celu uzyskania informacji, których odnośnik dotyczy.

35. Dostęp bezpośredni nie prowadzi do utworzenia nowych baz danych, ale wymaga interoperacyjności baz danych równoważnych właściwych systemów w państwach członkowskich. Ponadto konieczne będzie wprowadzenie nowego sposobu wykorzystania już istniejących baz danych poprzez zapewnienie wszystkim właściwym organom państw członkowskich narzędzi, które dotychczas były dostępne wyłącznie dla właściwych organów krajowych. Dostęp bezpośredni automatycznie oznaczać będzie dostęp większej liczby osób do bazy danych i tym samym prowadzić może do zwiększenia ryzyka związanego z niewłaściwym wykorzystaniem danych.

<sup>(1)</sup> Opinia z dnia 26 września 2005 r. na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zatrzymywania danych przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej zmieniającej dyrektywę 2002/58/WE (COM (2005) 438 wersja ostateczna).

36. W przypadku bezpośredniego dostępu właściwego organu innego państwa członkowskiego, wyznaczone organy państwa członkowskiego udostępniającego dane nie mają żadnej kontroli nad dostępem ani nad dalszym wykorzystaniem danych. Na takie konsekwencje dostępu bezpośredniego przewidzianego w treści wniosku należy zwrócić szczególną uwagę, zważywszy że:

- Wydaje się, że naruszają one uprawnienia wyznaczonych organów do odmowy udzielenia informacji (przewidziane w art. 14).
- Zmuszają one do postawienia pytania o ponoszenie odpowiedzialności za dokładność i aktualizowanie danych po uzyskaniu do nich dostępu. W jaki sposób wyznaczony organ państwa członkowskiego udostępniającego dane może zagwarantować aktualizację danych?
- Nie tylko wyznaczony organ nie jest w stanie dłużej wypełniać wszystkich swoich obowiązków wynikających z przepisów dotyczących ochrony danych, ale również krajowy organ ochrony danych państwa członkowskiego udostępniającego dane nie może dłużej sprawować nadzoru nad wypełnianiem takich obowiązków, ponieważ nie posiada on żadnych uprawnień w odniesieniu do organów ścigania innych państw członkowskich.
- Kwestie te nabierają jeszcze większego znaczenia w przypadku dostępu do baz danych przez wyznaczone organy i wyznaczone strony niebędące organami ścigania (patrz pkt 25-28 niniejszej opinii).

Opisane skutki dostępu bezpośredniego stanowią istotną przyczynę, dla której przyjęcie omawianego wniosku powinno zostać uzależnione od przyjęcia decyzji ramowej w sprawie ochrony danych osobowych. Jeden problem pozostaje nierozstrzygnięty: trudno jest wyobrazić sobie, w jaki sposób wyznaczone organy mogłyby odmówić udzielenia informacji na mocy art. 14.

37. W odniesieniu do dostępu pośredniego poprzez odnośniki, które dostarczają informacji zgodnie z systemem trafienia/brak trafienia: nie jest to nowe rozwiązanie. Stanowi ono podstawę funkcjonowania europejskich systemów informacyjnych o dużym zasięgu, takich jak system informacyjny Schengen. Korzyścią utworzenia systemu odnośników jest umożliwienie państwom członkowskim udostępniającym dane sprawowania kontroli nad wymianą informacji pochodzących z ich kartotek policyjnych. Jeżeli zostanie znaleziony odnośnik do poszukiwanej informacji, organ wnioskujący może złożyć wniosek o udzielenie informacji na temat osoby, której dane dotyczą. Wniosek ten może zostać rozpatrzony w sposób właściwy przez organ, do którego został skierowany.

38. Niemniej jednak konieczna jest również dokładna analiza, zważywszy że utworzenie systemu odnośników — w dziedzinach, w których systemy takie dotychczas nie istniały, innych niż europejskie systemy informacyjne o dużym zasięgu — może skutkować powstaniem nowego ryzyka

dla osoby, której dane dotyczą. EIOD podkreśla fakt, że chociaż odnośniki same w sobie nie zawierają dużo informacji na temat osób, których dane dotyczą, to znalezienie potrzebnego odnośnika może prowadzić do danych szczególnie wrażliwych. Odnośnik może ujawniać, że dana osoba jest notowana w kartotekach policyjnych w związku z popełnieniem przestępstwa.

39. Kwestią najwyższej wagi staje się zatem ustanowienie przez europejskiego prawodawcę odpowiednich przepisów, przynajmniej w odniesieniu do tworzenia odnośników, dotyczących zarządzania systemami przechowywania odnośników oraz właściwej organizacji dostępu do odnośników. W opinii EIOD wniosek pod tym względem nie jest zadowalający. Na obecnym etapie prac EIOD zgłasza trzy uwagi:

- Definicja odnośników jest niejasna. Brak wyraźnego wskazania, czy odnośniki są postrzegane jako meta-dane, dane podstawowe, czy może zarówno jako jedno i drugie. Należy wyjaśnić pojęcie odnośników, jako że ma ono bezpośredni wpływ na poziom ochrony danych i wymaganych zabezpieczeń.
- We wniosku powinna zostać dokładniej określona rola krajowych punktów kontaktowych w zakresie odnośników. Udział krajowych punktów kontaktowych może okazać się konieczny, zwłaszcza w przypadkach, w których interpretacja odnośników wymaga wiedzy specjalistycznej, na przykład w przypadku ewentualnego dopasowywania odcisków palców.
- Wniosek pozostawia przyjęcie przepisów koniecznych do utworzenia odnośników przepisom wykonawczym zgodnie z procedurą komitologii przewidzianą w art. 19. Chociaż przepisy wykonawcze mogą być potrzebne, to podstawowe przepisy dotyczące utworzenia odnośników powinny być zawarte w samej decyzji ramowej.

#### **Wcześniejsze zezwolenie udzielane przez organy sądowe**

40. Wymiana informacji nie powinna uniemożliwiać państwu członkowskim, w których konieczne jest wcześniejsze uzyskanie zezwolenia organów sądowych, przekazywania informacji organowi wnioskującemu, jeżeli dane informacje objęte są w państwie, do którego skierowano wniosek, kontrolą sądową. Jest to istotna uwaga, zważywszy że, jak wynika z przeprowadzonego badania na temat uprawnień policji w zakresie wymiany danych osobowych<sup>(1)</sup>, nie we wszystkich państwach członkowskich policja może mieć niezależny dostęp do tych danych. W opinii EIOD zasada dostępności nie powinna naruszać wynikającego z prawa krajowego obowiązku uzyskania wcześniejszego zezwolenia w celu uzyskania informacji lub przynajmniej powinna doprowadzić do ustanowienia przepisów szczególnych określających kategorie danych, dla których konieczne jest uzyskanie takiego zezwolenia, które to przepisy miałyby zastosowanie we wszystkich państwach członkowskich.

<sup>(1)</sup> Odpowiedź na kwestionariusz dotyczący decyzji ramowej w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania Państw Członkowskich UE, w szczególności w odniesieniu do poważnych przestępstw, w tym aktów terroryzmu (dokument Rady nr 5815/1/05).

41. Obowiązek ten powinien być interpretowany w powiązaniu z art. 11 ust. 2 wniosku dotyczącego decyzji ramowej w sprawie ochrony danych osobowych, który przewiduje również wpływ państw członkowskich przekazujących informacje na dalsze wykorzystanie tych informacji w państwie członkowskim, do którego dane zostały przekazane. EIOD odnotowuje znaczenie tej zasady, która jest potrzebna do zagwarantowania, że dostępność nie będzie prowadziła do obchodzenia restrykcyjnych przepisów krajowych dotyczących dalszego wykorzystania danych osobowych.

#### Uwaga końcowa

42. Omówione elementy wymagają zastosowania wysokich standardów ochrony danych. Szczególną uwagę należy zwrócić na zagwarantowanie stosowania zasady ograniczenia celu i zasady związanej z dalszym przetwarzaniem, jak również na dokładność i wiarygodność informacji, które są udostępniane (patrz opinia EIOD na temat decyzji ramowej w sprawie ochrony danych osobowych, pkt IV.2 i IV.6).

### V. INNE PODEJŚCIA

#### Wniosek Szwecji

43. Wniosek Szwecji nie ogranicza się do określonych rodzajów informacji, ale obejmuje wszystkie informacje wraz z danymi wywiadowczymi, nawet informacje i dane wywiadowcze przechowywane przez inne podmioty niż właściwe organy ścigania. Wniosek ten zacieśnia współpracę poprzez ustanowienie ograniczeń czasowych w odniesieniu do rozpatrywania wniosków o udzielenie informacji oraz poprzez zniesienie zróżnicowanego podejścia do kwestii wymiany informacji w ramach jednego państwa członkowskiego i ponadgranicznej wymiany informacji. Nie przewiduje on dodatkowych środków zapewniających skuteczny dostęp do informacji. W tym świetle zrozumią stają się przyczyny, dla których Komisja nie była usatysfakcjonowana wnioskiem Szwecji jako właściwym instrumentem zapewniającym dostępność<sup>(1)</sup>.

44. Z punktu widzenia ochrony danych podejście zaprezentowane we wniosku Szwecji ma następujące konsekwencje natury ogólnej:

— Z zadowoleniem zostaje odnotowany fakt, że wniosek został ściśle ograniczony do przetwarzania istniejących danych i nie prowadzi do tworzenia nowych baz danych — nie przewiduje nawet tworzenia „odnośników”.

— Brak „odnośników” jednakże nie stanowi z definicji pozytywnego elementu. Odnośniki, o ile zostaną odpowiednio zabezpieczone, mogą ułatwić ukierunkowane, a tym samym mniej inwazyjne wyszukiwanie danych o wrażliwym charakterze. Mogą również ułatwić sprawne rozpatrywanie wniosków i zapewnić skuteczniejszy nadzór.

— W każdym razie wniosek prowadzi do zwiększenia ponadgranicznej wymiany danych osobowych pociągającego za sobą ryzyko niewystarczającej ochrony danych osobowych, między innymi ze względu na fakt,

że narusza uprawnienia państw członkowskich do pełnego kontrolowania podmiotów dokonujących wymiany danych. Wniosek ten nie powinien zostać przyjęty, jeżeli nie zostanie przyjęta decyzja ramowa w sprawie ochrony danych osobowych.

#### Konwencja z Prüm

45. W konwencji z Prüm zostało przyjęte inne podejście do kwestii stosowania zasady dostępności. W omawianym wniosku dotyczącym decyzji ramowej zostało zawarte podejście ogólne — mające zastosowanie do wszystkich rodzajów informacji, o ile są one wymienione w załączniku II (patrz pkt 21-28 niniejszej opinii), a nie zakładające ustanowienia przepisów szczególnych dotyczących wymiany poszczególnych rodzajów informacji — natomiast podejście przedstawione w konwencji z Prüm jest podejściem stopniowym.

46. Podejście takie nazywane jest czasami podejściem zakładającym dostęp do danych w układzie tematycznym („*data field-by-data field approach*”). Ma ono zastosowanie do poszczególnych rodzajów informacji (DNA, odciski palców i dane rejestracyjne pojazdów) i ustanawia obowiązek uwzględniania szczególnego charakteru takich danych. Konwencja ustanawia obowiązek zakładania i prowadzenia — do celów śledztw lub dochodzeń prowadzonych w sprawach karnych — kartotek analiz DNA. Podobny obowiązek odnosi się do danych dotyczących odcisków palców. W odniesieniu do danych rejestracyjnych pojazdów, należy zapewnić dostęp bezpośredni do krajowych punktów kontaktowych znajdujących się w innych państwach członkowskich.

47. Podejście prezentowane w konwencji z Prüm skłania do zgłoszenia trzech rodzajów uwag.

48. Po pierwsze, jest oczywiste, że EIOD nie zatwierdza procedury prowadzącej do stosowania omawianej konwencji z pominięciem ram instytucjonalnych Unii Europejskiej, a co za tym idzie, bez poważnego zaangażowania Komisji w tę procedurę. Ponadto, procedura ta oznacza brak demokratycznej kontroli sprawowanej przez Parlament Europejski, jak również brak kontroli sądowej sprawowanej przez Trybunał Sprawiedliwości, co w rezultacie prowadzi do zmniejszenia gwarancji prawidłowego wyważenia wszelkich interesów (publicznych). Obejmuje to również podejście do zagadnienia z punktu widzenia ochrony danych. Innymi słowy instytucje Unii Europejskiej nie mają możliwości — przed utworzeniem systemu — oceny konsekwencji, jakie wybór określonej strategii może mieć na ochronę danych osobowych.

49. Po drugie, w sposób oczywisty niektóre elementy konwencji z Prüm w większym stopniu naruszają prywatność osoby, której dane dotyczą, niż czyni to treść decyzji ramowej w sprawie dostępności. Konwencja z założenia prowadzi do utworzenia nowych baz danych, które same w sobie zwiększają ryzyko niewystarczającej ochrony danych osobowych. Należy wykazać konieczność i adekwatność utworzenia takich nowych baz danych. Należy zagwarantować właściwe zabezpieczenia służące ochronie danych osobowych.

<sup>(1)</sup> Patrz dokument roboczy służb Komisji: załącznik do wniosku dotyczącego decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności, SEC 2005 (1270) z 12.10.2005 r.

### Podejście zakładające dostęp do danych w układzie tematycznym („data field-by-data field approach”)

50. Po trzecie, jak już stwierdzono wcześniej, konwencja przyjmuje podejście zakładające dostęp do danych w układzie tematycznym („data field-by-data field approach”). EIOD wspominał powyżej problemy i wątpliwości związane z warunkami, w jakich zasada proporcjonalności ma znaleźć zastosowanie. W takich okolicznościach zdaniem EIOD, lepszym rozwiązaniem byłoby — zamiast tworzenia systemu dla różnych rodzajów danych — zastosowanie bardziej ostrożnego podejścia, zakładającego objęcie systemem jednego rodzaju danych oraz kontrolowanie, w jakim stopniu zasada dostępności może rzeczywiście pomóc w ściganiu przestępstw, przy równoczesnej kontroli konkretnych zagrożeń mogących pojawić się w odniesieniu do ochrony danych osobowych. Na podstawie takich doświadczeń systemem prawdopodobnie mogłyby zostać objęte inne rodzaje danych, jak również mógłby on zostać zmodyfikowany w celu zwiększenia jego skuteczności.
51. Podejście zakładające dostęp do danych w układzie tematycznym w większym stopniu spełniłoby również wymogi wynikające z zasady proporcjonalności. W opinii EIOD, potrzeba sprawniejszej ponadgranicznej wymiany danych służącej ściganiu przestępstw mogłaby uzasadnić przyjęcie aktu prawnego na szczeblu europejskim, ale w celu zachowania zasady proporcjonalności akt ten powinien być dostosowany do założonych w nim celów, które będzie można dokładniej określić dopiero po zdobyciu praktycznych doświadczeń. Co więcej, omawiany akt prawny nie powinien w sposób nieproporcjonalny naruszać prywatności osoby, której dane dotyczą. Wymiana danych nie powinna dotyczyć większej liczby rodzajów danych niż jest to bezwzględnie konieczne, ani możliwości anonimowej wymiany danych, oraz powinna odbywać się zgodnie z restrykcyjnymi warunkami regulującymi ochronę danych.
52. Ponadto, popierane przez EIOD bardziej wyważone podejście mogłoby obejmować — jeżeli jest to możliwe wraz z podejściem zakładającym dostęp do danych w układzie tematycznym — rozpoczęcie wprowadzania w życie zasady dostępności wyłącznie przy wykorzystaniu dostępu pośredniego, czyli poprzez odnośniki. EIOD poruszył tę kwestię w celu poddania jej pod rozwagę na dalszych etapach procesu legislacyjnego.

### VI. KTÓRE DANE?

53. Załącznik II wymienia rodzaje informacji, jakie można uzyskać na mocy proponowanej decyzji ramowej. Wszystkie sześć rodzajów informacji wymienionych w tym załączniku w większości przypadków stanowi dane osobowe ze względu na fakt, że wszystkie dotyczą osoby zidentyfikowanej lub możliwej do zidentyfikowania.
54. Zgodnie z art. 3 lit. g) wniosku termin „odnośniki” oznacza „dane, których celem jest określenie informacji w jednoznaczny sposób i które można przeszukiwać za pomocą

zwykłej funkcji szukania, aby ustalić, czy dane informacje są dostępne”. W dokumencie zatytułowanym „Sposób wdrażania zasady dostępności”<sup>(1)</sup> za odnośniki uznane zostały następujące dane:

- tożsamość danych osób;
- numery identyfikacyjne danych przedmiotów (pojazdów/dokumentów);
- odciski palców/fotografie cyfrowe.

Innym rodzajem danych, który mógłby zostać uznany za odnośniki, mogą być profile DNA. Powyższy wykaz odnośników wskazuje, że odnośniki mogą zawierać dane osobowe i w związku z tym konieczne jest zapewnienie ich właściwej ochrony.

55. EIOD w szczególności zajmuje kwestia profili DNA. Zostało udowodnione, że analizy DNA mają istotne znaczenie w prowadzeniu dochodzenia lub śledztwa w sprawach karnych, a sprawna wymiana danych DNA może mieć podstawowe znaczenie w walce z przestępczością. Niemniej jednak konieczne jest jasne zdefiniowanie samego pojęcia „dane DNA”, jak również odpowiednie uwzględnienie szczególnego charakteru tych danych. W rzeczy samej z punktu widzenia ochrony danych istnieje zasadnicza różnica między próbkami DNA a profilami DNA.
56. Próbkę DNA (często zbierane i przechowywane przez organy ścigania) należy traktować jako dane szczególnie wrażliwe, ponieważ istnieje zwiększone prawdopodobieństwo, że mogą one zawierać cały „obraz” DNA. Mogą one dostarczać informacji o cechach genetycznych i stanie zdrowia danej osoby, które mogą być potrzebne do zupełnie innych celów, takich jak udzielanie porad medycznych poszczególnym osobom lub młodym parom.
57. W przypadku profili DNA mamy do czynienia z sytuacją odwrotną, ponieważ profile takie zawierają tylko niektóre informacje na temat DNA pobrane z próbki DNA: mogą być one wykorzystywane do sprawdzania tożsamości danej osoby, ale zasadniczo nie ujawniają jej cech genetycznych. Tym niemniej postęp naukowy może doprowadzić do zwiększenia liczby informacji, które można odczytać z profili DNA: to, co w danym momencie może być postrzegane jako „niewinny” profil DNA, wraz z upływem czasu może ujawnić znacznie więcej informacji, niż było to oczekiwane i potrzebne, w tym zwłaszcza informacji dotyczących cech genetycznych danej osoby. Tym samym informacje, które można odczytać z profili DNA powinny być uważane za informacje o charakterze dynamicznym.
58. W tym kontekście EIOD zauważa, że chociaż zarówno konwencja z Prüm, jak i wniosek Komisji wspierają wymianę danych DNA między organami ścigania, to istnieją zasadnicze różnice w proponowanym sposobie dokonywania takiej wymiany.

<sup>(1)</sup> Dokument prezydencji z dnia 5 kwietnia 2005 r. skierowany do Rady (nr dok.: 7641/05).

59. EIOD z zadowoleniem przyjmuje fakt, że we wniosku Komisji nie został przewidziany obowiązek gromadzenia danych DNA oraz że wymiana danych DNA w wyraźny sposób została ograniczona do profili DNA. Załącznik II definiuje profile DNA na podstawie wspólnego wykazu wskaźników DNA używanego w ekspertyzach sądowych DNA przeprowadzanych w państwach członkowskich. Wykaz ten — ustalony na podstawie siedmiu wskaźników DNA Europejskiego Zestawu Standardowego określonego w załączniku do rezolucji Rady z dnia 25 czerwca 2001 r. w sprawie wymiany wyników analizy DNA <sup>(1)</sup> — gwarantuje, że profile DNA nie będą zawierać, w momencie ich pobierania, żadnych informacji na temat szczególnych cech dziedzicznych.
60. EIOD podkreśla, że wspomniana rezolucja Rady ustanawia kilka bardzo istotnych zabezpieczeń powiązanych ściśle z dynamicznym charakterem profili DNA. I tak, w sekcji III rezolucji, po ograniczeniu wymiany wyników analiz DNA do „stref chromosomów [...] które zgodnie z obecnym stanem wiedzy nie dostarczają informacji o konkretnych cechach dziedzicznych”, państwu członkowskim zostaje zalecone zaprzestanie dalszego wykorzystywania tych wskaźników DNA, które, ze względu na postęp naukowy, mogą dostarczać informacji na temat szczególnych cech dziedzicznych.
61. Konwencja z Prüm przewiduje inne podejście: zobowiązuje umawiające się strony do tworzenia i prowadzenia kartotek analiz DNA do celów śledztw lub dochodzeń prowadzonych w sprawach karnych. Tym samym prowadzi do utworzenia nowych baz danych DNA i zwiększenia liczby zgromadzonych danych DNA. Ponadto nie jest jasne, jaki rodzaj danych ma być wprowadzany do „kartotek analiz DNA”, a konwencja nie uwzględnia dynamicznego charakteru profili DNA.
62. EIOD wskazuje, że każdy akt prawny przewidujący wymianę danych DNA powinien:
- W wyraźny sposób ograniczać i definiować rodzaj informacji na temat DNA, które można wymienić (przy uwzględnieniu zasadniczej różnicy między próbkami DNA a profilami DNA).
  - Ustalać wspólne standardy techniczne mające na celu unikanie sytuacji, w których różnice w sposobach prowadzenia w państwach członkowskich sądowych baz danych DNA mogłyby prowadzić do trudności i niedokładnych wyników przy wymianie danych.
  - Zapewniać właściwe prawnie wiążące zabezpieczenia mające na celu zapobieganie sytuacjom, w których postęp naukowy prowadziłby do uzyskiwania z profili DNA danych osobowych będących nie tylko danymi wrażliwymi, ale również zbędnymi do celów, dla których zostały zgromadzone.
63. W świetle powyższego EIOD niniejszym potwierdza i ujednolica uwagi zawarte we wcześniejszej opinii dotyczącej decyzji ramowej w sprawie ochrony danych osobowych (pkt 80). We wspomnianej opinii EIOD wskazał na konieczność zapewnienia szczególnych zabezpieczeń w odniesieniu do danych DNA celem zagwarantowania, że: dostępne informacje mogą być wykorzystywane jedynie do identyfikowania osób do celów zapobiegania przestępstwom, ich wykrywania lub ścigania; stopień dokładności profili DNA jest należycie uwzględniony i może być podważony przez osobę, której dane dotyczą, przy pomocy dostępnych sposobów; jest w pełni zapewnione poszanowanie godności osobistej <sup>(2)</sup>.
64. Powyższe uwagi prowadzą ponadto do konkluzji, że akty prawne dotyczące tworzenia kartotek DNA i wymiany danych pochodzących z tych kartotek powinny zostać przyjęte dopiero po dokonaniu oceny skutków regulacji pozwalającej na właściwą ocenę korzyści i ryzyka. EIOD zaleca, aby takie akty prawne zawierały obowiązek przeprowadzania regularnych ocen po wejściu w życie tych aktów prawnych.
65. Załącznik II przewiduje także innego rodzaju informacje, które mogą być wymieniane. Są to informacje pochodzące od osób prywatnych, jako że numery telefoniczne i inne dane dotyczące połączeń, a także dane odnoszące się do ruchu połączeń zazwyczaj nie pochodzą od operatorów telefonicznych. Uzasadnienie wniosku potwierdza obowiązek państw członkowskich dotyczący zagwarantowania, że informacje służące organom ścigania, kontrolowane przez organy lub osoby prywatne wyznaczone do tego celu, są udostępniane równoważnym właściwym organom innych państw członkowskich i Europolowi. Jako że wniosek dotyczy danych osobowych pochodzących od osób prywatnych, zdaniem EIOD stosowane ramy prawne powinny zawierać dodatkowe zabezpieczenia w celu ochrony osób, których dane dotyczą, jak również powinny zapewniać dokładność danych.

## VII. ZASADY OCHRONY DANYCH

66. Przepisy dotyczące ochrony danych osobowych nie zostały wyszczególnione w proponowanej decyzji ramowej Rady; natomiast inne akty prawne, takie jak konwencja z Prüm czy wspomniany wcześniej wniosek Szwecji, zawierają przepisy szczególne w zakresie ochrony tych danych. Brak we wniosku dotyczącym zasady dostępności przepisów szczególnych regulujących ochronę danych osobowych jest dopuszczalny wyłącznie o ile przepisy ogólne zawarte we wniosku dotyczącym decyzji ramowej w sprawie ochrony danych w trzecim filarze będą w pełni stosowane i zapewnią wystarczającą ochronę. Ponadto przepisy dotyczące ochrony danych osobowych przewidziane w poszczególnych aktach prawnych — takich jak wniosek Szwecji czy konwencja z Prüm — nie powinny obniżać poziomu ochrony zapewnianego przez ogólne ramy prawne. EIOD zaleca włączenie specjalnej klauzuli regulującej ewentualną kolizję między różniącymi się między sobą przepisami dotyczącymi ochrony danych.

<sup>(1)</sup> Dz.U. C 187, str. 1.

<sup>(2)</sup> Ten sam tok rozumowania – patrz również dokument Rady Europy zatytułowany „Sprawozdanie okresowe w sprawie stosowania zasad Konwencji 108 do gromadzenia i przetwarzania biometrycznych danych osobowych”, luty 2005 r.



67. W tym miejscu EIOD chciałby ponownie podkreślić, przypominając swoją opinię na temat decyzji ramowej w sprawie ochrony danych, znaczenie istnienia spójnych i wyczerpujących przepisów dotyczących ochrony danych, uwzględniających współpracę organów ścigania, mających zastosowanie do wszystkich etapów przetwarzania danych. EIOD podtrzymuje również pozostałe założenia przedstawione we wspomnianej opinii. W niniejszym ustępie uwaga zostaje zwrócona na następujące kwestie dotyczące ochrony danych:

- Zgodne z prawem przetwarzanie danych osobowych. EIOD podtrzymuje pogląd, zgodnie z którym informacje mogą zostać udostępnione, wyłącznie jeżeli zostały zgromadzone zgodnie z prawem (o czym mówi art. 2 ust. 2 w odniesieniu do informacji zgromadzonych przy użyciu środków przymusu). Przetwarzanie danych osobowych zgodne z prawem zagwarantowałoby również, że informacje udostępnione i wymienione mogą być we właściwy sposób wykorzystane także w postępowaniu sądowym. Rzeczywiście, chociaż informacje przetwarzane po rozpoczęciu postępowania karnego nie są objęte zakresem zastosowania proponowanego aktu prawnego, nadal istnieje prawdopodobieństwo, że informacje wymienione wcześniej między organami ścigania mogą zostać wykorzystane podczas postępowania sądowego.
- Jakość danych osobowych ma szczególne znaczenie, zważywszy że zasada dostępności sprzyja wykorzystaniu informacji przez organy ścigania działające poza kontekstem, w którym dane zostały zgromadzone. Organy te mają dostęp bezpośredni nawet do baz danych innych państw członkowskich. Zapewnienie jakości danych osobowych jest możliwe tylko przy regularnym i odpowiednim sprawdzaniu ich dokładności, przy podziale informacji zgodnie z różnymi kategoriami osób, których one dotyczą (ofiary, podejrzani, świadkowie itp.), oraz, gdy jest to konieczne, przy wskazaniu stopnia dokładności (patrz opinia EIOD w sprawie ochrony danych osobowych, IV.6).

Wymienione punkty raz jeszcze wyraźnie pokazują, dlaczego przepisy dotyczące ochrony danych, a zwłaszcza aspektu dokładności, powinny być stosowane do wszystkich rodzajów przetwarzania, w tym także przetwarzania na szczeblu krajowym. Nieprzestrzeganie tej zasady mogłoby prowadzić do sytuacji, w której dane osobowe, do których dostęp jest bezpośredni mogłyby być nieprawidłowe lub nieaktualne, co wpłynęłoby zarówno na prawa osób, których dane dotyczą, jak i na skuteczność prowadzonych śledztw lub dochodzeń.

- Ograniczenie celu. Zgodnie z zasadą dostępności, dostęp do danych osobowych mogą mieć równoważne właściwe organy innych państw członkowskich. Niemniej jednak uprawnienia organów ścigania mogą różnić się zasadniczo w poszczególnych państwach. Konieczne staje się zatem zapewnienie przestrzegania podstawowej zasady ograniczenia celu, bez względu na różny zakres uprawnień różnych właściwych organów wymienianych dane. Informacje gromadzone i przetwarzane przez dany organ w określonym celu nie

mogą następnie być wykorzystane w innym celu tylko ze względu na inne, być może szersze, uprawnienia organu otrzymującego dane.

EIOD z zadowoleniem przyjmuje zatem art. 7 proponowanej decyzji ramowej, który należy odczytywać jako doprecyzowanie przepisów ogólnych ustanowionych w proponowanej decyzji ramowej w sprawie ochrony danych osobowych. EIOD zauważa również, że ocena stopnia równoważności poszczególnych organów (która we wniosku w obecnym brzmieniu podlega procedurze komitologii) powinna być przeprowadzana w sposób staranny, przy zachowaniu należytego poszanowania dla zasady ograniczenia celu.

- Ograniczenia czasowe dotyczące przechowywania wymienionych informacji należy również postrzegać w świetle zasady ograniczenia celu: informacje udostępnione lub wymienione w danym celu powinny zostać usunięte, gdy tylko przestaną być potrzebne do tego celu. Dzięki temu uniknie się zbędnego powielania baz danych, a jednocześnie zapewni się właściwym organom ponowny dostęp do (uaktualnionych) dostępnych informacji, w przypadku, w którym byłoby to konieczne w innym uzasadnionym celu.
- Rejestr informacji przekazanych zgodnie z zasadą dostępności. Rejestry informacji powinny być tworzone po obu stronach: zarówno w państwie członkowskim, do którego skierowano wniosek o udzielenie informacji, jak i w państwie członkowskim składającym taki wniosek. Należy prowadzić rejestry nie tylko wymiany, ale również dostępu do danych (patrz opinia EIOD w sprawie ochrony danych osobowych, pkt 133), co służyć ma między innymi budowie wzajemnego zaufania między właściwymi organami krajowymi oraz zachowaniu przynajmniej częściowej kontroli nad dostępnymi informacjami. Potrzeba śledzenia informacji zakłada również możliwość uaktualniania lub poprawiania informacji.
- Prawa osób, których dane dotyczą. Systemy wymiany informacji pomiędzy organami ścigania UE zwiększają prawdopodobieństwo wystąpienia sytuacji, w których dane osobowe są (chwilowo) przetwarzane w tym samym momencie przez właściwe organy w różnych państwach członkowskich. Oznacza to z jednej strony konieczność opracowania wspólnych norm UE odnoszących się do praw osób, których dane dotyczą, a z drugiej strony — umożliwienie tym osobom wykonywanie ich praw w zakresie, w jakim jest to dozwolone przepisami regulującymi ochronę danych w trzecim filarze, w odniesieniu zarówno do organów udostępniających dane, jak i organów, którym dane są udostępniane i które je przetwarzają.
- Nadzór. EIOD wskazuje, że, w zależności od przypadku, uprawnionym do kontroli przetwarzania danych osobowych na podstawie omawianego wniosku może być więcej niż jeden krajowy organ nadzoru. W tym kontekście bezpośredni dostęp przez Internet do informacji służących organom ścigania wymaga zwiększenia nadzoru i koordynacji przez właściwe krajowe organy ochrony danych.

## VIII. WNIOSKI

**Ogólne wnioski dotyczące zasady dostępności**

68. EIOD, korzystając z nadarzającej się okazji, przedstawił w niniejszej opinii kilka podstawowych założeń o charakterze bardziej ogólnym dotyczących wymiany informacji służących organom ścigania oraz różnorodnych podejść do uregulowania tego tematu. Na późniejszym etapie prac będzie można zgłaszać do EIOD kolejne wnioski o wydanie opinii w zależności od postępów poczynionych na kolejnych etapach procesu legislacyjnego obejmującego zarówno omawiany wniosek, jak i inne wnioski z nim powiązane.
69. Zdaniem EIOD zasada dostępności powinna zostać wprowadzona do wiążącego aktu prawnego przy wykorzystaniu podejścia bardziej wyważonego, stopniowego podejścia obejmującego jeden rodzaj danych; podejście to powinno przewidywać kontrolę stopnia, w jakim zasada dostępności może skutecznie wspierać ściganie przestępstw, a także konkretne zagrożenia dla ochrony danych osobowych. Takie bardziej wyważone podejście mogłoby obejmować rozpoczęcie wprowadzania w życie zasady dostępności wyłącznie przy wykorzystaniu dostępu pośredniego, czyli poprzez odnośniki. Na podstawie takich doświadczeń, systemem prawdopodobnie mogłyby zostać objęte inne rodzaje danych, jak również mogłoby on zostać zmodyfikowany w celu zwiększenia jego skuteczności.
70. Nie należy przyjmować żadnego aktu prawnego wdrażającego zasadę dostępności bez uprzedniego przyjęcia podstawowych zabezpieczeń w celu ochrony danych, o których mowa we wniosku dotyczącym decyzji ramowej w sprawie ochrony danych osobowych.

**Zalecenia mające na celu wprowadzenie zmian do omawianego wniosku**

71. EIOD zaleca sprecyzowanie zakresu zastosowania zasady dostępności w następujący sposób:
- Wprowadzenie jasnej i precyzyjnej definicji danych, które będą uważane za dostępne.
  - Pierwsza możliwość: ograniczenie zakresu zastosowania zasady dostępności do informacji kontrolowanych przez właściwe organy.
  - Druga możliwość: w przypadku szerszego zakresu zastosowania, wprowadzenie wystarczających zabezpieczeń w celu ochrony danych osobowych. Należy uwzględnić kwestie poruszone w pkt 27 niniejszej opinii.
72. EIOD ma następujące uwagi w odniesieniu do bezpośredniego dostępu do baz danych przez właściwy organ innego państwa członkowskiego:
- Kwestią tą trzeba się zająć w należyty sposób, zważywszy że, w przypadku dostępu bezpośredniego, wyznaczone organy państwa członkowskiego udostęp-

nijącego dane nie mają żadnej kontroli nad dostępem i dalszym wykorzystaniem danych.

- Wniosek nie może przyczyniać się do tworzenia nieograniczonych wzajemnych połączeń między bazami danych, a tym samym do tworzenia trudnej do nadzorowania sieci baz danych.
73. Decyzja ramowa powinna być dokładniejsza w odniesieniu do utworzenia systemu odnośników. W szczególności:
- Wniosek powinien zawierać odpowiednie przepisy, przynajmniej w odniesieniu do tworzenia odnośników, dotyczące zarządzania systemami przechowywania odnośników oraz właściwej organizacji dostępu do odnośników.
  - Definicję pojęcia odnośników należy uczynić bardziej zrozumiałą.
  - We wniosku powinna zostać dokładniej określona rola krajowych punktów kontaktowych w zakresie odnośników.
  - Podstawowe przepisy dotyczące utworzenia odnośników powinny zostać włączone do decyzji ramowej, a nie pozostawione przepisom wykonawczym zgodnie z procedurą komitologii.
74. EIOD wskazuje, że wniosek — w zakresie, w jakim przewiduje wymianę danych DNA — powinien:
- W wyraźny sposób ograniczyć i zdefiniować rodzaje informacji na temat DNA, które można wymieniać (przy uwzględnieniu zasadniczej różnicy między próbkami DNA a profilami DNA).
  - Ustalać wspólne standardy techniczne mające na celu unikanie sytuacji, w których różnice w sposobach prowadzenia w państwach członkowskich sądowych baz danych DNA mogłyby prowadzić do trudności i niedokładnych wyników przy wymianie danych.
  - Zapewniać właściwe, prawnie wiążące zabezpieczenia mające na celu zapobieganie sytuacjom, w których postęp naukowy prowadziłby do uzyskiwania z profili DNA danych osobowych będących nie tylko danymi wrażliwymi, ale również zbędnymi do celów, dla których zostały zgromadzone.
  - Zostać przyjęty po dokonaniu oceny wpływu.
75. EIOD doradza ograniczenie wymiany informacji z Europolem do celów, zgodnie z którymi działa ta organizacja, wymienionych w art. 2 konwencji o Europolu i w załączniku do niej.

Sporządzono w Brukseli, dnia 28 lutego 2006 r.

Peter HUSTINX

*Europejski Inspektor Ochrony Danych*