I

(Rezolucje, zalecenia, stanowiska i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Trzecia 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 139/01)

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:

I. **WPROWADZENIE**

1. Europejski Inspektor Ochrony Danych wydał, w dniu 19 grudnia 2005 r. i w dniu 29 listopada 2006 r., dwie opinie ([3]) w sprawie wniosku Komisji dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. W opiniach tych EIOD podkreślił znaczenie wniosku jako skutecznego narzędzia ochrony danych osobowych w dziedzinie objętej tytułem VI Traktatu UE. W szczególności, w drugiej z wydanych opinii EIOD wyraził obawy, że dotychczasowe wyniki negocjacji prowadzą do osiągnięcia poziomu ochrony danych osobowych, który nie tylko nie spełnia norm określonych w dyrektywie 95/46/WE, ale jest również niezgodny z bardziej ogólnymi postulatami konwencji Rady Europy nr 108 ([4]).

2. W styczniu 2007 roku prezydencja niemiecka określiła pewne podstawowe kwestie wymagające zmiany we wniosku, tak by możliwe było wycofanie pozostałych zastrzeżeń oraz poprawienie ochrony danych w trzecim filarze ([5]). Zmieniony projekt wniosku ([6]) przedłożono PE w dniu 13 kwietnia 2007 r. w celu uzyskania drugiej opinii.

([1]) Dz.U. L 281 z 23.11.1995, str. 31.
([2]) Dz.U. L 8 z 12.1.2001, str. 1.
([3]) Pierwsza opinia została opublikowana w Dz.U. C 47 z 25.2.2006, str. 27; druga jest dostępna na stronie internetowej EIOD: www.edps.europa.eu.
([4]) Konwencja Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.
([5]) Dokument Rady 5435/07 z dnia 18 stycznia 2007 r. dostępny pod adresem: register.consilium.europa.eu.
([6]) Dokument Rady 7315/07 z dnia 13 marca 2007 r. dostępny pod adresem: register.consilium.europa.eu.

3. Ze względu na zmiany merytoryczne zawarte w zmienionym wniosku, a także jego znaczenie, wymagana jest nowa opinia EIOD. Niniejsza opinia będzie się skupiać na głównych zastrzeżeniach EIOD; nie powraca on w niej do wszystkich uwag zawartych w poprzednich opiniach, ponieważ zachowują one ważność w odniesieniu do omawianego zmienionego wniosku.

II. **NOWY BODZIEC ZE STRONY PREZYDENCJI NIEMIECKIEJ**

4. EIOD z zadowoleniem przyjmuje fakt, że prezydencja niemiecka wkłada wiele wysiłku w negocjacje nad omawianą decyzją ramową Rady. Powszechnie wiadomo, że negocjacje w Radzie utknęły w martwym punkcie ze względu na fundamentalne różnice opinii różnych państw członkowskich na temat kluczowych zagadnień. Dlatego mądrym posunięciem ze strony prezydencji było ponowne ożywienie tych negocjacji dzięki przedstawieniu nowego tekstu.

5. Fakt nadania negocjacjom przez prezydencję niemiecką nowego impulsu ma sam w sobie bardzo pozytywny wydźwięk. Jednak po dogłębnej analizie najnowszego tekstu EIOD jest rozczarowany jego treścią. Tekst przedstawiony przez prezydencję niemiecką nie spełnia oczekiwań. Składają się na to następujące powody:

— Tekst osłabia poziom ochrony obywateli, ponieważ usunięto z niego pewne istotne przepisy służące ich ochronie, które zawierał wniosek Komisji.

— Pod wieloma względami zmieniony wniosek nie zapewnia nawet poziomu ochrony przyznawanego w konwencji nr 108. Nie jest więc satysfakcjonujący, a ponadto nie jest nawet zgodny z międzynarodowymi zobowiązaniami państw członkowskich.

— Omawiany tekst wnosi do sprawy dodatkowe zawiłości, ponieważ obejmuje przetwarzanie danych przez Europol, Eurojust i system informacji celnej trzeciego filara i wywołuje dyskusję nad nadzorem nad tym organami. Niniejsza opinia poświęcona będzie zwłaszcza kwestii, czy decyzja ramowa Rady jest właściwym instrumentem prawnym w odniesieniu do tych zagadnień.

— Nie zadowala jakość omawianego tekstu pod względem prawnym. Pomijając już wybór instrumentu prawnego, kilka przepisów nie spełnia wymogów określonych we wspólnych wytycznych dotyczących jakości przygotowania projektów prawodawstwa wspólnotowego ([7]). W szczególności, sformułowania zawarte w tekście nie są jasne, proste ani precyzyjne, co utrudnia obywatelom jednoznaczne określenie swoich praw i obowiązków.

— Niski poziom ochrony przewidziany we wniosku nie może w odpowiedni sposób przysłużyć się tworzeniu przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której informacje służące ochronie porządku publicznego mogą podlegać wymianie między organami policyjnymi i sądowymi ponad granicami państwowymi. W istocie, przy braku wysokiego i szeroko stosowanego poziomu ochrony danych wymiana informacji nadal podlega w myśl wniosku różnym krajowym „regułom pochodzenia" i „podwójnym normom", które wywierają znaczny niekorzystny wpływ na skuteczność współpracy w zakresie ochrony porządku publicznego, nie służąc przy tym poprawie ochrony danych osobowych ([8]).

6. EIOD jest świadomy, jak trudno jest osiągnąć jednomyślność w Radzie. Jednak taka procedura podejmowania decyzji nie może usprawiedliwiać podejścia opierającego się na znalezieniu najniższego wspólnego mianownika, którego rezultatem byłoby naruszenie podstawowych praw obywateli UE i zmniejszenie skuteczności ochrony porządku publicznego. W tym kontekście pożądane byłoby pełne uwzględnienie specjalistycznej wiedzy w zakresie ochrony danych oraz zastosowanie się do zaleceń, jakie w swoich rezolucjach ([9]) sformułował Parlament Europejski.

([7]) Porozumienie międzyinstytucjonalne z dnia 22 grudnia 1998 r. w sprawie wspólnych wytycznych dotyczących jakości przygotowania projektów prawodawstwa wspólnotowego (Dz.U. C 73 z 17.3.1999, str. 1). Przykłady podano w rozdziale V niniejszej opinii.

([8]) Zob. np. art. 14 dotyczący przekazywania danych organom w państwach trzecich lub instytucjom międzynarodowym; art. 12 ust. 1 lit. d) dotyczący dalszego przetwarzania danych osobowych; art. 10 dotyczący przestrzegania terminu usunięcia danych i terminu weryfikacji; art. 13 dotyczący przestrzegania krajowych ograniczeń przetwarzania danych.

([9]) Parlament Europejski przyjął swoją pierwszą rezolucję w sprawie pierwotnego wniosku Komisji w dniu 27 września 2006 r. Oczekuje się, że druga rezolucja, w sprawie zmienionego wniosku, zostanie przyjęta w czerwcu.

III. RAMY PRAWNE I GŁÓWNY PRZEDMIOT NINIEJSZEJ OPINII

7. Decyzja ramowa w sprawie ochrony danych osobowych w trzecim filarze jest kluczowym elementem rozwoju przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Rosnące znaczenie współpracy policyjnej i sądowej w sprawach karnych, a także działania wynikające z programu haskiego ([10]) wyeksponowały potrzebę wspólnych norm ochrony danych osobowych w ramach trzeciego filara.

8. Niestety, jak to wielokrotnie stwierdzali EIOD i inne właściwe podmioty ([11]), instrumenty istniejące na poziomie europejskim nie są wystarczające. Konwencja nr 108 Rady Europy, która wiąże państwa członkowskie, określa podstawowe ogólne zasady ochrony danych, jednak choć należy ją interpretować w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka, jej zapisy nie są wystarczająco precyzyjne, jak przy wielu okazjach stwierdzał wcześniej EIOD ([12]). Dyrektywę 95/46/WE, w której połączono i doprecyzowano zasady konwencji nr 108 w odniesieniu do rynku wewnętrznego, przyjęto już w roku 1995. Dyrektywa ta nie ma zastosowania do działań objętych zakresem trzeciego filara. W odniesieniu do działań w zakresie współpracy policyjnej i sądowej wszystkie państwa członkowskie uznają zalecenie nr R (87) 15 ([13]), które w pewnym stopniu dookreśla konwencję nr 108, jeśli chodzi o sektor policyjny, nie jest jednak instrumentem o charakterze prawnie wiążącym.

9. W tym kontekście art. 30 ust. 1 lit. b) TUE wymaga, aby wspólne działania w dziedzinie współpracy policyjnej, pociągające za sobą przetwarzanie informacji przez organy ochrony porządku publicznego, podlegały „właściwym przepisom o ochronie danych osobowych". Takie właściwe przepisy nie istnieją, bo brak jest decyzji ramowej Rady o odpowiedniej treści.

10. Łatwo stwierdzić podobieństwo sytuacji z rozwojem rynku wewnętrznego, w przypadku którego wysoki poziom ochrony danych osobowych w całej Wspólnocie uznano za nieodzowny, by znieść przeszkody w swobodnym przepływie towarów, usług, kapitału i osób; doprowadziło to do przyjęcia dyrektywy 95/46/WE. Analogicznie, przestrzeń wolności, bezpieczeństwa i sprawiedliwości, w której powinien istnieć swobodny przepływ informacji między organami odpowiedzialnymi za ochronę porządku publicznego zarówno na poziomie krajowym, jak i UE, wymaga istnienia wysokiego i jednolitego poziomu ochrony danych osobowych we wszystkich państwach członkowskich.

11. Te postulaty stoją w sprzeczności z obecną sytuacją, w której brak takich ogólnych ram i w której przepisy o ochronie danych osobowych w trzecim filarze mają charakter „sektorowy" i są rozproszone po różnych instrumentach prawnych ([14]). Kilka niedawnych wniosków ([15]) jedynie potwierdziło i zwiększyło już istniejące rozdrobnienie przepisów dotyczących ochrony danych w tej dziedzinie i zagroziło ich spójności. Ponadto brak ogólnych ram utrudnia szybkie przyjmowanie wielu wniosków w dziedzinie współpracy policyjnej i sądowej.

12. Z tych powodów w swych poprzednich opiniach EIOD zdecydowanie poparł wniosek Komisji i przedstawił odpowiednie zalecenia służące jego udoskonaleniu, co było konieczne dla zapewnienia obywatelom właściwego poziomu ochrony. EIOD niezmiennie twierdzi, że ogólne ramy ochrony danych w trzecim filarze muszą zapewniać wysoki i spójny standard ochrony danych, czerpiąc z zasad ochrony danych określonych w konwencji nr 108 i dyrektywie 95/46/WE, ale w razie potrzeby uwzględniając również szczególny charakter działań związanych z ochroną porządku publicznego.

13. Zapewnienie spójności tych ogólnych ram z zasadami ochrony danych w pierwszym filarze jest tym ważniejsze w sytuacji, w której rosnące zaangażowanie sektora prywatnego w ochronę porządku publicznego pociąga za sobą przenoszenie danych osobowych z pierwszego filara do trzeciego (jak w

([10]) Zob. również Plan działania Rady i Komisji służący realizacji programu haskiego mającego na celu wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, Dz.U. C 198 z 12.8.2005, str. 1.

([11]) Konferencja europejskich organów ochrony danych wydała opinię w dniu 24 stycznia 2006 r.; jest ona dostępna jako dok. 6329/06 na stronie register.consilium.europa.eu. Komitet konsultacyjny Rady Europy ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych przyjął w dniu 20 marca 2007 r. dokument zawierający jego wstępne uwagi, który jest dostępny pod adresem www.coe.int/dataprotection/.

([12]) Z niedawno wydanych zob. opinię EIOD z dnia 4 kwietnia 2007 r. w sprawie inicjatywy 15 państw członkowskich w celu przyjęcia decyzji Rady w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną, pkt 60.

([13]) Zalecenie nr R (87) 15 Komitetu Ministrów dla państw członkowskich regulujące wykorzystywanie danych osobowych w sektorze policyjnym, przyjęte w dniu 17 stycznia 1987 r. i dostępne pod adresem www.coe.int/dataprotection/.

([14]) Takich jak akty prawne regulujące działalność Europolu, Eurojustu oraz systemu informacji celnej trzeciego filara.

([15]) Takich jak niedawne inicjatywy dotyczące Europolu, konwencji z Prüm oraz dostępu organów ochrony porządku publicznego do bazy danych VIS.

przypadku danych dotyczących przelotu pasażera (PNR)) i z trzeciego filaru do pierwszego. Łatwo znaleźć pasujące przykłady: stosowanie listy „zakaz lotu", obejmującej osoby, którym należy odmówić wstępu na pokład samolotu, i ustanowionej przez linie lotnicze dla ochrony porządku publicznego do celów mieszczących się w ramach pierwszego filara (cele handlowe i związane z bezpieczeństwem lotu), a także wniosek dotyczący dostępu organów ochrony porządku publicznego do bazy danych VIS, ustanowionej jako narzędzie wspólnej polityki wizowej ([16]). Dlatego EIOD podkreśla, że zasady ochrony danych w pierwszym filarze muszą być stosowane również w trzecim filarze. Jednak szczególny charakter działań związanych z ochroną porządku publicznego sprawia, że mogą być konieczne przepisy dodatkowe lub specjalne ([17]).

14. Właściwe, spójne i mające szerokie zastosowanie gwarancje ochrony danych w trzecim filarze są kluczowe, nie tylko aby zagwarantować podstawowe prawo osób do ochrony danych, ale również aby wspierać skuteczność współpracy w zakresie ochrony porządku publicznego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

15. Z tego względu niniejsza opinia dokonuje oceny tego, na ile zmieniony wniosek w swym obecnym kształcie ustanawia właściwe przepisy dotyczące ochrony danych osobowych, zgodnie z art. 30 ust. 1 lit. b) TUE. Przeprowadzając tę ocenę, EIOD będzie się odnosił do pewnych zaleceń poczynionych w swych poprzednich opiniach. Niniejsza opinia dotyczyć będzie również tego, czy zmieniony wniosek respektuje międzynarodowe zobowiązania państw członkowskich wynikające z konwencji nr 108 Rady Europy oraz orzecznictwa Europejskiego Trybunału Praw Człowieka, a także z zasad określonych w zaleceniu nr R (87) 15 w sprawie wykorzystania danych osobowych w sektorze policyjnym. Ponadto EIOD rozważy, w jakim stopniu przepisy wniosku wpłynęłyby na skuteczność współpracy policyjnej i sądowej.

IV. **GŁÓWNE ZASTRZEŻENIA**

IV.1. **Możliwość stosowania do przetwarzania danych osobowych na użytek krajowy**

16. We wniosku znajduje się obecnie motyw zawierający stwierdzenie, że państwa członkowskie kierują się przepisami omawianej decyzji ramowej podczas przetwarzania danych na użytek krajowy, tak by już podczas ich pobierania *mogły* zostać spełnione warunki pozwalające na ich późniejsze przekazywanie (motyw 6a). Motyw ten jest próbą odpowiedzi na zastrzeżenia zgłoszone nie tylko przez EIOD w poprzednich opiniach, ale również przez wiele innych podmiotów. Parlament Europejski, konferencja organów ochrony danych osobowych, a nawet komitet konsultacyjny Rady Europy ds. konwencji o ochronie osób, w którego skład wchodzą przedstawiciele europejskich rządów odpowiedzialni za ochronę danych — wszystkie te podmioty jasno stwierdzały bowiem przy różnych okazjach, że możliwość stosowania omawianej decyzji ramowej do przetwarzania danych osobowych na użytek krajowy jest warunkiem koniecznym nie tylko do zapewnienia wystarczającego poziomu ochrony danych osobowych, ale również do umożliwienia skutecznej współpracy między organami ochrony porządku publicznego ([18]).

17. Jednak motyw jako taki nie może narzucać obowiązku, jeśli obowiązek ten nie jest jednoznacznie ustanowiony przepisami danej decyzji. Niestety, art. 1 (cel i zakres zastosowania) jednoznacznie ogranicza możliwość stosowania wniosku wyłącznie do danych wymienianych między państwami członkowskimi lub organami UE, które dopilnowują, aby „*w pełni przestrzegane były prawa i wolności podstawowe, a zwłaszcza aby nienaruszana była prywatność odnośnych osób, kiedy państwa członkowskie lub instytucje i organy […] przekazują sobie dane osobowe*".

18. Obecny projekt pozostawia zatem uznaniu państw członkowskich stosowanie jednolitych zasad ochrony danych do przetwarzania danych osobowych na użytek krajowy i nie zobowiązuje państw członkowskich do przestrzegania takich samych wspólnych standardów ochrony danych; wszystko to dotyczy dziedziny współpracy policyjnej i sądowej, w której zniesione zostać mają granice wewnętrzne. W związku z powyższym EIOD po raz kolejny podkreśla, że ewentualne istnienie odmiennych poziomów ochrony danych w różnych państwach członkowskich w ramach trzeciego filara byłoby rozwiązaniem:

— niespójnym z celem, jakim jest utworzenie przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w obrębie której obywatele poruszają się swobodnie i w której nastąpiło właściwe zbliżenie przepisów, zgodnie z art. 34 ust. 2 lit. b) TUE;

— niewłaściwym z punktu widzenia ochrony danych osobowych w świetle art. 30 ust. 1 lit. b) TUE;

([16]) Zob. wniosek dotyczący 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).

([17]) W tym samym duchu zob. również uzasadnienie zalecenia nr R (87) 15, pkt 37.

([18]) Zob. dokumenty wspomniane w przypisie 9.

— nieefektywnym i niewykonalnym dla organów ochrony porządku publicznego, które zostałyby niepotrzebnie obciążone koniecznością niemożliwego do przeprowadzenia rozróżniania między danymi przetwarzanymi na użytek krajowy a danymi przekazywanymi czy możliwymi do przekazania, które to dane w większości przypadków będą częścią tych samych akt ([19]).

19. EIOD zdecydowanie zaleca, aby prawodawca rozszerzył zakres stosowania przez zobowiązanie, a nie tylko zachęcenie, państw członkowskich do stosowania omawianej decyzji ramowej do przetwarzania danych osobowych na użytek krajowy. Ponadto brak jest przekonujących argumentów prawnych na poparcie poglądu, że stosowanie decyzji do danych przetwarzanych na użytek krajowy nie byłoby możliwe na mocy art. 34 TUE.

IV.2. **Ograniczenie celów dalszego przetwarzania danych osobowych**

20. Zasada ograniczenia celu jest jedną z podstawowych zasad ochrony danych. W szczególności konwencja nr 108 stanowi, że dane osobowe są „*gromadzone dla określonych i usprawiedliwionych celów i nie mogą być wykorzystywane w sposób niezgodny z tymi celami*" (art. 5 lit. b). Odstępstwa od tej zasady są dopuszczalne, tylko jeżeli przewiduje je prawo jako środek konieczny w społeczeństwie demokratycznym dla m.in. „zwalczania przestępczości" (art. 9). W swym orzecznictwie Europejski Trybunał Praw Człowieka jasno stwierdził, że odstępstwa te muszą być proporcjonalne, precyzyjne i przewidywalne, zgodnie z art. 8 ust. 2 europejskiej konwencji o prawach człowieka ([20]).

21. W obecnym wniosku przepisy o ograniczeniu celu są określone zarówno w art. 3, jak i art. 12. Art. 3 zezwala na dalsze przetwarzanie do celów, które nie są sprzeczne z celem, w jakim dane te zostały pobrane, jest zatem pod tym względem zgodny z podstawowymi zasadami ochrony danych.

22. Jednak art. 3 jest zbyt ogólnikowy i nie zawiera odpowiedniego ograniczenia celów przechowywania, którego wymaga się również na mocy wspomnianego powyżej art. 5 lit. b) konwencji nr 108. Nie można uznać celów zdefiniowanych przez ogólne odesłanie do celów tytułu VI Traktatu UE za jednoznaczne i legalne. Cel, jakim jest współpraca policyjna i sądowa, nie stanowi sam w sobie celu zgodnego z prawem ([21]), a już z pewnością celu jednoznacznego.

23. Art. 3 nie zawiera żadnego odstępstwa, które byłoby dozwolone zgodnie z art. 9 konwencji nr 108. Za to w art. 12 omawianego wniosku ustanawia się bardzo szerokie i niejasno zdefiniowane odstępstwa od zasady ograniczenia celu w odniesieniu do danych osobowych przekazanych lub udostępnionych przez inne państwo członkowskie. W artykule tym brak w szczególności jednoznacznego zapisu o warunku, że zastosowanie odstępstwa powinno wynikać z konieczności. Po drugie niejasne jest, czym są „inne postępowania […] administracyjne", w przypadku których art. 12 ust. 1 lit. b) zezwala na przetwarzanie danych osobowych zgromadzonych lub przekazanych w innym celu. Ponadto art. 12 ust. 1 lit. d) zezwala na przetwarzanie „w jakimkolwiek innym celu" uwarunkowane jedynie wyrażeniem zgody przez właściwy organ, który przekazał odnośne dane osobowe. W tym kontekście należy zauważyć, że w żadnych okolicznościach nie można uznać, iż zgoda organu przekazującego dane za zastępuje zgodę osoby, której te dane dotyczą, lub stanowi prawną podstawę do skorzystania z odstępstwa od zasady ograniczenia celu. EIOD pragnąłby w związku z tym podkreślić, że takie szerokie i otwarte odstępstwo nie spełnia podstawowych wymogów właściwej ochrony danych, a nawet przeczy podstawowym zasadom konwencji nr 108. EIOD zaleca zatem, aby prawodawca przeredagował stosowne przepisy.

24. Ostatnia uwaga dotyczy art. 12 ust. 2, który dopuszcza możliwość nadrzędności decyzji Rady dotyczących trzeciego filara względem ustępu 1 określającego właściwe warunki przetwarzania danych osobowych. EIOD zauważa, że sformułowanie tego ustępu jest bardzo ogólnikowe i nie odpowiada charakterowi decyzji ramowej Rady, będącej prawem ogólnym w odniesieniu do współpracy policyjnej i sądowej. Tego prawa ogólnego należy przestrzegać w odniesieniu do wszelkich przypadków przetwarzania danych osobowych w tej dziedzinie.

25. EIOD uważa, że obecne przepisy dotyczące dalszego przetwarzania danych osobowych naruszają podstawową zasadę ograniczenia celu i nie zapewniają nawet obowiązującego standardu określonego w konwencji nr 108. Z tego względu EIOD zaleca, aby prawodawca przeredagował stosowne przepisy w świetle obowiązujących międzynarodowych zasad ochrony danych i odpowiedniego orzecznictwa.

([19]) Bardziej szczegółowy wywód znajduje się w drugiej opinii EIOD, pkt 11–13.
([20]) Spośród skonsolidowanego orzecznictwa najbardziej dobitny tego przykład stanowi sprawa Rotaru przeciwko Rumunii.
([21]) Nie wystarczy wyjść z założenia, że policja w każdych okolicznościach i we wszystkich przypadkach działa w granicach obowiązujących ją przepisów.

IV.3. **Właściwa ochrona w przypadku wymiany danych osobowych z państwami trzecimi**

26. Konwencja nr 108 dotyczy również przekazywania danych państwom trzecim. Protokół dodatkowy odnoszący się do organów nadzoru i transgranicznych przepływów danych określa ogólną zasadę — podlegającą pewnym odstępstwom — zgodnie z którą przekazywanie danych osobowych stronie trzeciej jest dozwolone jedynie wtedy, gdy strona ta „zapewni wystarczający poziom ochrony danych, które mają zostać przekazane". Zasada „wystarczającego poziomu ochrony" była wdrażana i objaśniana w ramach wielu instrumentów prawnych Unii Europejskiej, nie tylko instrumentów z pierwszego filaru dotyczących ochrony danych, takich jak dyrektywa 95/46/WE ([22]), ale również instrumentów prawnych w ramach trzeciego filara, np. aktów prawnych ustanawiających Europol i Eurojust.

27. W motywie 12 obecnego wniosku stwierdza się, że w przypadku przekazywania danych osobowych państwom trzecim lub instytucjom międzynarodowym „dane te powinny z zasady być odpowiednio chronione". Ponadto art. 14 zezwala na przekazanie państwom trzecim lub instytucjom międzynarodowym danych otrzymanych od innego państwa członkowskiego, jeżeli organ, który te dane przekazał, wyraził zgodę na ich przekazanie zgodnie ze swoim prawem krajowym. Przepisy omawianego wniosku nie ustanawiają zatem konieczności zapewnienia odpowiedniego poziomu ochrony, nie przewidują żadnych wspólnych kryteriów ani mechanizmów oceny, czy ten poziom jest odpowiedni. Oznacza to, że każde państwo członkowskie będzie wedle własnego uznania oceniać poziom ochrony zapewniany przez dane państwo trzecie czy organizację międzynarodową. W związku z powyższym wykazy państw i organizacji międzynarodowych, które zapewniają odpowiedni poziom ochrony i którym przekazywanie danych jest dozwolone, będą się istotnie różnić pomiędzy poszczególnymi państwami członkowskimi.

28. Takie ramy prawne utrudniłyby również współpracę policyjną i sądową. Organy ochrony porządku publicznego danego państwa członkowskiego podejmując decyzję w sprawie przekazanego przez państwo trzecie wniosku dotyczącego pewnych akt karnych będą bowiem musiały nie tylko rozważyć, czy państwo to zapewnia odpowiedni poziom ochrony, ale również wziąć pod uwagę zgodę lub jej brak ze strony każdego z pozostałych (nawet 26) państw członkowskich, które wniosły wkład w te akta, państwa te zaś decyzję o zgodzie lub jej braku podejmą według własnej oceny odnośnego państwa trzeciego.

29. W tym kontekście art. 27 omawianego wniosku, dotyczący statusu względem umów z państwami trzecimi, wnosi jeszcze więcej niepewności, stanowiąc, że omawiana decyzja ramowa nie narusza żadnych obowiązków ani zobowiązań państw członkowskich lub Unii Europejskiej wynikających z dwu- lub wielostronnych umów z państwami trzecimi. Zdaniem EIOD w przepisie tym powinien się znaleźć wyraźny zapis, że jego stosowanie ogranicza się do obowiązujących umów i że umowy zawierane w przyszłości powinny być zgodne z przepisami omawianego wniosku.

30. EIOD uważa, że obecne przepisy dotyczące przekazywania danych osobowych państwom trzecim oraz organizacjom międzynarodowym nie są wystarczające, aby zapewnić ochronę danych osobowych i są niewykonalne dla organów ochrony porządku publicznego. Dlatego też EIOD ponownie stwierdza ([23]), że konieczne jest zapewnienie odpowiedniego poziomu ochrony danych w przypadku przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym i że należy ustanowić mechanizmy gwarantujące wspólne standardy oceny poziomu ochrony i koordynację decyzji w tej dziedzinie. Tę samą opinię wyraził wcześniej Parlament Europejski oraz komitet konsultacyjny Rady Europy ds. konwencji o ochronie osób.

IV.4. **Jakość danych**

31. Art. 5 konwencji nr 108 określa zasady zapewnienia jakości danych osobowych. Bardziej szczegółowe informacje zawarte są w aktach niemających wiążącego charakteru, takich jak zalecenie nr R (87) 15 oraz trzy dotychczas przeprowadzone oceny tego zalecenia.

32. Z porównania obecnego wniosku z wyżej wspomnianymi aktami prawnymi wynika jasno, że w zmienionej wersji zabrakło pewnych istotnych gwarancji, które w niektórych przypadkach przewidywał już pierwotny wniosek Komisji:

    — Art. 3 wniosku nie daje gwarancji, że dane są pozyskiwane oraz przetwarzane w sposób rzetelny, zgodnie z wymogiem zawartym w art. 5 konwencji nr 108.

([22]) W tym miejscu należy zauważyć, że Komisja stwierdziła ostatnio w swoim *Komunikacie z dnia 7 marca 2007 roku w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych*, że przepisy ustanowione w dyrektywie 95/46/WE w odniesieniu do przekazywania danych osobowych państwom trzecim są zasadniczo właściwe i nie wymagają zmiany.

([23]) Zob. zastrzeżenia już zasygnalizowane w pierwszej opinii, rozdział IV.8, i w drugiej opinii, pkt 22–23.

— Wniosek nie zawiera obecnie żadnych przepisów stanowiących — jak tego wymaga zasada 3.2 zalecenia nr R (87) 15 — że podział danych na różne kategorie odbywa się według stopnia ich ścisłości i wiarygodności i że należy czynić rozróżnienie między danymi opartymi na faktach, a tymi opartymi na opiniach lub osobistej ocenie ([24]). Brak takiego ogólnego wymogu może w istocie podważyć sens wymiany danych między organami policji, ponieważ nie będą one w stanie stwierdzić, czy dane można interpretować jako „dowód", „fakt", „informacje potwierdzone" czy „niepotwierdzone". Może to nie tylko zakłócać prowadzenie operacji w zakresie bezpieczeństwa i gromadzenie danych wywiadowczych, dla których to działań powyższe rozróżnienie ma istotne znaczenie, ale także utrudniać doprowadzenie do skazania przez sąd.

— Wniosek nie przewiduje rozróżnienia między różnymi kategoriami podmiotów danych (przestępcami, podejrzanymi, ofiarami, świadkami itp.) ani konkretnych gwarancji wobec danych odnoszących się do osób niebędących podejrzanymi, co jest sprzeczne z zasadą nr 2 zalecenia nr R (87) 15 i sprawozdań z jego oceny ([25]). I znowu — uczynienie takiego rozróżnienia jest konieczne nie tylko dla ochrony danych osobowych obywateli, ale również dla zapewnienia odbiorcom danych możliwości ich pełnego wykorzystania. Bez takiego rozróżnienia służby policji otrzymujące dane nie mogą od razu z nich skorzystać, lecz muszą najpierw stwierdzić, jaki jest charakter tych danych i w jaki sposób można je wykorzystać i udostępniać do różnych celów związanych z ochroną porządku publicznego.

— Okresowa weryfikacja danych przewidziana w art. 6 nie gwarantuje okresowej weryfikacji jakości danych ani oczyszczania policyjnych akt ze zbędnych lub nieścisłych danych i aktualizacji tych akt, czego wymaga zalecenie nr R (87) 15 ([26]). Znaczenie takiej weryfikacji dla ochrony danych jest oczywiste, jednak jest ona również kluczowa dla skutecznego działania służb policji. Stare i nieaktualne dane wywiadowcze są w najlepszym przypadku bezwartościowe, w najgorszym — prowadzą do przeznaczania zasobów na sprawy, które nie są i nie powinny być centralnym przedmiotem dochodzenia, kosztem aktualnych priorytetów.

— Jeśli okaże się, że dane osobowe otrzymane od innego państwa członkowskiego są nieścisłe, we wniosku nie przewidziano obowiązku ani mechanizmów ich poprawiania w państwie członkowskim, które je przekazało. Wypada znów powtórzyć, że kwestia ścisłości ma kluczowe znaczenie dla skuteczności działania policji i organów sądowych. Niemożność zagwarantowania jakości danych wpłynie niekorzystnie na użyteczność przekazywania danych jako narzędzia transgranicznej walki z przestępczością.

33. Z tego względu EIOD jest zdania, że przepisy odnoszące się do jakości danych zawarte we wniosku w jego obecnym kształcie nie są właściwe ani kompletne — zwłaszcza biorąc pod uwagę zalecenie nr R (87) 15, które uznają wszystkie państwa członkowskie — oraz że przepisy te nie zapewniają nawet poziomu ochrony wymaganego na mocy konwencji nr 108. Należy również przypomnieć po raz kolejny, że ścisłość danych osobowych leży w interesie zarówno porządku publicznego, jak i danej osoby ([27]).

IV.5. **Wymiana danych osobowych z organami innymi niż właściwe i podmiotami prywatnymi**

34. Zgodnie z zasadą nr 5 (przekazywanie danych) zalecenia nr R (87) 15 przekazywanie danych osobowych przez organy ochrony porządku publicznego innym organom publicznym lub podmiotom prywatnym powinno być dopuszczalne jedynie w pewnych ściśle określonych okolicznościach. Takie przepisy, które znajdowały się w pierwotnym wniosku Komisji i do których z zadowoleniem odnieśli się EIOD i Parlament Europejski, w obecnej wersji wniosku zostały wykreślone. Nowy tekst nie ustala zatem żadnych szczególnych gwarancji dotyczących przekazywania danych osobowych podmiotom prywatnym oraz organom niezwiązanym z ochroną porządku publicznego.

([24]) W pkt 52 uzasadnienia zalecenia stwierdza się, że *„możliwe powinno być dokonanie rozróżnienia między danymi potwierdzonymi a danymi niepotwierdzonymi, w tym oceną ludzkiego zachowania, między faktami a opiniami, między informacjami wiarygodnymi (i różnymi stopniami ich wiarygodności) a domysłami, między uzasadnionym powodem, by wierzyć, że informacje są ścisłe, a bezpodstawnym przekonaniem co do ich ścisłości"*. Zob. również drugą ocenę stosowności zalecenia nr R (87) 15 regulującego wykorzystanie danych osobowych w sektorze policyjnym (1998), pkt 5.1.

([25]) Zob. w szczególności pkt 5.2 drugiej oceny, wspomniany powyżej, oraz punkty 24–27 trzeciej oceny zalecenia nr R (87) 15 regulującego wykorzystanie danych osobowych w sektorze policyjnym (2002).

([26]) Zob. zasadę nr 7 (okres przechowywania i aktualizacja danych) oraz uzasadnienie, pkt 96–98.

([27]) Uzasadnienie zalecenia nr R (87) 15, pkt 74.

35. Ponadto możliwość dostępu organów ochrony porządku publicznego do danych osobowych kontrolowanych przez podmioty prywatne oraz dalszego wykorzystywania przez nie tych danych powinna podlegać dokładnie określonym warunkom i ograniczeniom. W szczególności, jak już wspomniał EIOD w swych poprzednich opiniach, decyzję o umożliwieniu dostępu do danych organom ochrony porządku publicznego należy podejmować oddzielnie dla każdego przypadku; dostęp taki powinien być możliwy w określonych okolicznościach, w określonym celu i podlegać prawnej kontroli państw członkowskich. Ostatnie wydarzenia, takie jak przyjęcie dyrektywy 2006/24/WE ([28]) w sprawie zatrzymywania danych, podpisanie ze Stanami Zjednoczonymi umowy w sprawie danych dotyczących przelotu pasażera ([29]) oraz umożliwienie organom ochrony porządku publicznego dostępu do danych przechowywanych przez SWIFT ([30]), potwierdzają fundamentalne znaczenie takich gwarancji. Szkoda, że wniosek w swym obecnym kształcie nie przewiduje żadnych szczególnych gwarancji dotyczących dostępu organów ochrony porządku publicznego do danych osobowych gromadzonych przez podmioty prywatne oraz dalszego wykorzystywania przez nie tych danych.

36. W związku z powyższym EIOD zauważa, że jeśli chodzi o wymianę danych osobowych z podmiotami prywatnymi oraz organami innymi niż właściwe, wniosek w obecnym kształcie nie respektuje zasad zalecenia nr R (87) 15 i nie podejmuje fundamentalnej kwestii dostępu organów ochrony porządku publicznego do danych osobowych kontrolowanych przez podmioty prywatne oraz dalszego wykorzystywania przez nie tych danych.

IV.6. **Inne merytoryczne zastrzeżenia**

37. Poza wyżej wspomnianymi zastrzeżeniami EIOD pragnąłby zwrócić uwagę prawodawcy na poniższe problemy, które w większości przypadków omówił już bardziej szczegółowo w swych poprzednich opiniach:

— Szczególne kategorie danych. Art. 7 zmienionego wniosku stoi w sprzeczności z zakazem przetwarzania „z zasady" określonym w art. 6 konwencji nr 108. Ponadto nie ma w nim odniesienia do danych osobowych dotyczących wyroków karnych, które niewątpliwe są wysoce użyteczne w kontekście współpracy policyjnej i sądowej, nie przewiduje się w nim również żadnych szczególnych gwarancji ochrony wobec danych biometrycznych i profili DNA.

— Zautomatyzowane decyzje dotyczące indywidualnych przypadków. EIOD z zadowoleniem przyjmuje fakt, że w art. 8 włącza się ten przepis do zmienionego wniosku.

— Protokoły i dokumentacja. Aby skutecznie służyć celowi weryfikacji, czy przetwarzanie danych jest w danym przypadku legalne, art. 11 powinien ustanawiać stosowne mechanizmy rejestrowania w protokołach i dokumentacji nie tylko wszelkich przypadków przetwarzania danych, ale również *wszelkich przypadków dostępu* do danych.

— Prawo do otrzymania powiadomienia. Art. 16 ma charakter niekompletny, gdyż brak w nim wzmianki o informacjach dotyczących tożsamości kontrolera i odbiorców. Ponadto sformułowanie w motywie 13 („może być konieczne, aby osobę, której dotyczą dane, poinformować o tym […]") określa przekazanie takiej informacji jako możliwość, nie zaś jeden z podstawowych obowiązków kontrolera.

— Prawo do zasięgnięcia informacji. Art. 17 ma charakter niekompletny, ponieważ możliwość zasięgnięcia informacji powinna dotyczyć także *celów* przetwarzania danych oraz obejmować powiadomienie *w zrozumiały sposób*. Ponadto wyjątki określone w ust. 2, jak w przypadku gdy udzielenie informacji „zagroziłoby […] innym interesom narodowym", są zbyt szerokie i nieprzewidywalne. Na koniec — nie istnieje żaden mechanizm gwarantujący, że skutkiem odwołania do organu nadzoru będzie udzielenie informacji, jeśli odmowa udzielenia tych informacji była niezgodna z prawem.

V. **NOWE KWESTIE WYNIKAJĄCE ZE ZMIENIONEGO KSZTAŁTU WNIOSKU**

38. Zmieniony wniosek zawiera, w stosunku do wniosku Komisji, całkiem nowy element. Obejmuje on działania instytucji i organów europejskich w ramach trzeciego filara (art. 1 ust. 2 omawianego wniosku). Zgodnie z motywem 20 dotyczy to przetwarzania danych przez Europol, Eurojust i system informacji celnej trzeciego filara. W art. 1 ust. 2 znajduje się wzmianka nie tylko o organach, lecz także instytucjach europejskich, co oznacza, że np. przetwarzanie danych w ramach Rady powinno podlegać

([28]) Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. 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 z 13.4.2006, str. 54).

([29]) 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 z 27.10.2006, str. 29).

([30]) Zob. opinię 10/2006 grupy roboczej art. 29 w sprawie przetwarzania danych osobowych przez Towarzystwo Światowej Finansowej Telekomunikacji Międzybankowej (SWIFT), dostępną pod adresem http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf, oraz opinię EIOD w sprawie roli Europejskiego Banku Centralnego w przypadku SWIFT, dostępną na stronie internetowej EIOD.

omawianej decyzji ramowej Rady. Niejasne jest, czy autorzy projektu planowali taki szeroki zakres stosowania, czy też zamierzali ograniczyć stosowanie omawianej decyzji do trzech organów wymienionych w motywie 20. Należałoby w każdym razie doprecyzować tekst, by uniknąć braku pewności prawnej.

39. W związku z powyższym nasuwa się uwaga bardziej ogólnej natury. Zdaniem EIOD sprawą najwyższej wagi jest zagwarantowanie właściwego poziomu ochrony danych w całym trzecim filarze, ponieważ tylko spełnienie tego warunku dostatecznie usprawniłoby swobodną wymianę informacji w przestrzeni wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych. Oznacza to również stosowanie ogólnych ram ochrony danych do europejskich organów działających w ramach trzeciego filara. EIOD podkreślał taką potrzebę już wcześniej, w IV części swojej opinii w sprawie wniosku dotyczącego decyzji Rady ustanawiającej Europol.

40. Ze względu jednak na skuteczne stanowienie prawa EIOD wyraża poważną wątpliwość co do sensu objęcia omawianą decyzją ramową Rady działań europejskich organów funkcjonujących w trzecim filarze. Pierwszy argument przeciwko temu szerokiemu zakresowi stosowania wiąże się z polityką legislacyjną. EIOD obawia się, ze włączenie organów europejskich do obecnego tekstu mogłoby spowodować, że dyskusje w Radzie skupią się na tym nowym elemencie, zamiast na merytorycznych przepisach dotyczących ochrony danych. Skomplikuje to proces legislacyjny. Drugi argument jest natury prawnej. Od początku wydaje się, że decyzja ramowa Rady — akt prawny o charakterze porównywalnym do dyrektywy w rozumieniu Traktatu WE — nie jest właściwym instrumentem prawnym, aby regulować prawa i obowiązki organów europejskich. Art. 34 TUE wprowadza ten instrument w celu zbliżania przepisów ustawowych i wykonawczych państw członkowskich. Istnieje w każdym razie spore ryzyko, że ta podstawa prawna zostanie podważona w trakcie procesu legislacyjnego lub później.

41. Podobny pogląd, również co do wyboru instrumentu prawnego, EIOD wyznaje w przypadku art. 26 projektu, który przewiduje ustanowienie nowego, wspólnego organu nadzoru, zastępującego istniejące organy prowadzące nadzór nad przetwarzaniem danych w ramach organów trzeciego filara. Sam w sobie zamiar ustanowienia takiego organu może wydawać się logiczny. Doprowadziłoby to być może do jeszcze większego usprawnienia systemu nadzoru, a ponadto zwiększyło spójność poziomu ochrony w obrębie organów ustanowionych w ramach trzeciego filara.

42. Nie ma jednak w obecnej chwili palącej potrzeby istnienia takiego nowego organu nadzoru. System nadzoru jako taki funkcjonuje zadowalająco. Co więcej przewodniczący Eurojustu wyraził zastrzeżenia co do stosowania tego systemu nadzoru wobec Eurojustu. Bez wchodzenia w szczegóły tych zastrzeżeń jasne jest, że włączenie tematu nadzoru nad organami UE do omawianej decyzji ramowej Rady jeszcze bardziej utrudniłoby proces legislacyjny. Dodatkowo takie podejście byłoby niespójne z innymi wnioskami w tej dziedzinie, które są obecnie przedmiotem dyskusji ([31]) lub zostały niedawno przyjęte ([32]).

43. W skrócie — EIOD zaleca niewprowadzanie przepisów dotyczących przetwarzania danych przez organy UE do tekstu omawianej decyzji ramowej Rady. Opinia taka jest podyktowana względami skutecznego stanowienia prawa. Ważne jest, by wszystkie wysiłki w Radzie koncentrowały się na merytorycznych przepisach dotyczących ochrony danych, tak by obywatele zyskali niezbędną ochronę.

VI. **WNIOSKI**

44. EIOD przychylnie odnosi się do dostarczenia nowego impulsu przez prezydencję niemiecką. Jak już wielokrotnie podkreślali EIOD i inne właściwe podmioty, przyjęcie ogólnych ram ochrony danych w trzecim filarze jest konieczne dla wsparcia rozwoju przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której prawo obywateli do ochrony danych osobowych podlega jednakowym gwarancjom, a współpraca między organami ochrony porządku publicznego może odbywać się ponad granicami państwowymi.

45. Zmieniony wniosek nie spełnia jednak żadnego z tych założeń. W istocie, przy braku wysokiego i szeroko stosowanego poziomu ochrony danych wymiana informacji nadal podlega w myśl wniosku różnym krajowym „regułom pochodzenia" i „podwójnym normom", które wywierają znaczny niekorzystny wpływ na skuteczność współpracy w zakresie ochrony porządku publicznego, nie służąc przy tym poprawie ochrony danych osobowych.

([31]) Np. niedawny wniosek Komisji ustanawiający Europejski Urząd Policji, COM(2006)817 wersja ostateczna.

([32]) Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, str. 4).

46. Żeby posłużyć się konkretnym przykładem, powyższa sytuacja oznaczałaby to, że organ ochrony porządku publicznego na poziomie krajowym lub unijnym zajmując się aktami w sprawie karnej, na które składają się informacje otrzymane od różnych organów krajowych, organów innych państw członkowskich i organów UE, musiałby stosować różne zasady przetwarzania w odniesieniu do różnych elementów informacji, w zależności od tego czy: dane osobowe zebrano w kraju czy nie; czy każdy z organów, które przekazały dane, wyraził zgodę na ich wykorzystanie w zamierzonym celu; czy dane przechowywane są zgodnie z terminami określonymi w stosownych przepisach każdego z organów przekazujących dane; czy ograniczenie dalszego przetwarzania zgłoszone przez każdy z organów przekazujących dane nie uniemożliwia przetwarzania; czy w razie wniosku ze strony państwa trzeciego każdy z organów przekazujących dane wydał zgodę na podstawie własnej oceny tego państwa trzeciego pod katem zapewnienia odpowiedniego poziomu ochrony lub zgodnie ze zobowiązaniami międzynarodowymi. Ponadto poziom ochrony obywateli i ich prawa są ogromnie zróżnicowane, a wspomniana ochrona i prawa podlegają różnym szerokim odstępstwom, w zależności od państwa członkowskiego, w którym odbywa się przetwarzanie.

47. Poza tym EIOD z żalem zauważa, że jakość omawianego tekstu pod względem prawnym nie jest zadowalająca i że wniosek wnosi do sprawy dodatkowe zawiłości, rozszerzając możliwość stosowania omawianej decyzji ramowej do Europolu, Eurojustu oraz systemu informacji celnej trzeciego filara i proponując stworzenie wspólnego organu nadzoru na podstawie niewłaściwie wybranego instrumentu prawnego.

48. Zaniepokojenie EIOD budzi fakt, że w obecnym tekście nie ma już kluczowych przepisów dotyczących ochrony danych osobowych, które to przepisy zawierał wniosek Komisji. Usunięcie tych przepisów znacznie osłabia poziom ochrony obywateli. Po pierwsze, wniosek nie wnosi wartości dodanej w stosunku do konwencji nr 108, co uczyniłoby jego przepisy właściwymi z punktu widzenia ochrony danych, zgodnie z wymogiem zawartym w art. 30 ust. 1 TUE. Po drugie, pod wieloma względami nie gwarantuje również poziomu ochrony wymaganego przez konwencję nr 108. Z tej przyczyny EIOD uważa, że wniosek wymagałby znacznego udoskonalenia, zanim mógłby stać się podstawą dyskusji nad właściwymi ogólnymi ramami ochrony danych w trzecim filarze. Te udoskonalenia muszą dać pewność, że te ogólne ramy:

— wnoszą wartość dodaną w stosunku do konwencji nr 108 przez ustanowienie stosownych przepisów dotyczących ochrony danych osobowych zgodnie z wymogiem art. 30 ust. 1 TUE;

— mogą być stosowane do przetwarzania danych osobowych na użytek krajowy przez organy ochrony porządku publicznego;

— są spójne z zasadami ochrony danych w pierwszym filarze, jednak uwzględniają również w razie potrzeby szczególny charakter działań związanych z ochroną porządku publicznego;

— są zgodne z zasadami określonymi w konwencji nr 108 oraz zaleceniu nr R (87) 15, w szczególności jeśli chodzi o:

  — ograniczenie celów dalszego przetwarzania danych osobowych;

  — jakość danych, w tym rozróżnienie między różnymi kategoriami podmiotów danych (przestępców, podejrzanych, ofiar, świadków itp.), ocenę zróżnicowanego stopnia ścisłości i wiarygodności danych osobowych, mechanizmy zapewniające okresową weryfikację i poprawianie;

  — warunki przekazywania danych osobowych organom innym niż właściwe i podmiotom prywatnym, a także dostępu organów ochrony porządku publicznego do danych osobowych kontrolowanych przez podmioty prywatne oraz dalszego wykorzystywania przez nie tych danych;

— zapewniają odpowiedni poziom ochrony podczas wymiany danych osobowych z państwami trzecimi, również w odniesieniu do umów międzynarodowych;

— poruszają również inne kwestie wspomniane w niniejszej i poprzednich opiniach EIOD.

49. EIOD jest świadomy, jak trudno jest osiągnąć jednomyślność w Radzie. Jednak taka procedura podejmowania decyzji nie może usprawiedliwiać podejścia opierającego się na znalezieniu najniższego wspólnego mianownika, którego rezultatem byłoby naruszenie podstawowych praw obywateli UE i zmniejszenie skuteczności ochrony porządku publicznego.

Sporządzono w Brukseli, dnia 27 kwietnia 2007 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych