

Druga opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych

(2007/C 91/02)

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 ⁽¹⁾,

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 ⁽²⁾, w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1. Dnia 19 grudnia 2005 r. Europejski Inspektor Ochrony Danych (EIOD) wydał opinię ⁽³⁾ w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. W tej opinii EIOD podkreślił znaczenie wniosku jako skutecznego narzędzia ochrony danych osobowych w dziedzinie objętej tytułem VI Traktatu UE. Taki akt prawny powinien nie tylko szanować zasady ochrony danych określone w konwencji nr 108 Rady Europy ⁽⁴⁾, a zwłaszcza w dyrektywie 95/46/WE, ale także ustanawiać dodatkowy zbiór zasad uwzględniających szczególny charakter dziedziny ochrony porządku publicznego. Dla EIOD kwestią o kluczowym znaczeniu jest, by zakres decyzji ramowej obejmował wszystkie dane policyjne i sądowe, nawet jeżeli nie są one przekazywane ani udostępniane przez właściwe organy innych państw członkowskich. Niezwykle istotna jest spójność w zakresie ochrony danych, niezależnie od tego gdzie, przez kogo i do jakich celów są one przetwarzane. EIOD złożył kilka propozycji zmierzających do podwyższenia poziomu ich ochrony.
2. Dnia 27 września 2006 r. Parlament Europejski przyjął rezolucję legislacyjną dotyczącą wniosku Komisji. Zasadniczo rezolucja ma te same cele, co opinia EIOD: ogólne poparcie dla wniosku i poprawki mające na celu podwyższenie poziomu ochrony zapewnianego na mocy decyzji ramowej.
3. Wniosek Komisji obecnie został poddany dyskusji na forum Rady. Rada rzekomo ⁽⁵⁾ czyni postępy i modyfikuje kluczowe elementy tekstu wniosku. Prezydencja Rady dokłada wysiłków, by postępy były jak największe. Jej celem jest wypracowanie wspólnego podejścia do głównych elementów wniosku do grudnia 2006 r.
4. EIOD z zadowoleniem przyjmuje uwagę, jaką Rada darzy ten istotny wniosek. Napawa go jednak troską kierunek wprowadzanych zmian. Teksty obecnie omawiane na forum Rady nie ujmują poprawek proponowanych przez Parlament Europejski ani opinii EIOD i konferencji europejskich organów ds. ochrony danych. Wręcz przeciwnie, w niejednym przypadku przepisy zawarte we wniosku Komisji, oferujące obywatelom pewne zabezpieczenia, zostały skreślone lub znacznie osłabione. W rezultacie istnieje znaczne prawdopodobieństwo, że poziom ochrony będzie niższy niż zapewniony na mocy dyrektywy 95/46/WE, a nawet bardziej ogólnej konwencji nr 108 Rady Europy, którą są związane państwa członkowskie.

⁽¹⁾ Dz.U. L 281 z 23.11.1995, str. 31.

⁽²⁾ Dz.U. L 8 z 12.1.2001, str. 1.

⁽³⁾ Dz.U. C 47 z 25.2.2006, str. 27.

⁽⁴⁾ Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, 28 stycznia 1981 r.

⁽⁵⁾ Z formalnego punktu widzenia brak jest publicznie dostępnych dokumentów, a EIOD nie uczestniczy bezpośrednio w pracach grupy roboczej Rady. Dokumenty odzwierciedlające stan prac w Radzie są dostępne na stronie internetowej Statewatch (www.statewatch.org).

5. EIOD zauważył także, że Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego ostatnio wyraziła obawy dotyczące podejmowanych przez Radę decyzji w sprawie omawianego wniosku.
6. Z tego powodu EIOD wydaje niniejszą drugą opinię. Skupia się ona na pewnych podstawowych problemach i nie powtarza wszystkich zagadnień ujętych w opinii z grudnia 2005 r., która w całości pozostaje w mocy.

Uwagi ogólne

7. W procesie tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości wymiana informacji politycznych i sądowych między państwami członkowskimi staje się coraz ważniejsza. Złożono wnioski dotyczące kilku aktów prawnych — kilka też już przyjęto — by ułatwić tę wymianę. EIOD raz jeszcze podkreśla, że w tym kontekście — by zagwarantować poszanowanie praw podstawowych obywateli — konieczne są solidne ramy prawne chroniące osoby, których dotyczą dane. Omawiana decyzja ramowa (wniosek jej dotyczący) jest bezpośrednio powiązana z wnioskami mającymi na celu ułatwienie takiej wymiany informacji.
8. Choć EIOD uznaje, że jak najszybsze przyjęcie decyzji ramowej przez Radę jest istotne, przestrzega również, że tempo podejmowania decyzji nie powinno prowadzić do obniżenia standardów ochrony. Teksty omawiane obecnie przez Radę budzą wątpliwości co do tego, czy ich rezultaty będą wystarczająco solidne, by zapewnić obywatelom skuteczną ochronę. W obecnej sytuacji skutkiem skupienia się na krótkim terminie wydaje się być skreślenie lub osłabienie potencjalnie kontrowersyjnych przepisów. Brak czasu, by osiągnąć porozumienie w sprawie tych potencjalnie kontrowersyjnych przepisów, mógłby zaowocować utratą wymaganej od decyzji ramowej jakości.
9. W tej sytuacji EIOD zaleca Radzie dłuższy okres negocjacji, by osiągnąć rezultaty zapewniające wystarczającą ochronę.

Zastosowanie do przetwarzania danych w kontekście krajowym

10. To zagadnienie stanowi zasadniczy element opinii z grudnia 2005 r. i zostało później gruntownie przedyskutowane. Wspólne zasady ochrony danych powinny mieć zastosowanie do wszystkich danych w dziedzinie współpracy policyjnej i sądowej, nie zaś być ograniczone do transgranicznej wymiany danych między państwami członkowskimi. Bardziej ograniczony zakres zastosowania nie byłby w stanie zaowocować właściwym poziomem ochrony wymaganym przez art. 30 ust. 1 lit. b) Traktatu UE. Punkt ten był wielokrotnie podkreślany, nie tylko przez EIOD.
11. W opinii z grudnia 2005 r. EIOD oświadczył, że ograniczenie do danych, które są wymieniane między państwami członkowskimi, uczyniłoby zakres zastosowania decyzji ramowej szczególnie niepewnym, co jest sprzeczne z zasadniczym celem tej decyzji. Przez cały okres gromadzenia lub przetwarzania danych osobowych nie jest wiadomo, czy dane te będą później użyteczne do celów wymiany z właściwymi organami innych państw członkowskich.
12. Z tego powodu bardziej ograniczony zakres stosowania jest niewłaściwy i, o ile zostanie wprowadzony, będzie wymagał trudnych i precyzyjnych rozróżnień w ramach baz danych organów ochrony porządku publicznego, co będzie prowadzić jedynie do dodatkowych komplikacji i kosztów ponoszonych przez te organy, a ponadto negatywnie wpłynie na pewność prawną z punktu widzenia poszczególnych osób.
13. Kwestię tę można zilustrować na dwóch przykładach. Po pierwsze, dodatkowe komplikacje i koszty wynikają z faktu, że akta dotyczące przestępstw w wielu przypadkach składają się z danych pochodzących od różnych organów. Skutkiem ograniczenia zakresu zastosowania decyzji byłoby to, że części takich złożonych akt — części zawierające dane pochodzące od organów innych państw członkowskich — byłyby objęte ochroną na mocy decyzji ramowej, zaś pozostałe części akt byłyby tej ochrony pozbawione. Po drugie, negatywnie wpłynęłoby to na pewność prawną z punktu widzenia poszczególnych osób, gdyż — w przypadku ograniczonego zakresu zastosowania — dane pochodzące z państw trzecich, ale nie będące przedmiotem wymiany między państwami członkowskimi, nie byłyby objęte decyzją ramową. Nie trzeba powtarzać, że przetwarzanie tych danych pociąga za sobą konkretne ryzyko dla osób, których one dotyczą, jeżeli na przykład brak będzie prawnego zobowiązania do sprawdzania ścisłości takich danych. Dobrym przykładem jest wykorzystanie przez państwo członkowskie do celów ochrony porządku publicznego sporządzanych przez państwa trzecie list osób objętych zakazem lotów do tych państw.

14. EIOD po raz kolejny podkreśla, że niezbędny jest wysoki poziom ochrony danych w dziedzinie współpracy policyjnej i sądowej — w której przetwarzanie danych osobowych z samej swojej natury stanowi szczególne ryzyko dla obywateli, co uznano m.in. w art. 30 ust. 1 lit. b) Traktatu UE. Ponadto duże rozbieżności między ochroną danych w obrębie pierwszego i trzeciego filaru wpłynęłyby nie tylko na prawo obywateli do ochrony ich danych osobowych, ale także na skuteczność ochrony porządku publicznego i wzajemne zaufanie między państwami członkowskimi.
15. Omawiany wniosek służy obydwoóm celom. Powinien on zabezpieczać obywateli przed niewłaściwym wykorzystaniem ich danych osobowych. Dla obywatela, którego dotyczą przetwarzane dane, nie ma znaczenia, czy są one przetwarzane w kontekście wymiany między państwami członkowskimi, czy też w kontekście czysto krajowym. Ponadto zabezpieczenie obywateli przed niewłaściwym wykorzystaniem ich danych powinno przyczynić się do wzrostu wzajemnego zaufania między państwami członkowskimi, co stanowi warunek skutecznej wymiany informacji. Zastosowanie do przetwarzania danych wspólnych standardów ułatwi akceptację danych wymienianych przez państwa członkowskie.
16. EIOD ostrzega, że ograniczenie zakresu zastosowania decyzji ramowej do danych w kontekście wymiany nie zapewniłoby w pełni warunków do budowy zaufania między organami poszczególnych państw członkowskich. Ponadto tak ograniczony tekst nie oferuje odpowiedniej ochrony obywateli. W tych okolicznościach decyzja ramowa nie oferowałaby obywatelom odpowiedniego zabezpieczenia przez ewentualnym nadużyciem ich danych ze strony organów publicznych. Zdaniem EIOD sprawowana przez prawodawstwo funkcja „tarczy ochronnej” jest funkcją zasadniczą, choćby tylko dla zapewnienia, że Unia Europejska respektuje prawa podstawowe zgodnie z art. 6 Traktatu UE.
17. Ponadto istnieje argument strategiczny przemawiający za zastosowaniem decyzji ramowej do wszelkich typów przetwarzania. Jak pokazują niedawne negocjacje ze Stanami Zjednoczonymi dotyczące nowej umowy o przetwarzaniu i przekazywaniu danych dotyczących przelotu pasażera (PNR) ⁽¹⁾, solidne prawodawstwo unijne chroniące obywateli we wszystkich sytuacjach wewnątrz UE wzmocniłoby również stanowisko UE w negocjacjach z państwami trzecimi. Z braku takiego solidnego prawa byłoby raczej trudne wymaganie od państw trzecich odpowiedniego poziomu ochrony jako warunku wstępnego przekazywania danych osobowych.

Inne kwestie

18. *Nacisk na jakość danych.* Art. 4 wniosku Komisji ujmuje nie tylko główne zasady jakości danych zawarte w dyrektywie 95/46/WE, ale także zawiera pewne zasady szczegółowe. Obejmują one rozróżnienie między różnymi rodzajami osób, których dotyczą dane (podejrzani, skazani, ofiary, świadkowie itd.). Dane z nimi związane powinny być traktowane w różny sposób, z użyciem odpowiednich zabezpieczeń, szczególnie w odniesieniu do osób niebędących podejrzanymi. Ponadto artykuł ten ustanawia obowiązek rozróżniania przez państwa członkowskie danych zgodnie ze stopniem ich ścisłości i wiarygodności. Jest to istotny przepis, gdyż organy ochrony porządku publicznego wykorzystują również dane oparte na przypuszczeniach, niekoniecznie zaś na faktach. EIOD uważa te przepisy za podstawowe zabezpieczenia, których nie należy usuwać z wniosku ani uznawać za fakultatywne.
19. *Przetwarzanie danych i ograniczenie celu.* W opinii z grudnia 2005 r. EIOD przeanalizował potrzebę lepszych uregulowań prawnych dotyczących dalszego wykorzystania danych, które zostały zgromadzone przez organ w konkretnym celu. Obecnie obawy EIOD związane z art. 5 są związane głównie z jego przekonaniem, że choć z jednej strony należy zezwolić na (dalsze) przetwarzanie danych do szerzej zakrojonych celów, z drugiej strony prawo musi określić precyzyjne warunki takiego przetwarzania, by chronić osobę, której dotyczą dane. EIOD przestrzega przed rozwiązaniami, które pozostawiają tę kwestię w pełni w gestii prawa krajowego lub nie ograniczają warunków dalszego przetwarzania danych zgodnie z dyrektywą 95/46/WE i konwencją nr 108 Rady Europy ⁽²⁾. Odnośnie do przetwarzania szczególnych kategorii danych: zajmuje się nim dyrektywa 95/46/WE oraz konwencja nr 108, zawierająca ogólny zakaz wraz z wyjątkami od niego ⁽³⁾. EIOD wyraża obawę, że ogólny zakaz zostanie z decyzji ramowej usunięty, a co za tym idzie wyjątek stanie się regułą. Takie rozwiązanie byłoby nie tylko niespójne z dyrektywą 95/46/WE, ale też niezgodne z konwencją nr 108.

⁽¹⁾ Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Dz.U. L 298, str. 29.

⁽²⁾ Patrz: Art. 13 w związku z art. 6 ust. 1 lit. b) dyrektywy 95/46/WE i art. 9 w związku z art. 5 lit. b) konwencji nr 108.

⁽³⁾ Patrz: art. 8 dyrektywy 95/46/WE oraz art. 6 konwencji nr 108.

20. Wymiana danych z innymi organami i osobami prywatnymi. Wniosek Komisji zawiera ograniczenia i szczególne zabezpieczenia dotyczące wymiany informacji z innymi organami poza policją i organami sądowymi, osobami prywatnymi i organami państw trzecich. EIOD podkreśla znaczenie takich szczególnych przepisów z poniższych przyczyn. Po pierwsze, wymiana informacji z tymi „stronami trzecimi” pociąga za sobą szczególne zagrożenia (naruszenia bezpieczeństwa, dalsze przetwarzanie do innych celów itd.). Po drugie, udział stron trzecich w ochronie porządku publicznego oraz w przetwarzaniu informacji służących takiej ochronie staje się coraz powszechniejszy. Dobrymi tego przykładami są dyrektywa 2006/24/WE o zatrzymywaniu danych ⁽¹⁾, umowa ze Stanami Zjednoczonymi o danych dotyczących przelotu pasażera (PNR) oraz tak zwana sprawa Swift ⁽²⁾. Po trzecie, wyrok Trybunału Sprawiedliwości dotyczący PNR z dnia 30 maja 2006 r. ⁽³⁾ stawia poważne wątpliwości dotyczące ochrony danych osobowych gromadzonych przez przedsiębiorstwa lub osoby prywatne do celów komercyjnych, a później przetwarzanych do celów ochrony porządku publicznego.
21. Odnośnie do transferu do i z innych zainteresowanych stron — publicznych i prywatnych — w obrębie UE ważne jest, że wniosek zajmuje się tą kwestią w sposób precyzyjny i oferuje rozwiązania spójne z dyrektywą 95/46/WE. Rozwiązania te muszą zagwarantować, że konsekwencje struktury opartej na podziale na filary — zwłaszcza niepewność dotycząca granic obu filarów w tym, co się tyczy wymiany danych osobowych między organami ochrony porządku publicznego a innymi stronami — nie zaszkodzi skuteczności ochrony.
22. Odnośnie do transferu danych do i z państw trzecich wniosek Komisji przewiduje podjęcie przez Komisję decyzji o tym, czy jest on właściwy. Jeżeli okaże się to nie do zaakceptowania dla Rady, w rezultacie każde państwo członkowskie będzie samo decydować o tym, czy taki transfer jest właściwy lub, co gorsza, przekazywać dane bez analizy poziomu ochrony w państwie trzecim. Brak ujednoliconego systemu wymiany danych osobowych z państwami trzecimi mógłby również:
- zmniejszyć zaufanie między organami państw członkowskich, gdyż organy jednego państwa, mogłyby być mniej chętne do dzielenia się informacjami z organami innego państwa członkowskiego, jeżeli to państwo członkowskie mogłoby również dzielić te informacje z organami państw trzecich w sytuacji braku konkretnych zabezpieczeń;
 - spowodować powrót do punktu wyjścia. Jeżeli jakiś organ w jednym państwie członkowskim nie mógłby uzyskać informacji bezpośrednio z innego państwa członkowskiego z powodu ochrony na mocy decyzji ramowej, mógłby zwrócić się o pomoc do organu państwa trzeciego;
 - skłonić organy państw trzecich do tzw. *forum shopping* — organy te mogłyby zwracać się o informacje do państwa członkowskiego o najniższych wymaganiach prawnych związanych z transferem.
- EIOD uważa za kwestię kluczową wprowadzenie mechanizmów zapewniających wspólne normy i skoordynowane decyzje dotyczące tego, czy transfer jest właściwy, również w celu wypełnienia postanowień konwencji nr 108 Rady Europy (w szczególności jej art. 12) ⁽⁴⁾. Tekst decyzji ramowej powinien przewidywać takie mechanizmy.
23. EIOD rozumie kwestionowanie przez niektóre państwa członkowskie podstawy prawnej włączenia do decyzji przepisu o wymianie danych osobowych z państwami trzecimi w przypadkach, gdy te dane nie są przesyłane lub udostępniane przez właściwy organ innego państwa członkowskiego. W opinii EIOD kwestionowanie tej podstawy prawnej nie ma uzasadnienia. Przykłady przedstawione w opinii z grudnia 2005 r. oraz argumenty zawarte w poprzednim punkcie pokazują bezpośredni związek tej wymiany danych z państwami trzecimi ze współpracą policyjną i sądową na mocy art. 29 Traktatu UE. Przepis dotyczący wymiany danych osobowych z państwami trzecimi musi być traktowany jako dodatkowy i niezbędny przepis, by osiągnąć cele art. 29 Traktatu UE w związku z art. 6 tego Traktatu, zwłaszcza ściślejszą współpracę organów policji w połączeniu z poszanowaniem praw podstawowych.

⁽¹⁾ Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz.U. L 105, str. 54.

⁽²⁾ Zob. opinia 10/2006 z dnia 22 listopada 2006 r. Zespołu Roboczego ds. Ochrony Danych art. 29 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (SWIFT).

⁽³⁾ Wyrok w sprawach C-317/04 i C-318/04.

⁽⁴⁾ Zob. dokładniejsze informacje: art. 2 protokołu dodatkowego (ratyfikowanego przez część państw członkowskich), zgodnego z art. 25-26 dyrektywy 95/46/WE.

24. *Prawa osób, których dotyczą dane.* Osoba, której dotyczą dane, ma prawo do informacji o przetwarzaniu danych osobowych jej dotyczących. To prawo jest związane z zasadą uczciwego i zgodnego z prawem przetwarzania danych osobowych, którą decyzja ramowa respektuje, a ponadto jest chronione konwencją nr 108 Rady Europy, w szczególności jej art. 5 lit. a) i art. 8. Zasadniczym elementem tego prawa jest to, że informacji tych kontroler danych powinien udzielać z urzędu. Jako że osoba, której dotyczą dane, zwykle nie zna i nie może znać przetwarzanych informacji na swój temat, wymaganie złożenia przez tę osobę wniosku byłoby sprzeczne z samym charakterem jej prawa. Naturalnie prawo do informacji podlega pewnym wyjątkom i jest jasne, że może odgrywać ważną rolę w dziedzinie ochrony porządku publicznego, gdy informacje dotyczące postępowań karnych mogłyby zaszkodzić tym postępowaniom. Jednak wszelkie rozwiązania uzależniające prawo do informacji od złożenia wniosku przez osobę, której dotyczą dane, są nie do przyjęcia i są niezgodne z konwencją nr 108 Rady Europy.
25. EIOD podkreśla, że *stanowisko organów ochrony danych* powinno być zgodne z pozycją przyznaną im na mocy dyrektywy 95/46/WE. Stanowisko to w dziedzinie współpracy policyjnej i sądowej staje się tym istotniejsze. Współpraca pomiędzy organami ochrony porządku publicznego w celu skutecznego zwalczania terroryzmu i innych poważnych przestępstw wymaga przetwarzania często wrażliwych danych osobowych oraz czynienia wyjątków od praw osób, których dotyczą dane (zob. np. poprzedni punkt dotyczący prawa do informacji).
26. EIOD wskazuje po pierwsze potrzebę sprawowania przez organy skutecznego nadzoru i kontroli przetwarzania danych osobowych w zakresie zastosowania omawianej decyzji ramowej, szczególnie jeżeli dane osobowe są wymieniane między państwami członkowskimi w zakresie współpracy policyjnej. Po drugie, należy zagwarantować doradczą rolę organów w ramach jurysdykcji krajowej oraz zinstytucjonalizowanej sieci organów ochrony danych, zespołu roboczego złożonego z tych organów (w dyrektywie określonego jako zespół roboczy art. 29). Konieczny jest wkład ze strony organów ochrony danych, by zwiększyć spójność ochrony na mocy omawianego aktu z ochroną na mocy dyrektywy 95/46/WE, zapewnić poszanowanie zobowiązań prawnych i osiągnąć pełne ujednoczenie wśród państw członkowskich, w tym na poziomie praktycznym.
27. Art. 24 wniosku Komisji zawiera szczegółowe zasady dotyczące *bezpieczeństwa*, porównywalne do zasad zawartych w konwencji o Europolu. EIOD przestrzega przed wykreśleniem tych zasad z tekstu wniosku. Ujednoczony poziom bezpieczeństwa stanowi ważne narzędzie zwiększania zaufania dla osób, których dotyczą dane, oraz dla organów państw członkowskich.
28. W opinii z grudnia 2005 r. EIOD zalecił zastosowanie konkretnych zabezpieczeń odnośnie do *przetwarzania określonych kategorii danych*, takich jak dane biometryczne i profile DNA. W dziedzinie ochrony porządku publicznego wykorzystanie tych kategorii danych przybiera na znaczeniu, choć może ono pociągać za sobą określone ryzyko dla osoby, której dotyczą dane. Niezbędne są wspólne zasady. EIOD wyraża żal, że zalecenie to nie zostało uwzględnione przez Radę, a przynajmniej że nie zostało to uwidocznione. EIOD wzywa Komisję i Radę do przyjęcia wniosku w tej sprawie, związanego z zasadą dostępności lub nie.

Podsumowanie

29. EIOD zaleca Radzie dłuższy okres negocjacji, by osiągnąć rezultaty zapewniające wystarczającą ochronę. Choć EIOD uznaje, że przyjęcie decyzji ramowej przez Radę w krótkim terminie jest istotne, przestrzega również, że tempo podejmowania decyzji nie powinno prowadzić do obniżenia standardów ochrony.
30. Niezwykle istotna jest spójność w zakresie ochrony danych osobowych, niezależnie od tego gdzie, przez kogo i do jakich celów są one przetwarzane. EIOD wzywa Radę do utrzymywania poziomu ochrony, który nie byłby niższy niż zapewniony na mocy dyrektywy 95/46/WE, a nawet bardziej ogólnej konwencji nr 108 Rady Europy, którą są związane państwa członkowskie.
31. Wspólne zasady ochrony danych powinny mieć zastosowanie do wszystkich danych w dziedzinie współpracy policyjnej i sądowej, nie zaś być ograniczone do transgranicznej wymiany danych między państwami członkowskimi. Niniejsza opinia zawiera argumenty wskazujące, że bardziej ograniczony zakres zastosowania jest niewłaściwy i, o ile zostanie wprowadzony, będzie prowadzić jedynie do dodatkowych komplikacji i kosztów ponoszonych przez organy, a ponadto negatywnie wpłynie na pewność prawną z punktu widzenia poszczególnych osób.

32. Inne zastrzeżenia EIOD są następujące:

- konkretne przepisy dotyczące jakości danych zawarte we wniosku Komisji nie powinny zostać skreślone ani uczynione fakultatywnymi;
- przepisy dotyczące dalszego wykorzystania danych oraz szczególnych kategorii danych powinny być spójne z dyrektywą 95/46/WE i zgodne z konwencją nr 108 Rady Europy;
- nie należy wykreślać z tekstu wniosku konkretnych przepisów dotyczących wymiany danych z innymi stronami poza organami ochrony porządku publicznego w obrębie UE ani ograniczać zakresu ich zastosowania. Odnośnie do wymiany danych z państwami trzecimi należy co najmniej wprowadzić mechanizmy zapewniające wspólne normy i skoordynowane decyzje dotyczące tego, czy transfer jest właściwy, również w celu wypełnienia postanowień konwencji nr 108 Rady Europy. Tekst decyzji ramowej powinien przewidywać takie mechanizmy;
- wszelkie rozwiązania uzależniające prawo do informacji od złożenia wniosku przez osobę, której dotyczą dane, są nie do przyjęcia i są niezgodne z konwencją nr 108 Rady Europy;
- stanowisko organów ochrony danych powinno być zgodne z pozycją przyznaną im na mocy dyrektywy 95/46/WE;
- nie należy wykreślać z tekstu wniosku szczegółowych zasad dotyczących bezpieczeństwa, porównywalnych do zasad zawartych w konwencji o Europolu;
- Komisja i Rada powinny przyjąć wniosek dotyczący przetwarzania określonych kategorii danych, takich jak dane biometryczne i profile DNA, związany z zasadą dostępności lub nie.

Sporządzono w Brukseli, dnia 29 listopada 2006 r.

Peter HUSTINX
Europejski Inspektor Ochrony Danych
