OPINIA EUROPEJSKIEGO INSPEKTORA OCHRONY DANYCH

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 (COM (2005) 475 wersja ostateczna)

(2006/C 47/12)

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**

Konsultacje z Europejskim Inspektorem Ochrony Danych

1. Pismem z dnia 4 października 2005 r. Komisja przesłała Europejskiemu Inspektorowi Ochrony Danych (EIOD) wniosek dotyczący decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. EIOD rozumie, że pismo to oznacza prośbę o opinię dla instytucji i organów wspólnotowych, zgodnie z art. 28 ust. 2 rozporządzenia nr 45/2001/WE. EIOD uważa, że należy uwzględnić niniejszą opinię w preambule do decyzji ramowej.

Znaczenie omawianego wniosku

2. EIOD podkreśla znaczenie omawianego wniosku z punktu widzenia podstawowych praw i wolności osób fizycznych do ochrony danych osobowych. Przyjęcie omawianego wniosku stanowiłoby znaczący krok w zakresie ochrony danych osobowych w ważnej dziedzinie, która szczególnie wymaga spójnego i skutecznego mechanizmu ochrony danych osobowych na szczeblu Unii Europejskiej.

3. W związku z tym EIOD podkreśla, że współpraca policyjna i sądowa pomiędzy państwami członkowskimi, będąca jednym z elementów procesu stopniowego tworzenia obszaru wolności, bezpieczeństwa i sprawiedliwości, ma coraz większe znaczenie. Program Haski wprowadził zasadę dostępności w celu usprawnienia transgranicznej wymiany informacji istotnych dla ochrony porządku publicznego Zgodnie z Programem Haskim ([1]), sam fakt, że informacja przekracza granice, nie powinien już mieć znaczenia. Wprowadzenie zasady dostępności odzwierciedla bardziej ogólną tendencję do ułatwiania wymiany informacji istotnych dla ochrony porządku publicznego (patrz na przykład: tzw. konwencja z Prüm ([2]), podpisana przez siedem państw członkowskich, oraz wniosek Szwecji dotyczący decyzji ramowej w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ochrony porządku publicznego ([3])). W ten sam sposób można spojrzeć na niedawne zatwierdzenie przez Parlament Europejski dyrektywy Parlamentu Europejskiego i Rady w sprawie zatrzymywania danych w zakresie łączności ([4]). Zmiany te wymagają przyjęcia instrumentu prawnego, który zagwarantuje skuteczną ochronę danych osobowych we wszystkich państwach członkowskich Unii Europejskiej w oparciu o wspólne normy.

([1]) Str. 18 programu.

([2]) Konwencja pomiędzy Królestwem Belgii, Republiką Federalną Niemiec, Królestwem Hiszpanii, Republiką Francuską, Wielkim Księstwem Luksemburga, Królestwem Niderlandów i Republiką Austrii w sprawie zwiększenia współpracy transgranicznej, szczególnie w zakresie zwalczania terroryzmu, przestępczości transgranicznej i nielegalnej migracji. Prüm (Niemcy), 27 maja 2005 r.

([3]) Inicjatywa Królestwa Szwecji mająca na celu przyjęcie decyzji ramowej w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ochrony porządku publicznego państw członkowskich Unii Europejskiej, w szczególności w odniesieniu do poważnych przestępstw, w tym aktów terroryzmu (Dz.U. C 281).

([4]) Na podstawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie w sprawie zatrzymywania przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej/zatrzymywania danych przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej zmieniającej dyrektywę 2002/58/WE (COM (2005) 438 wersja ostateczna).

4. EIOD zwraca uwagę na fakt, że obecne ogólne ramy prawne w zakresie ochrony danych w tej dziedzinie są niewystarczające. Przede wszystkim dyrektywa 95/46/WE nie ma zastosowania do przetwarzania danych osobowych w przypadku rodzajów działalności, które nie są objęte zakresem prawa wspólnotowego, takich jak rodzaje działalności przewidziane w tytule VI traktatu o Unii Europejskiej (art. 3 ust. 2 dyrektywy). Pomimo że w większości państw członkowskich zakres przepisów wykonawczych jest szerszy, niż wymaga tego sama dyrektywa, i nie wyłącza przetwarzania danych do celów ochrony porządku publicznego, przepisy krajowe w tym zakresie znacznie różnią się od siebie. Ponadto konwencja nr 108 Rady Europy ([1]), która wiąże wszystkie państwa członkowskie, nie zapewnia wystarczająco szczegółowej ochrony, zatwierdzonej już w chwili przyjęcia dyrektywy 95/46/WE. Co więcej, żaden z tych dwóch instrumentów prawnych nie uwzględnia szczególnego charakteru wymiany danych przez organy policyjne i sądowe ([2]).

Przyczynienie się do sukcesu samej współpracy

5. Skuteczna ochrona danych osobowych ma znaczenie nie tylko dla osób, których dane dotyczą, ale ma również korzystny wpływ na skuteczność samej współpracy policyjnej i sądowej. Pod wieloma względami interesy te są zbieżne.

6. Należy pamiętać, że przedmiotowe dane osobowe są często danymi wrażliwymi i że zostały one uzyskane przez organy policyjne i sądowe w wyniku śledztwa prowadzonego w danej sprawie. Organy będą bardziej skłonne do wymiany tego rodzaju danych z organami innych państw członkowskich, gdy będą miały pewność, że poziom ochrony w innym państwie członkowskim jest wystarczający. EIOD wymienia poufność i bezpieczeństwo danych oraz ograniczenia dostępu do danych i ich dalszego wykorzystywania jako istotne elementy ochrony danych.

7. Ponadto wysoki poziom ochrony danych może zapewnić ścisłość i wiarygodność danych osobowych. Przy wymianie danych pomiędzy organami policyjnymi lub sądowymi ich ścisłość i wiarygodność mają jeszcze większe znaczenie, zwłaszcza że w wyniku kolejnych operacji wymiany i przekazywania danych pomiędzy organami ochrony porządku publicznego ostatecznie są one przetwarzane daleko od ich źródła i bez kontekstu, w którym były pierwotnie zebrane i wykorzystane. Zazwyczaj organy otrzymujące dane nie znają dodatkowych okoliczności i muszą w pełni polegać na samych danych.

8. Harmonizacja krajowych zasad w zakresie danych osobowych w dziedzinie policji i wymiaru sprawiedliwości, w tym odpowiednie zabezpieczenia dotyczące ochrony tych danych, mogą zatem zwiększać wzajemne zaufanie oraz skuteczność samej wymiany.

Poszanowanie zasad ochrony danych w połączeniu z zestawem dodatkowych zasad

9. Przy wielu okazjach podkreślano potrzebę i znaczenie omawianego wniosku. Podczas wiosennej konferencji europejskich organów ochrony danych, która odbyła się w kwietniu 2005 r. w Krakowie, przyjęto oświadczenie i dokument określający stanowisko wzywające do przyjęcia nowych ram prawnych mających zastosowanie do działalności objętych trzecim filarem. Te nowe ramy prawne powinny nie tylko być zgodne z zasadami ochrony danych, zgodnie z dyrektywą 95/46/WE — należy zagwarantować spójność ochrony danych w ramach Unii Europejskiej — ale również określić zestaw dodatkowych zasad uwzględniających szczególny charakter dziedziny ochrony porządku publicznego ([3]). EIOD z zadowoleniem przyjmuje fakt, że omawiany wniosek uwzględnia te zagadnienia: jest zgodny z zasadami ochrony danych, określonymi zgodnie z dyrektywą 95/46/WE i przewiduje zestaw dodatkowych zasad.

10. Niniejsza opinia będzie stanowić analizę zakresu, w jakim przedstawiona wersja jest możliwa do przyjęcia z punktu widzenia ochrony danych, z należytym uwzględnieniem szczególnego kontekstu ochrony danych w dziedzinie ochrony porządku publicznego. Z jednej strony przedmiotowe dane są często danymi wrażliwymi (patrz pkt 6 niniejszej opinii), a z drugiej strony istnieje silna presja, by były one dostępne organom ochrony porządku publicznego w celu zapewnienia ich skutecznego działania, co może obejmować ochronę życia i bezpieczeństwa fizycznego osób. EIOD uważa, że zasady ochrony danych powinny odpowiadać uzasadnionym potrzebom ochrony porządku publicznego, ale powinny także chronić podmioty danych przed nieuzasadnionym przetwarzaniem i dostępem do danych ich dotyczących. Aby uzyskać zgodność z zasadą proporcjonalności, rozwiązanie prawodawcy europejskiego powinno odzwierciedlać dwa potencjalnie sprzeczne interesy publiczne. W związku z tym, EIOD przypomina, że często interesy te są zbieżne.

Kontekst tytułu VI traktatu o Unii Europejskiej

11. W końcu należy wspomnieć, że omawiany wniosek stanowi część tytułu VI traktatu o Unii Europejskiej, czyli tzw. trzeciego filara. Możliwości działania prawodawcy europejskiego są zatem wyraźnie ograniczone przez ograniczenia kompetencji prawodawczych Unii wobec podmiotów wymienionych w art. 30 i 31, ograniczenia w zakresie procedury prawodawczej, która nie obejmuje pełnego udziału Parlamentu Europejskiego, oraz ograniczenia dotyczące kontroli sądowej ze względu na to, że kompetencje Europejskiego Trybunału Sprawiedliwości wynikające z art. 35 TUE są niepełne. Ograniczenia te wymagają jeszcze dokładniejszej analizy tekstu wniosku.

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

([2]) W 1987 roku Rada Europy wydała zalecenie nr R (87) 15 regulujące wykorzystanie danych osobowych w sektorze policji, ale zalecenie to ze swojej natury nie jest wiążące dla państw członkowskich.

([3]) Patrz w takim samym zakresie „EIOD doradza Instytucjom Wspólnoty w sprawie wniosków legislacyjnych i związanych z nimi dokumentów", 18 marca 2005 r., opublikowano na stronie www.edps.eu.int.

II. KONTEKST: WYMIANA INFORMACJI NA PODSTAWIE ZASADY DOSTĘPNOŚCI, ZATRZYMYWANIE DANYCH I SZCZEGÓLNE RAMY PRAWNE DLA SYSTEMÓW SIS II I VIS

II.1 Zasada dostępności

12. Wniosek jest ściśle powiązany z wnioskiem dotyczącym decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności (COM(2005) 490 wersja ostateczna). Ten drugi wniosek ma na celu wdrożenie zasady dostępności i tym samym zapewnienie, że informacje dostępne właściwym organom państwa członkowskiego w związku z walką z przestępczością zostaną przekazane równoważnym organom innych państw członkowskich. Powinno to doprowadzić do zniesienia granic wewnętrznych w zakresie wymiany takich informacji poprzez objęcie jej jednolitymi warunkami w całej Unii.

13. Bliski związek pomiędzy tymi dwoma wnioskami wynika z faktu, że informacje istotne dla ochrony porządku publicznego obejmują w szerokim zakresie dane osobowe. Prawodawstwa w zakresie wymiany informacji istotnych dla porządku publicznego nie można przyjąć bez zabezpieczenia odpowiedniej ochrony danych osobowych. Jeżeli działanie na szczeblu Unii Europejskiej doprowadzi do zniesienia granic wewnętrznych w zakresie wymiany takich informacji, ochrona danych osobowych nie może być już regulowana tylko prawem krajowym. Do zadań instytucji europejskich dodano zagwarantowanie ochrony danych osobowych na terytorium Unii bez granic wewnętrznych. Zadanie to zostało wyraźnie określone w art. 30 ust. 1 lit. b) TUE, a wynika ono z obowiązku Unii w zakresie przestrzegania praw podstawowych (art. 6 TUE). Ponadto:

— w art. 1 ust. 2 niniejszego wniosku wyraźnie stwierdza się, że państwa członkowskie nie mogą już ograniczać bądź zakazywać transgranicznego przepływu informacji z powodów związanych z ochroną danych osobowych.

— wniosek dotyczący decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności obejmuje kilka odniesień do niniejszego wniosku.

14. EIOD zaznacza, że należy przyjąć decyzję ramową Rady w sprawie wymiany informacji w ramach zasady dostępności wyłącznie pod warunkiem jednoczesnego przyjęcia decyzji ramowej w sprawie ochrony danych osobowych. Jednak omawiany wniosek dotyczący decyzji ramowej Rady w sprawie ochrony danych jest ważny sam w sobie, a jego przyjęcie jest niezbędne nawet w przypadku braku instrumentu prawnego dotyczącego dostępności. Kwestia ta została podkreślona w sekcji I niniejszej opinii.

15. W takim przypadku EIOD przeanalizuje obydwa wnioski w dwóch odrębnych opiniach. Wynika to także z przyczyn praktycznych. Nie ma bowiem gwarancji, że wnioski będą omawiane wspólnie i w tym samym tempie przez Radę i Parlament Europejski.

II.2 Zatrzymywanie danych

16. Dnia 26 września 2005 r. EIOD przedstawił swoją opinię na temat wniosku dotyczącego dyrektywy w sprawie zatrzymywania danych w zakresie łączności ([1]). W opinii tej EIOD zwrócił uwagę na kilka istotnych braków we wniosku i zaproponował dodanie do dyrektywy konkretnych przepisów dotyczących dostępu do ruchu oraz danych dotyczących lokalizacji przez właściwe organy, a także przepisów dotyczących dalszego wykorzystywania tych danych, oraz dodanie dalszych zabezpieczeń w zakresie ochrony danych. Tekst dyrektywy w wersji przyjętej przez Parlament Europejski i Radę zawiera ograniczony i w żadnym wypadku niewystarczający przepis dotyczący ochrony danych oraz bezpieczeństwa danych oraz jeszcze bardziej niewystarczający przepis dotyczący dostępu, który przekazuje prawu krajowemu możliwość wydawania środków dotyczących dostępu, z zastrzeżeniem odpowiednich przepisów prawa Unii Europejskiej lub międzynarodowego prawa publicznego.

17. W związku z zatwierdzeniem dyrektywy w sprawie zatrzymywania danych w zakresie łączności kwestia ustanowienia ram prawnych dla ochrony danych w ramach trzeciego filaru staje się jeszcze pilniejsza. Przyjmując dyrektywę, prawodawca wspólnotowy zobowiązuje dostawców usług telekomunikacyjnych i internetowych do zatrzymywania danych do celów ochrony porządku publicznego bez stosowania koniecznych i odpowiednich zabezpieczeń w zakresie ochrony osób, których dane dotyczą. Ochrona nie jest jednak kompletna, ponieważ dyrektywa nie reguluje (w wystarczającym zakresie) kwestii dostępu do danych ani ich dalszego wykorzystywania po ich użyciu przez właściwe organy ochrony porządku publicznego.

18. Omawiany wniosek w znaczącym stopniu uzupełnia powstałą lukę, jako że ma zastosowanie do dalszego wykorzystywania danych po ich użyciu przez organy ochrony porządku publicznego. EIOD ubolewa, że niniejszy wniosek nie reguluje także kwestii dostępu do tych danych. W przeciwieństwie do sytuacji dotyczącej systemów SIS II i VIS (patrz sekcja II.3 niniejszej opinii), kwestia ta jest pozostawiona w gestii prawodawcy krajowego.

II.3 Przetwarzanie danych w ramach systemów SIS II i VIS

19. Obecnie Unia Europejska wykorzystuje lub rozwija kilka systemów informacyjnych na dużą skalę (Eurodac, SIS II, VIS) i dąży do osiągnięcia synergii pomiędzy tymi systemami. Istnieje także coraz częstsza tendencja do przyznawania szerszego dostępu do tych systemów w celach ochrony porządku publicznego. Te daleko idące zmiany powinny uwzględniać, zgodnie z Programem Haskim, „potrzebę osiągnięcia równowagi pomiędzy celami ochrony porządku publicznego a ochroną podstawowych praw osób fizycznych".

([1]) Opinia Europejskiego Inspektora Ochrony Danych 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), opublikowana na stronie

20. W swojej opinii z dnia 19 października 2005 r. na temat wniosków dotyczących Systemu Informacyjnego Schengen drugiej generacji (SIS II) [1], EIOD zwrócił uwagę na niektóre elementy dotyczące równoczesnego stosowania zasad ogólnych (*lex generalis*) i zasad bardziej szczególnych (*lex specialis)* w zakresie ochrony danych. Niniejszy wniosek można uznać za *lex generalis,* czyli prawo zastępujące konwencję nr 108 w ramach trzeciego filaru [2].

21. W tym kontekście EIOD podkreśla, że wniosek przewiduje ogólne ramy ochrony danych w ramach konkretnych instrumentów, takich jak część SIS II dotycząca trzeciego filaru oraz dostęp do Systemu Informacji Wizowej przez organy ochrony porządku publicznego [3].

III. GŁÓWNA CZĘŚĆ WNIOSKU

III.1 Wspólne normy mające zastosowanie do wszelkich operacji przetwarzania danych

Punkt wyjścia

22. Zgodnie ze swoim art. 1 ust. 1 wniosek ma określić wspólne normy w celu zapewnienia ochrony danych osobowych podczas działań prowadzonych w ramach współpracy policyjnej i sądowej w sprawach karnych. Art. 1 ust. 1 należy odczytywać w związku z art. 3 ust. 1, w którym stwierdza się, że wniosek ma zastosowanie do przetwarzania danych osobowych (…) przez właściwe organy do celów zapobiegania, dochodzenia, wykrywania i ścigania przestępstw.

23. Z przepisów tych wynika, że wnioskowana decyzja ramowa składa się z dwóch głównych elementów: określa wspólne normy i ma zastosowanie do wszelkich operacji przetwarzania danych do celów ochrony porządku publicznego, nawet gdy dane te nie zostały przekazane lub udostępnione przez właściwe organy innych państw członkowskich.

24. EIOD podkreśla znaczenie tych dwóch zagadnień. Ambitnym celem omawianego wniosku powinno być ustalenie ram prawnych dla ochrony danych, które w pełni uzupełniałyby ramy prawne już obowiązujące w pierwszym filarze. Jedynie w przypadkach, gdy warunek ten jest spełniony, Unia Europejska całkowicie wypełnia swój obowiązek wynikający z art. 6 ust. 2 TUE dotyczący poszanowania praw podstawowych zagwarantowanych w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności.

Wspólne normy

25. W odniesieniu do pierwszego elementu: niniejszy wniosek ma na celu zapewnienie, że obowiązujące zasady ochrony danych będą stosowane w dziedzinie objętej trzecim filarem. Ponadto przewiduje wspólne normy określające te zasady, mając na uwadze ich zastosowanie w tej dziedzinie. EIOD podkreśla znaczenie tych aspektów wniosku. Odzwierciedlają one szczególny i wrażliwy charakter przetwarzania danych w tej dziedzinie. EIOD przywiązuje szczególną wagę do wprowadzenia zasady rozróżnienia pomiędzy danymi osobowymi kategorii osób jako zasady ochrony danych w dziedzinie współpracy policyjnej i sądowej w sprawach karnych, oprócz obowiązujących zasad ochrony danych (art. 4 ust. 4). EIOD uważa, że zasada sama w sobie oraz jej skutki prawne dla osób, których dane dotyczą powinny być określone w sposób bardziej szczegółowy (patrz pkt 88-92 niniejszej opinii).

26. Zasady muszą mieć zastosowanie w różnych sytuacjach, więc nie mogą być zbyt szczegółowe. Z drugiej jednak strony powinny one zapewniać obywatelowi konieczną pewność prawną oraz odpowiednią ochronę jego danych osobowych. EIOD jest zdania, że wniosek w ogólnym zakresie zachowuje równowagę pomiędzy tymi dwoma potencjalnie sprzecznymi wymogami prawodawczymi. Przepisy pozostawiają swobodę wyboru w razie potrzeby, ale w większości dziedzin są wystarczająco szczegółowe, by zapewnić ochronę obywatela.

27. W niektórych jednak kwestiach wniosek jest zbyt elastyczny i nie przewiduje niezbędnych zabezpieczeń. Na przykład w art. 7 ust. 1 wniosek przewiduje ogólny wyjątek od zabezpieczeń, pod jedynym warunkiem „przewidzianym w innych przepisach". Pozostawienie tak szerokiej swobody decydowania na okres dłuższy niż jest to konieczne dla planowanego celu byłoby nie tylko niezgodne z podstawowym prawem ochrony danych, ale również miałoby szkodliwy wpływ na podstawową potrzebę harmonizacji ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

28. Wyjątki, w razie potrzeby, powinny ograniczać się do krajowych lub europejskich przepisów prawnych, wydanych w celu ochrony konkretnych interesów publicznych. Te interesy publiczne należy wyszczególnić w art. 7 ust. 1.

29. Prowadzi to do następnego zagadnienia: W przypadku gdy jakikolwiek inny instrument prawny na podstawie tytułu VI traktatu UE przewiduje bardziej szczegółowe warunki lub ograniczenia dla przetwarzania lub dostępu do danych, zastosowanie powinny mieć przepisy bardziej szczegółowe jako *lex specialis*. W art. 17 niniejszego wniosku przewidziano odstępstwa od art. 12-15, w przypadku gdy bardziej szczegółowe przepisy na podstawie tytułu VI ustanawiają szczególne warunki przekazywania danych. Stanowi to odzwierciedlenie ogólnego charakteru wniosku (jak wyjaśniono powyżej), ale nie

[1] Pkt 2.2.4 opinii.

[2] Konwencja Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, 28 stycznia 1981 r.

[3] Wniosek dotyczący decyzji Rady dotyczącej dostępu w celach konsultacyjnych do Systemu Informacji Wizowej przez organy państw członkowskich odpowiedzialne za bezpieczeństwo wewnętrzne i przez Europol do celów zapobiegania, dochodzenia, wykrywania i ścigania przestępstw terrorystycznych i innych poważnych przestępstw (COM (2005) 600 wersja ostateczna), wydany w dniu 24 listopada 2005 r. EIOD zamierza wydać opinię na temat tego wniosku na początku roku 2006.

wyczerpuje wszystkich możliwości. EIOD uważa, że art. 17 powinien:

— być opracowany w sposób bardziej ogólny: jeżeli istnieją bardziej szczegółowe przepisy regulujące którykolwiek aspekt przetwarzania danych (nie tylko przekazywanie danych), zastosowanie mają przepisy bardziej szczegółowe;

— zawierać zabezpieczenie stanowiące, że odstępstwa nie mogą obniżać poziomu ochrony.

Stosuje się do wszelkiego rodzaju przetwarzania danych

30. W odniesieniu do drugiego elementu: idealnym rozwiązaniem byłoby objęcie każdej czynności zbierania i przetwarzania danych w ramach trzeciego filaru.

31. Istotnym czynnikiem umożliwiającym osiągnięcie celu decyzji ramowej jest, by jej zakres obejmował wszystkie dane policyjne i sądowe, nawet jeżeli nie są one przekazywane ani udostępniane przez właściwe organy innych państw członkowskich.

32. Jest to jeszcze bardziej istotne, jako że ograniczenie zakresu do danych przekazywanych lub udostępnianych właściwym organom innych państw członkowskich sprawiłoby, że dziedzina stosowania decyzji ramowej byłaby szczególnie niepewna i nieokreślona, co stałoby w sprzeczności z jej podstawowym celem ([1]). Spowodowałoby to szkodę dla pewności prawnej osób fizycznych. W zwykłych okolicznościach nikt nie potrafi określić z wyprzedzeniem, w chwili zbierania lub przetwarzania danych osobowych, czy dane te będą podlegały wymianie informacji z właściwymi organami innych państw członkowskich. W związku z tym EIOD odnosi się do zasady dostępności i zniesienia granic wewnętrznych w celu wymiany danych istotnych dla ochrony porządku publicznego.

33. Poza tym EIOD zauważa, że wniosek nie ma zastosowania w przypadku:

— przetwarzania danych w ramach drugiego filaru traktatu UE (wspólna polityka zagraniczna i obronna).

— przetwarzania danych przez służby wywiadowcze oraz dostępu tych służb do tych danych, gdy są one przetwarzane przez właściwe organy lub inne strony (wynika to z art. 33 TUE).

W tych dziedzinach prawo krajowe powinno zapewniać odpowiednią ochronę podmiotów danych. Przy ocenie wniosku należy uwzględnić tę niepełną ochronę na szczeblu UE ([2]): jako że nie wszystkie operacje przetwarzania danych w dziedzinie ochrony porządku publicznego mogą być objęte zakresem wniosku, prawodawca powinien zapewnić jeszcze skuteczniejszą ochronę w dziedzinach, których wniosek nie obejmuje.

III.2 **Podstawa prawna**

34. W motywach wniosku dotyczącego decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności wspomniana jest podstawa prawna, a mianowicie art. 30 ust. 1 lit. b). Natomiast w omawianym wniosku nie określono, który przepis art. 30 lub 31 stanowi jego podstawę prawną.

35. Chociaż do obowiązków EIOD, jako doradcy w zakresie prawa Unii Europejskiej, nie należy wybór podstawy prawnej wniosku, użytecznym wydaje się założenie, że podstawę prawną także niniejszego wniosku mógłby stanowić art. 30 ust. 1 lit. b). Ponadto podstawę wniosku mógłby stanowić również art. 31 ust. 1 lit. c) TUE i powinien on mieć w całości zastosowanie w sytuacjach krajowych, pod warunkiem że jest to konieczne, by usprawnić współpracę policyjną i sądową pomiędzy państwami członkowskimi. W związku z tym EIOD ponownie podkreśla, że wszystkie dane osobowe, które zostały zebrane, zachowane, przetworzone lub przeanalizowane do celów ochrony porządku publicznego mogą, zwłaszcza na podstawie zasady dostępności, być objęte wymianą z właściwymi organami innego państwa członkowskiego.

36. EIOD podziela opinię, że art. 30 ust. 1 lit. b) i art. 31 ust. 1 lit. c) TUE stanowią podstawę prawną zasad ochrony danych, która nie ogranicza się do ochrony danych osobowych faktycznie wymienianych pomiędzy właściwymi organami państw członkowskich, ale dotyczy także sytuacji krajowych. W szczególności:

— Art. 30 ust. 1 lit. b), który może służyć jako podstawa prawna dla zasad w zakresie gromadzenia, przechowywania, przetwarzania, analizowania i wymiany stosownych informacji nie ogranicza się do informacji, które zostały udostępnione lub przekazane innym państwom członkowskim. Jedyne ograniczenie nałożone przez art. 30 ust. 1 lit. b) dotyczy kwestii, czy dana informacja jest istotna do celów współpracy policyjnej.

— W przypadku współpracy sądowej art. 31 ust. 1 lit. c) jest nawet bardziej oczywisty, ponieważ wspólne działanie obejmuje „zapewnianie, w zakresie niezbędnym do usprawnienia tej współpracy, zgodności norm stosowanych w państwach członkowskich".

— Ze sprawy Pupino ([3]) wynika, że Trybunał Sprawiedliwości stosuje zasady prawa wspólnotowego w kwestiach objętych trzecim filarem. Sprawa ta odzwierciedla zmiany zachodzące w wyniku przejścia z samej współpracy pomiędzy organami państw członkowskich w ramach trzeciego filaru w kierunku obszaru wolności, bezpieczeństwa i sprawiedliwości, porównywalne do rynku wewnętrznego ustanowionego na podstawie traktatu WE.

([1]) EIOD odnosi się do tego samego uzasadnienia, jakie Trybunał przedstawił (między innymi) w wyroku w sprawie Österreichischer Rundfunk i inni, sprawy połączone C-465/00, C-138/01 i C-139/01, Zb.Orz. [2003], str. I-4989.

([2]) Patrz w tym samym zakresie: opinia EIOD 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, pkt 33.

([3]) Wyrok Trybunału z dnia 16 czerwca 2005 r., Pupino, sprawa C-105/03.

— Zdaniem EIOD zasada skuteczności wiąże się z interpretacją traktatu, która nie utrudnia instytucjom Unii Europejskiej skutecznego wykonywania ich zadań. Obejmuje to także zadanie polegające na ochronie praw podstawowych.

— Jak już wcześniej wspomniano, ograniczenie do sytuacji transgranicznych nie byłoby zgodne ze skutkami zasady dostępności i stanowiłoby szkodę dla pewności prawnej osób fizycznych.

37. Oddzielnie EIOD zwraca uwagę na *wymianę danych z państwami trzecimi*. Państwa członkowskie wykorzystują dane osobowe gromadzone i przetwarzane w państwach trzecich, które są im przekazywane do celów ochrony porządku publicznego i przekazują dane osobowe, które same zgromadziły lub przetworzyły właściwym organom państw trzecich lub organom międzynarodowym.

38. Art. 30 i 31 TUE nie wymagają, by dane osobowe zgromadzone przez organy państw trzecich były traktowane w inny sposób niż dane, które zostały pierwotnie zgromadzone przez właściwe organy w państwach członkowskich. Dane pochodzące z państw trzecich, przekazane organom państw członkowskich, powinny spełniać te same normy, co dane zgromadzone w państwach członkowskich. Jednakże nie zawsze można zapewnić jakość danych (kwestia ta zostanie omówiona w następnym rozdziale niniejszej opinii).

39. Przekazywanie danych osobowych przez właściwe organy państw członkowskich państwom trzecim wykracza poza zakres tytułu VI traktatu UE. Jednak przekazywanie państwom trzecim danych bez zapewnienia ochrony osób, których dane dotyczą poważnie naruszyłoby ochronę danych zalecaną w niniejszym wniosku na terytorium Unii Europejskiej z powodów wymienionych w sekcji III.4 niniejszej opinii. Krótko mówiąc:

— Prawa osób, których dane dotyczą, zapewnione w niniejszym wniosku są bezpośrednio naruszane, jeżeli ich przekazywanie państwom trzecim nie byłoby objęte zasadami ochrony danych.

— Powstałoby ryzyko, że właściwe organy państw członkowskich mogłyby obchodzić surowe normy w zakresie ochrony danych.

40. Podsumowując, możliwość stosowania wspólnych norm w zakresie ochrony danych osobowych wymienianych między właściwymi organami państw członkowskich a organami państw trzecich i organizacjami międzynarodowymi jest niezbędna dla zapewnienia skuteczności wspólnych zasad w zakresie ochrony danych osobowych między właściwymi organami państw członkowskich i dlatego należy usprawnić współpracę pomiędzy państwami członkowskimi. Art. 30 i 31 TUE zapewniają niezbędną podstawę prawną w tym zakresie.

III.3 **Szczegółowe uwagi dotyczące zakresu wniosku**

Dane osobowe przetwarzane przez organy sądowe

41. Dane osobowe są przetwarzane i wymieniane przez siły policyjne i organy sądowe. Wniosek, którego podstawę prawną stanowią art. 30 i 31 traktatu UE, ma zastosowanie w przypadku współpracy pomiędzy siłami policyjnymi oraz współpracy pomiędzy organami sądowymi. Na tym etapie omawiany wniosek ma szerszy zakres niż wniosek dotyczący decyzji ramowej Rady w sprawie wymiany informacji, która ogranicza się do współpracy policyjnej i ma zastosowanie wyłącznie do informacji poprzedzających wszczęcie postępowania.

42. EIOD z zadowoleniem przyjmuje fakt, że wniosek rozszerza swój zakres o dane osobowe przetwarzane przez organy sądowe. Istnieją solidne podstawy, by ten wniosek zajmował się danymi organów policyjnych i sądowych przetwarzanymi do celów ochrony porządku publicznego Po pierwsze, procedury ścigania i karania przestępstw w państwach członkowskich są różne. W różnych państwach członkowskich organy sądowe rozpoczynają swoje działania na różnych etapach. Poza tym wszystkie dane osobowe wykorzystywane w tej procedurze ostatecznie mogą znaleźć się w aktach sądowych. Stosowanie różnych systemów ochrony danych na wcześniejszych etapach jest nielogiczne.

43. Jednak w przypadku nadzoru nad przetwarzaniem danych konieczne jest stosowanie różnych rozwiązań. Art. 30 wniosku wylicza zadania organów nadzorujących. W art. 30 ust. 9 stwierdza się, że kompetencje organów nadzorujących nie mają wpływu na niezawisłość wymiaru sprawiedliwości. EIOD zaleca wyjaśnienie we wniosku, że organy nadzorujące nie monitorują przetwarzania danych przez organy sądowe, o ile działają one w ramach swoich uprawnień sądowych ([1]).

Przetwarzanie danych przez Europol i Eurojust (oraz System Informacji Celnej)

44. Zgodnie z art. 3 ust. 2 wniosku, przepisów decyzji ramowej nie stosuje się do przetwarzania danych osobowych przez Europol, Eurojust i System Informacji Celnej ([2]).

([1]) Przepis ten mógłby być podobny do przepisu art. 46 rozporządzenia 45/2001/WE.

([2]) System Informacji Celnej jest małym, ale dość skomplikowanym systemem składających się z krajowych i ponadkrajowych elementów, porównywalnym do Systemu Informacji Schengen. Z uwagi na stosunkowo ograniczoną wagę obecnego wniosku dla Systemu Informacji Celnej i złożoność samego systemu, pozostanie on na marginesie niniejszej opinii. EIOD zajmie się Systemem Informacji Celnej w innym kontekście.

45. Ściśle mówiąc przepis ten jest zbędny, w każdym razie o ile odnosi się do Europolu i Eurojustu. Decyzja ramowa na mocy art. 34 lit. b) TUE może zostać przyjęta jedynie w celu zbliżania przepisów ustawowych i wykonawczych państw członkowskich i nie może być skierowana do Europolu ani do Eurojustu.

46. Co do istoty, treść art. 3 ust. 2 prowadzi do następujących uwag:

— obecny wniosek przewiduje ogólne ramy, które należy w zasadzie stosować we wszystkich sytuacjach objętych trzecim filarem; spójność ram prawnych ochrony danych jest sama w sobie elementem, który zwiększa skuteczność ochrony danych;.

— w obecnej chwili Europol i Eurojust dobrze zdefiniowały systemy ochrony danych będące w ich dyspozycji, w tym system nadzoru. Z tego względu nie ma pilnej potrzeby dostosowania zasad mających zastosowanie do treści wniosku;

— w dłuższym okresie czasu jednak zasady dotyczące ochrony danych mające zastosowanie do Europolu i Eurojustu powinny być w pełni spójne z obecną decyzją ramową;

— powyższe ma nawet większe znaczenie z tego względu, że obecny wniosek dotyczący decyzji ramowej — oprócz rozdziału III — ma zastosowanie do gromadzenia i przetwarzania danych osobowych, które są przekazywane Europolowi i Eurojustowi przez państwa członkowskie;

III.4 **Struktura wniosku**

47. EIOD przeanalizował wniosek i stwierdził, że ogólnie rzecz ujmując wniosek przewiduje warstwową strukturę ochrony. Wspólne normy określone w rozdziale II wniosku (oraz dotyczące szczególnych obszarów, określone w rozdziałach IV-VII) obejmują dwie warstwy ochrony.

— transpozycję zasad ochrony danych do trzeciego filaru, zgodnie z dyrektywą 95/46/WE i innymi instrumentami prawnymi Wspólnot Europejskich oraz konwencją nr 108 Rady Europy;

— dodatkowe zasady dotyczące ochrony danych, mające zastosowanie do wszystkich danych przetwarzanych w ramach trzeciego filaru. Przykłady tych dodatkowych zasad znajdują się w art. 4 ust. 3 i 4 wniosku.

48. W rozdziale III dodano trzecią warstwę ochrony szczególnych form przetwarzania. Tytuły dwóch sekcji rozdziału III i treść kilku przepisów wniosku wydaje się sugerować, że rozdział ten stosuje się jedynie do danych przekazywanych lub udostępnianych przez właściwe organy w innych państwach członkowskich. Wobec powyższego pewne istotne przepisy ochrony danych osobowych nie miałyby zastosowania, gdyby nie były wymieniane pomiędzy państwami członkowskimi. A zatem tekst jest niejednoznaczny, ponieważ same przepisy wydają się wykraczać poza działania bezpośrednio związane z wymienianymi danymi. W każdym przypadku to ograniczenie zakresu nie jest wyraźnie wyjaśnione, ani wytłumaczone w uzasadnieniu ani też w ocenie skutków.

49. EIOD podkreśla wartość dodaną takiej warstwowej struktury, która sama w sobie może zapewnić optymalną ochronę osoby, której dane dotyczą, z uwzględnieniem szczególnych potrzeb ochrony porządku publicznego. Powyższe odzwierciedla potrzebę odpowiedniej ochrony danych, jak to określono na konferencji wiosennej w Krakowie w kwietniu 2005 r., oraz z zasady jest zgodne z art. 8 Karty Praw Podstawowych Unii Europejskiej i z europejską Konwencją o ochronie praw człowieka i podstawowych wolności, w szczególności z jej art. 8.

50. Jednak analiza tekstu wniosku prowadzi do następujących uwag:

51. Po pierwsze, należy zapewnić brak odstępstwa dodatkowych zasad dotyczących ochrony danych określonych w rozdziale II (druga warstwa, o której mowa w pkt 47) od ogólnych zasad dotyczących ochrony danych. Według EIOD dodatkowe zasady określone w rozdziale II powinny zapewniać dodatkową ochronę osobom, których dane dotyczą, w związku z szczególnym kontekstem trzeciego filaru (informacje dla policji i sądownictwa). Innymi słowy: te dodatkowe zasady nie mogą prowadzić do niższego poziomu ochrony.

52. Ponadto rozdział III dotyczący szczególnych form przetwarzania (do którego włączono trzecią warstwę ochrony) nie powinien naruszać przepisów rozdziału II. Według EIOD przepisy rozdziału III powinny zapewniać dodatkową ochronę osobom, których dane dotyczą, w sytuacjach, gdy dotyczy to właściwych organów więcej niż jednego państwa członkowskiego, przy czym przepisy te nie mogą prowadzić do niższego poziomu ochrony.

53. Po drugie, zasady o charakterze ogólnym nie powinny znajdować się w rozdziale III. EIOD zaleca przeniesienie tych przepisów do rozdziału II. Jedynie przepisy, które ściśle odnoszą się do ochrony danych osobowych w przypadku wymiany danych pomiędzy państwami członkowskimi, muszą być włączone do rozdziału III. Powyższe ma nawet większe znaczenie z tego względu, że rozdział III zawiera istotne przepisy mające na celu wysoki poziom ochrony osoby, której dane dotyczą w kontekście ochrony porządku publicznego (patrz pkt IV.1 niniejszej opinii).

IV. **ANALIZA ELEMENTÓW WNIOSKU**

IV.1 **Punkty wyjścia analizy**

54. EIOD, analizując różne istotne elementy wniosku, weźmie pod uwagę jego szczególną strukturę i treść. EIOD nie przedstawi komentarzy do każdego artykułu wniosku.

55. Przede wszystkim większość przepisów wniosku odzwierciedla inne instrumenty prawne UE dotyczące ochrony danych osobowych. Przepisy te są zgodne z ramami prawnymi UE dotyczącymi ochrony danych i wystarczające do zapewnienia odpowiednich zabezpieczeń ochrony danych w trzecim filarze.

56. Jednak EIOD zauważa, że niektóre przepisy zawarte obecnie w rozdziale III wniosku — dotyczące szczególnych punktów przetwarzania i, ogólnie rzecz ujmując, (patrz pkt 48 niniejszej opinii) mające zastosowanie jedynie do danych wymienianych z innymi państwami członkowskimi — łączą ogólne i podstawowe zasady prawa UE dotyczącego ochrony danych. Dlatego też te przepisy określone w rozdziale III powinny zostać przeniesione do rozdziału II i udostępnione przez organy porządku publicznego wszystkim przetwarzającym dane. Jest to przypadek przepisów dotyczących weryfikacji jakości danych (art. 9 ust. 1 i 6) i regulujących dalsze przetwarzanie danych osobowych (art. 11 ust. 1).

57. W niektórych pozostałych artykułach rozdziału III wniosku nie zawarto rozróżnienia na dodatkowe warunki szczególnie odnoszące się do wymiany danych z innymi państwami członkowskimi — takie jak zgoda właściwego organu przekazującego państwa członkowskiego — oraz zabezpieczenia istotne i niezbędne również w odniesieniu do danych przetwarzanych w danym państwie członkowskim. W tych przypadkach EIOsD zaleca, aby te zabezpieczenia miały generalnie zastosowanie nawet do tych danych osobowych, które nie zostały przekazane ani udostępnione przez inne państwo członkowskie. Zalecenie to dotyczy:

— przekazywania danych podmiotom prywatnym oraz organom niebędącym organami porządku publicznego (lit. a) i b) art. 13 i 14) oraz

— przekazywania państwom trzecim lub organom międzynarodowym (art. 15, z wyjątkiem lit. c)).

58. Ta część opinii zwraca również uwagę prawodawcy na niektóre dodatkowe zabezpieczenia, które nie zostały ustanowione w obecnym wniosku. Według EIOD te dodatkowe zabezpieczenia powinny być przewidziane w powiązaniu ze zautomatyzowanymi indywidualnymi decyzjami, danymi osobowymi otrzymanymi z państw trzecich, dostępem do baz danych podmiotów prywatnych, przetwarzaniem danych biometrycznych i profili DNA.

59. Ponadto następujące analizy zapewnią zalecenia zmierzające do poprawy obecnego tekstu w celu zapewnienia skuteczności przepisów, spójności tekstu I zgodności z obecnymi ramami prawnymi ochrony danych.

IV.2 **Ograniczenie celu i dalsze przetwarzanie**

60. Art. 4 ust. 1 lit. b) stwierdza, że dane osobowe muszą być gromadzone do określonych, wyraźnych i legalnych celów oraz nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z tymi celami. Zwykle dane są gromadzone w związku z określonym przestępstwem (lub pod pewnymi warunkami, w celu przeprowadzenia dochodzenia w sprawie grupy lub siatki przestępczej, itd.). Mogą one być wykorzystywane do tego pierwotnego celu, a następnie być przetwarzane w innym celu, o ile jest on zgodny z celem pierwotnym (na przykład dane gromadzone na temat osoby skazanej za handel narkotykami mogą być wykorzystywane w ramach dochodzenia dotyczącego siatki dealerów narkotyków). Podejście to dobrze odzwierciedla zasadę ograniczenia celu, która również została zawarta w art. 8 Karty praw człowieka Unii Europejskiej i wobec tego jest zgodne z obecnym prawodawstwem w zakresie ochrony danych.

Dalsze przetwarzanie do celów w zakresie decyzji ramowej

61. EIOD zauważa, że wniosek nie określa w sposób zadowalający pewnej sytuacji, która może wydarzyć się podczas pracy policji: a mianowicie, potrzeby dalszego wykorzystywania danych do celów uznanych za niezgodne z celem, dla którego zostały zebrane. Dane zebrane przez policję mogą być potrzebne do ścigania całkowicie innego przestępstwa. Dla zobrazowania powyższego można powiedzieć, że dane są zbierane w celu ściganie przewinień w ruchu ulicznym, a następnie wykorzystywane do zlokalizowania i ścigania złodzieja samochodów. Drugi cel, jakkolwiek zgodny z prawem, nie może być uznany za w pełni zgodny z celem gromadzenia danych. Jeżeli zakaże się organom porządku publicznego wykorzystywania danych w tym drugim celu, to można je skłonić do gromadzenia danych w szerokich lub źle zdefiniowanych celach, w którym to przypadku zasada ograniczenia celu straciłaby swą wartość w odniesieniu do gromadzenia danych. Ponadto stosowanie innych zasad, takich jak proporcjonalność, ścisłość i wiarygodność byłoby utrudnione (patrz art. 4 ust. 1 lit. c) i d)).

62. Zgodnie z prawem UE dotyczącym ochrony danych, dane osobowe muszą być gromadzone do określonych i wyraźnych celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Jednak EIOD jest zdania, że trzeba zezwolić na pewną elastyczność w odniesieniu do dalszego wykorzystania. Jest bardziej prawdopodobne, że ograniczenie dotyczące gromadzenia danych jest faktycznie przestrzegane, jeżeli organy odpowiedzialne za wewnętrzne bezpieczeństwo wiedzą, że mogą polegać, przy odpowiednich zabezpieczeniach, na odstępstwie od ograniczenia w odniesieniu do dalszego wykorzystania.

63. Należy wyjaśnić, że ta potrzeba dalszego przetwarzania jest określona w art. 11 wniosku, ale raczej w sposób niewystarczający. Art. 11 ma jedynie zastosowanie do danych otrzymanych od właściwych organów innego państwa członkowskiego lub przez nie udostępnionych i nie przewiduje wystarczających zabezpieczeń.

64. EIOD zaleca stosowanie art. 11 ust. 1 do wszystkich danych, bez względu na to, czy otrzymano je od innego państwa członkowskiego czy tez nie. Ponadto ściślejsze zabezpieczenia powinny zostać dodane do określeń zawartych w art. 11 ust. 1 lit. b): dalsze wykorzystanie danych w celu uznanym za niezgodny z celem oryginalnym powinno być dozwolone jedynie w przypadku, gdy jest to wyraźnie niezbędne, w określonym przypadku, do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania lub do celów ochrony interesów lub praw podstawowych danej osoby. EIOD proponuje włączenie tego przepisu do nowego art. 4a (w każdym razie do rozdziału II wniosku).

65. Art. 11 ust. 2 i 3 mogą być stosowane w obecnej formie; przewidują one dodatkowe zabezpieczenia dla danych otrzymanych od innego państwa członkowskiego. EIOD wskazuje, że art. 11 ust. 3 będzie miał zastosowanie do danych wymienionych w SIS II; EIOD już stwierdził w opinii dotyczącej SIS II, że należy zapewnić faktyczny brak możliwości wykorzystywania danych SIS w jakimkolwiek innym celu niż cele samego systemu.

Dalsze przetwarzanie do celów znajdujących się poza zakresem współpracy policyjnej i sądowej

66. W pewnych przypadkach dane należy przetwarzać w celu zabezpieczenia innych ważnych interesów. W tych przypadkach mogą nawet być przetwarzane przez organy inne niż organy właściwe na mocy tej decyzji ramowej. Do tych kompetencji państw członkowskich może należeć również przetwarzanie naruszające prywatność (na przykład kontrolowanie osoby niebędącej podejrzanym) i wobec tego muszą mu towarzyszyć surowe warunki, jak obowiązek państw członkowskich do przyjęcia szczególnego prawodawstwa, jeśli pragną skorzystać z tego odstępstwa. W ramach pierwszego filaru kwestia ta została określona w art. 13 dyrektywy 95/46/WE, w którym stwierdza się, że w szczególnych przypadkach dozwolone są ograniczenia wobec pewnych przepisów dyrektywy. Państwa członkowskie stosujące takie ograniczenia muszą stosować je zgodnie z art. 8 EKPC.

67. Zgodnie z takim samym sposobem rozumowania ta decyzja ramowa powinna określać w rozdziale II, że państwom członkowskim powinno się zezwolić na przyjęcie środków legislacyjnych w celu umożliwienia dalszego przetwarzania, gdy środek taki jest konieczny do zabezpieczenia:

— zapobiegania zagrożeniom bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego;

— ochrony ważnego interesu gospodarczego lub finansowego państwa członkowskiego lub Unii Europejskiej;

— ochrony osoby, której dane dotyczą.

IV.3 **Kryteria zapewniające zgodność z prawem przetwarzania danych**

68. Art. 5 wniosku stanowi, że dane osobowe mogą być przetwarzane przez właściwe organy wyłącznie, jeśli jest to przewidziane przepisami stanowiącymi, że przetwarzanie jest konieczne do celów wypełniania zgodnych z prawem zadań danego organu oraz do celów zapobiegania przestępstwom, ich ścigania, wykrywania lub karania. EIOD popiera surowe wymogi określone w art. 5.

69. Jednak tekst art. 5 nie docenia potrzeby zapewnienia przetwarzaniu danych zgodności z prawem na innych podstawach prawnych w określonych okolicznościach. Jest to istotny przepis, który powinien na przykład nie uniemożliwiać policji wypełniania obowiązków prawnych, zgodnie z prawem krajowym, ujawnienia informacji służbom imigracyjnym lub podatkowym. Wobec powyższego EIOD proponuje, aby art. 5 uwzględniał inne uzasadnione podstawy prawne przetwarzania danych osobowych, takie jak konieczność zgodności z obowiązkiem prawnym, któremu podlega kontroler, jednoznacznej zgody osoby, której dane dotyczą, o ile przetwarzanie przeprowadzane jest w interesie osoby, której dane dotyczą, lub konieczność ochrony istotnych interesów osoby, której dane dotyczą.

70. EIOD stwierdza, że poszanowanie kryteriów zapewniających przetwarzaniu danych zgodność z prawem ma szczególne znaczenie w odniesieniu do współpracy policyjnej i sądowej, jeżeli rozważy się, że niezgodne z prawem gromadzenie danych osobowych przez służby policyjne może oznaczać, że te dane osobowe nie będą mogły być wykorzystywane jako dowód w postępowaniu sądowym.

IV.4 **Konieczność i proporcjonalność**

71. Art. 4 i 5 wniosku mają również na celu zapewnienie — w ogólnie satysfakcjonujący sposób — że ograniczenia ochrony danych osobowych są konieczne i proporcjonalne zgodnie z wymogami prawa Unii Europejskiej oraz orzecznictwa Europejskiego Trybunału Praw Człowieka w art. 8 EKPC:

— Art. 4 ust. 1 lit. c) określa ogólną zasadę, że dane muszą być odpowiednie, istotne oraz nienadmierne w stosunku do celów, dla których są gromadzone lub przetwarzane dalej;

— Art. 5 określa, że przetwarzanie powinno być konieczne do celów wypełniania zgodnych z prawem zadań danego organu oraz do celów zapobiegania przestępstwom, ich ścigania, wykrywania lub karania;

— art. 4 ust. 4 stwierdza, że przetwarzanie danych osobowych jest konieczne wyłącznie, jeśli spełnione są pewne szczególne warunki.

72. EIOD zauważa, że wnioskowane sformułowanie art. 4 ust. 4 nie spełnia kryteriów określonych w orzecznictwie Europejskiego Trybunału Praw Człowieka odnoszącym się do art. 8 EKPC, zgodnie z którym ograniczenie życia prywatnego może być nałożone jedynie, gdy jest to konieczne w demokratycznym społeczeństwie. Zgodnie z wnioskiem, przetwarzanie danych będzie uważane za konieczne nie tylko, gdy *umożliwiłoby* ochronę porządku publicznego, a organy sądowe mogłyby wykonywać swoje zadania, ale również gdy istnieją *uzasadnione powody*, aby *sądzić*, że określone dane osobowe mogłyby zaledwie *ułatwić lub przyspieszyć* zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie.

73. Kryteria te nie są zgodne z wymogami art. 8 EKPC, ponieważ prawie każde przetwarzanie danych osobowych mogłoby być uważane za ułatwiające działania policji lub organów sądowych, nawet jeśli określone dane nie są rzeczywiście potrzebne do prowadzenia tych działań.

74. Obecna treść art. 4 ust. 4 wytyczyłaby drogę dla niemożliwego do zaakceptowania szerokiego gromadzenia danych osobowych, opartego zaledwie na osądzie, że dane osobowe *mogą ułatwić* zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie. Z drugiej strony przetwarzanie danych osobowych jest uważane za niezbędne jedynie, gdy właściwe organy mogą wyraźnie wykazać potrzebę tego przetwarzania oraz o ile nie są dostępne środki mniej naruszające prywatność.

75. Wobec powyższego EIOD zaleca przeformułowanie art. 4 ust. 4 tiret pierwsze w celu zapewnienia poszanowania orzecznictwa w zakresie art. 8 EKPC. Ponadto, dla usystematyzowania, EIOD proponuje, aby art. 4 ust. 4 został przeniesiony na koniec art. 5.

IV.5 **Przetwarzanie szczególnych kategorii danych**

76. Art. 6 ustanawia z zasady zakaz przetwarzania danych wrażliwych, np. danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych i danych dotyczących zdrowia lub życia seksualnego. Zakaz ten nie będzie miał zastosowania, gdy przetwarzanie przewidziane jest prawem i jest absolutnie niezbędne dla spełnienia zgodnego z prawem zadania określonego organu do celów zapobiegania przestępstwom, ich ścigania, wykrywania lub karania. Dane wrażliwe mogą również być przetwarzane, jeżeli osoba, której dane dotyczą, udzieli wyraźnej zgody. W obydwu przypadkach należy ustanowić odpowiednie szczególne zabezpieczenia.

77. Treść art. 6 prowadzi do dwóch uwag. Przede wszystkim, art. 6 zbyt szeroko opiera się na zgodzie osoby, której dane dotyczą. EIOD podkreśla, że przetwarzanie danych wrażliwych na podstawie wyraźnej zgody osoby, której dane dotyczą, powinno być dozwolone, jedynie, o ile przetwarzanie jest przeprowadzane w interesie osoby, której dane dotyczą, a odmowa udzielenia zgody nie doprowadzi do negatywnych skutków względem osoby, której dane dotyczą. EIOD zaleca odpowiednią zmianę art. 6, również w celu zachowania spójności artykułu z obecnym prawem UE dotyczącym ochrony danych.

78. Ponadto EIOD uważa, że również inne podstawy prawne przetwarzania, takie jak konieczność ochrony istotnych interesów osoby, której dane dotyczą, lub innej osoby (jeżeli osoba, której dane dotyczą jest fizycznie lub prawnie niezdolna do udzielenia zgody) mogłyby zostać wzięte pod uwagę.

79. W obszarze współpracy policyjnej i sądowej coraz ważniejsze staje się przetwarzanie innych kategorii możliwie wrażliwych danych osobowych, takich jak dane biometryczne lub profile DNA. Dane te nie są wyraźnie objęte art. 6 wniosku. EIOD zachęca prawodawcę UE do zwrócenia szczególnej uwagi podczas implementacji ogólnych zasad ochrony danych określonych w tym wniosku do dalszej legislacji, wiążącej się z przetwarzaniem tych szczególnych kategorii danych. Przykładem jest obecny wniosek dotyczący decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności (patrz pkt 12-15 powyżej), który wyraźnie zezwala na przetwarzanie i wymianę danych biometrycznych i profili DNA (patrz załącznik II wniosku), ale nie określa wrażliwości i szczególności tych danych z punktu widzenia ochrony danych.

80. EIOD zaleca określenie szczególnych zabezpieczeń, w szczególności w celu zagwarantowania, aby:

— dane biometryczne i profile DNA były wykorzystywane jedynie na podstawie dobrze określonych i interoperacyjnych norm technicznych;

— ich stopień ścisłości był uważnie uwzględniony i mógł być podważony przez osobę, której dane dotyczą, przy pomocy dostępnych sposobów, oraz

— było w pełni zapewnione poszanowanie godności osób.

Prawodawca decyduje o zapewnieniu tych dodatkowych zabezpieczeń w decyzji ramowej lub w szczególnych instrumentach prawnych regulujących gromadzenie i wymianę tych szczególnych kategorii danych.

IV.6 **Ścisłość i wiarygodność**

81. Art. 4 ust. 1 lit. d) ustanawia ogólne zasady odnoszące się do jakości danych. Zgodnie z niniejszym artykułem kontroler musi zapewnić, że dane są ścisłe i, jeśli jest to konieczne, aktualizowane. Musi on podjąć wszelkie stosowne kroki, aby zapewnić usunięcie lub poprawienie nieścisłych lub niekompletnych danych, mając na uwadze cele, w jakich były one gromadzone i w jakich są w dalszym ciągu przetwarzane, usuwane lub poprawiane. Jest to zgodne z ogólnymi zasadami prawodawstwa UE w zakresie ochrony danych.

82. Art. 4 ust. 1 lit. d) zdanie trzecie przewiduje, że państwa członkowskie mogą rozróżniać przetwarzanie danych w zależności od różnych stopni ścisłości i wiarygodności. EIOD interpretuje ten przepis jako odstępstwo od ogólnej zasady ścisłości i zaleca wyjaśnienie charakteru odstępstwa, o którym mowa w przepisie, poprzez dodanie słów „jednak" lub „niemniej jednak" na początku trzeciego zdania art. 4 ust. 1 lit. d). W tych przypadkach, w których nie można w pełni zapewnić ścisłości danych, kontroler będzie miał obowiązek rozróżnienia danych w zależności od różnych stopni ścisłości i wiarygodności, odnosząc się w szczególności do podstawowego rozróżnienia pomiędzy danymi opartymi na faktach i danymi opartymi na opiniach i prywatnych ocenach. EIOD podkreśla istotność tego obowiązku zarówno dla osób, których dane dotyczą, jak i dla organów porządku publicznego, szczególnie gdy dane są przetwarzane daleko od ich źródła (patrz pkt 7 niniejszej opinii).

Weryfikacja jakości danych

83. Do ogólnej zasady określonej w art. 4 ust. 1 lit. d) dodano bardziej szczegółowe zabezpieczenia ustanowione w art. 9 dotyczącym weryfikacji jakości danych. W szczególności w art. 9 stwierdza się, że:

1. jakość danych osobowych jest poddawana weryfikacji najpóźniej przed ich przekazaniem lub udostępnieniem. Dodatkowo jakość danych udostępnianych w sposób bezpośredni i zautomatyzowany podlega regularnej weryfikacji (art. 9 ust. 1 i 2);

2. przy każdorazowym przekazaniu danych powinny być wskazane orzeczenia sądowe oraz decyzje niewyegzekwowane drogą sądową, a dane oparte na opiniach powinny być sprawdzone u źródła przed ich przekazaniem wraz ze wskazaniem stopnia ich ścisłości lub wiarygodności (art. 9 ust. 1);

3. dane osobowe oznacza się na wniosek osoby, której dane dotyczą, w przypadku gdy osoba, której dane dotyczą, kwestionuje ich ścisłość oraz gdy nie można mieć pewności co do ich ścisłości lub nieścisłości (art. 9 ust. 6).

84. Wobec powyższego art. 4 ust. 1 i art. 9 zapewniają, w przypadku łącznego zastosowania, odpowiednią weryfikację danych osobowych, zarówno przez osobę, której dane dotyczą, jak i przez organy, które są najbliżej źródła przetwarzanych danych i dlatego też są w stanie najlepiej je sprawdzić.

85. EIOD z zadowoleniem przyjmuje te przepisy, ponieważ koncentrując się na potrzebach organów porządku publicznego, zapewniają odpowiednie uwzględnienie wszystkich danych i wykorzystywanie tych danych zgodnie z ich ścisłością i wiarygodnością, unikając dzięki temu nieproporcjonalnego wpływu braku ścisłości pewnych danych dotyczących osoby, której dane dotyczą, na tę osobę.

86. Weryfikacja jakości danych jest podstawowym elementem ochrony osoby, której dane dotyczą, szczególnie w odniesieniu do danych osobowych przetwarzanych przez organy policyjne i sądowe. Wobec powyższego EIOD żałuje, że stosowanie art. 9 dotyczącego weryfikacji jakości danych jest ograniczone do danych przekazywanych lub udostępnianych innym państwom członkowskim. Jest to niefortunne, ponieważ oznacza, że jakość danych osobowych, która jest podstawowa również dla celów ochrony porządku publicznego, byłaby w pełni zapewniona jedynie wówczas gdy dane te są przekazywane lub udostępniane innym państwom członkowskim, ale nie wtedy gdy są przetwarzane w państwie członkowskim ([1]). Natomiast niezbędne jest — zarówno w interesie osób, których dane dotyczą, jak i właściwych organów — zapewnienie, że właściwa weryfikacja jakości dotyczy wszystkich danych osobowych, włącznie z danymi nieprzekazanymi ani nieudostępnionymi przez inne państwo członkowskie.

87. Wobec powyższego, EIOD zaleca usunięcie w każdym przypadku ograniczeń w zakresie stosowania art. 9 ust. 1 i 6 poprzez przeniesienie tych przepisów do rozdziału II wniosku.

Rozróżnienie na różne kategorie danych

88. Art. 4 ust. 2 ustanawia dla kontrolera obowiązek dokonania jasnego rozróżnienia na dane osobowe różnych kategorii osób (podejrzany, skazany, świadek, ofiara, informator, kontakt, inna osoba). EIOD z zadowoleniem przyjmuje to podejście. Chociaż prawdą jest, że organy porządku publicznego i organy sądowe mogą potrzebować przetwarzać dane odnoszące się do bardzo różnych kategorii osób, niezbędne jest dokonanie rozróżnienia tych danych według różnych stopni zaangażowania w przestępstwo. W szczególności warunki dotyczące gromadzenia danych, terminów, odmowy dostępu lub informowania osoby, której dane dotyczą, dostępu do danych przez właściwe organy powinny odzwierciedlać cechy charakterystyczne różnych kategorii przetwarzanych danych i różnych celów, dla których dane te są gromadzone przez organy porządku publicznego i sądowe.

89. W tym kontekście, EIOD zwraca szczególną uwagę na dane odnoszące się do osób niebędących podejrzanymi. Szczególne warunki i zabezpieczenia są potrzebne w celu zapewnienia proporcjonalności i zapobieżenia poniesienia uszczerbku przez osoby, które nie są aktywnie zaangażowane w przestępstwo. Dla tej kategorii osób wniosek powinien zawierać dodatkowe przepisy ograniczające cel przetwarzania, określające dokładne terminy i ograniczające dostęp do danych. EIOD zaleca odpowiednią zmianę wniosku.

([1]) Dodatkowo, nie byłoby to zgodne z zaleceniem Rady Europy nr R (87) 15 Komitetu Ministrów do Pastw członkowskich w sprawie wykorzystania danych osobowych w sektorze policyjnym. W szczególności zasada 7.2 przewiduje, że „regularne kontrole" jakości danych osobowych powinny być ustanowione w porozumieniu z organem nadzoru lub zgodnie z prawem krajowym.

90. Obecny tekst wniosku zawiera jedno szczególne zabezpieczenie dotyczące osób niebędących podejrzanymi, a mianowicie art. 7 ust. 1 wniosku. Według EIOD jest to ważne zabezpieczenie, głównie z tego względu że zakazano państwom członkowskim określania odstępstw. Niestety art. 7 ust. 1 ustanawia szczególne zabezpieczenia jedynie w odniesieniu do terminów, a jego stosowanie jest ograniczone do kategorii osób, o których mowa w ostatnim tiret art. 4 ust. 3 wniosku. A zatem artykuł ten nie przewiduje odpowiednich zabezpieczeń i nie obejmuje całej grupy osób niebędących podejrzanymi ([1]).

91. Również dane odnoszące się do osób skazanych zasługują na szczególną uwagę. W przypadku tych danych powinny być należycie uwzględnione ostatnie i przyszłe inicjatywy dotyczące wymiany rejestrów karnych, a ponadto powinno się zapewnić spójność ([2]).

92. W świetle powyższych uwag, EIOD zaleca dodanie nowego ustępu do art. 4, który zawierałby następujące elementy:

— dodatkowe przepisy ograniczające cel przetwarzania, określające dokładne terminy i ograniczające dostęp do danych, w przypadku gdy jest mowa o osobach niebędących podejrzanymi;.

— obowiązek państw członkowskich określenia konsekwencji prawnych rozróżnienia, które zostanie dokonane na dane osobowe różnej kategorii osób, odzwierciedlające cechy charakterystyczne różnych kategorii przetwarzanych danych i różnych celów, dla których dane te są gromadzone przez organy porządku publicznego i sądowe;

— konsekwencje prawne powinny odnosić się do warunków dotyczących gromadzenia danych osobowych, terminów, dalszego przekazywania i wykorzystania danych oraz odmowy dostępu lub informowania osoby, której dane dotyczą.

IV.7 **Terminy przechowywania danych osobowych**

93. Ogólne zasady regulujące terminy przechowywania danych osobowych są określone w art. 4 ust. 1 lit. e) i art. 7 ust. 1 wniosku. Z zasady dane osobowe powinny być przechowywane przez okres nie dłuższy niż jest to niezbędne do celu, dla którego są gromadzone. Jest to zgodne z prawodawstwem UE w zakresie ochrony danych ([3]).

94. Niemniej jednak ogólny przepis art. 7 ust. 1 ma zastosowanie „chyba że prawo krajowe stanowi inaczej". EIOD zauważa, że wyjątek ten jest bardzo ogólny i wykracza poza odstępstwa dopuszczone na mocy art. 4 ust. 1 lit. e). EIOD wnioskuje, aby ogólne odstępstwo, o którym mowa w art. 7 ust. 1, zostało usunięte lub przynajmniej wyraźnie ograniczało interesy publiczne uzasadniające korzystanie z tego odstępstwa przez państwa członkowskie ([4]).

95. Art. 7 ust. 2 stwierdza, że należy zapewnić przestrzeganie terminów przy pomocy odpowiednich środków proceduralnych i technicznych oraz regularną kontrolę tych terminów. EIOD z zadowoleniem przyjmuje ten przepis, ale zaleca wyraźne stwierdzenie, że należy przewidzieć odpowiednie środki proceduralne i techniczne dla automatycznego i regularnego usuwania danych osobowych po pewnym okresie.

IV.8 **Wymiana danych osobowych z państwami trzecimi**

96. Skuteczna współpraca policyjna i sądowa w granicach UE w coraz większym stopniu zależy od współpracy z państwami trzecimi i organizacjami międzynarodowymi. Wiele działań mających na celu poprawę współpracy w zakresie ochrony porządku publicznego i współpracy sądowej z państwami trzecimi lub organizacjami międzynarodowymi jest obecnie dyskutowana lub określana zarówno na szczeblu krajowym jak i UE ([5]). Rozwój tej międzynarodowej współpracy prawdopodobnie będzie polegał w głównej mierze na wymianie danych osobowych.

97. Dlatego też jest niezwykle ważne, aby zasady uczciwego i zgodnego z prawem przetwarzania — oraz generalnie zasady należytego przetwarzania — również miały zastosowanie do gromadzenia i wymiany danych osobowych w całej Unii oraz aby dane osobowe były przekazywane państwom trzecim lub organizacjom międzynarodowym tylko wówczas, gdy te państwa trzecie zagwarantują odpowiedni poziom ochrony lub odpowiednie zabezpieczenia.

([1]) Patrz także pkt 94 niniejszej opinii.

([2]) Decyzja Rady 2005/876/WSiSW w sprawie wymiany informacji pochodzących z rejestru karnego weszła w życie dnia 9 grudnia. Decyzja ta dodaje takie instrumenty jak Europejska konwencja o pomocy prawnej w sprawach karnych z 1959 r. i konwencja w sprawie pomocy sądowej w sprawach karnych pomiędzy państwami członkowskimi z 1959 r. do istniejących mechanizmów przekazywania informacji dotyczących wyroków opartych na istniejących konwencjach i ułatwia funkcjonowanie tych mechanizmów. Tekst ten zostanie w późniejszym terminie zastąpiony przez szczegółową decyzję ramową Rady. Komisja przewiduje złożenie wniosku w sprawie nowej decyzji ramowej w tym obszarze.

([3]) Oprócz ogólnego przepisu dotyczącego terminów przechowywania danych osobowych, o których mowa w art. 7, wniosek określa dalsze szczególne przepisy dotyczące danych osobowych wymienianych z innymi państwami członkowskimi. W szczególności art. 9.7 stanowi, że dane osobowe podlegają skreśleniu:
19 jeżeli danych tych nie należało przekazać, udostępnić lub otrzymać,
2) po terminie określonym przez organ przekazujący, chyba że dane osobowe są dalej potrzebne w postępowaniu sądowym,
3) jeżeli dane nie są już niezbędne dla celu, dla którego zostały przekazane.

([4]) Należy rozważyć ograniczenie dla zwalczania terroryzmu lub dla szczególnych interesów publicznych określone w art. 4 ust. 1 lit. e): do użytku historycznego, statystycznego lub naukowego.

([5]) Na przykład patrz ostatni komunikat Komisji dotyczący „Strategii w sprawie zewnętrznego wymiaru obszaru wolności, bezpieczeństwa i sprawiedliwości" (COM(2005) 491 wersja ostateczna).

Przekazywanie danych osobowych do państw trzecich

98. Z tej perspektywy EIOD z zadowoleniem przyjmuje art. 15 wniosku, który przewiduje ochronę w przypadku przekazywania danych właściwym organom w państwach trzecich lub organom międzynarodowym. Jednak przepis ten zawarty w rozdziale III wniosku ma zastosowanie jedynie do danych otrzymywanych lub udostępnianych właściwym organom innych państw członkowskich. Wskutek tego ograniczenia, wada systemu ochrony danych na szczeblu Unii Europejskiej odnosi się do danych, które nie są otrzymywane od właściwych organów z innych państw członkowskich. Według EIOD nie można zaakceptować tej wady z uwagi na niżej określone powody.

99. Po pierwsze, poziom ochrony zapewniany przez prawo UE w przypadku przekazywania danych do państwa trzeciego nie powinien być uzależniony od źródła danych — sił policyjnych w państwie członkowskim, które przekazuje dane do państwa trzeciego lub służb policyjnych w innym państwie członkowskim.

100. Po drugie, należy zauważyć, że zasady regulujące przekazywanie danych osobowych państwom trzecim stanowią podstawę prawa ochrony danych. Zasada ta nie tylko stanowi jeden z podstawowych przepisów dyrektywy 95/46/WE, ale również jest określona w dodatkowym protokole do konwencji nr 108 ([1]). Wspólne normy w zakresie ochrony danych osobowych określone w art. 1 wniosku nie mogą zostać zapewnione, jeżeli wspólne zasady przekazywania danych osobowych państwom trzecim nie obejmą wszystkich operacji przetwarzania. Wobec powyższego zapewnione w obecnym wniosku prawa osób, których dane dotyczą, byłyby bezpośrednio naruszone, gdyby dane osobowe nie mogły zostać przekazane państwom trzecim, które nie gwarantują odpowiedniego poziomu ochrony.

101. Po trzecie, ograniczenie zakresu tych zasad do „danych wymienianych" oznaczałoby, że — w odniesieniu do danych przetwarzanych jedynie w jednym kraju — nie istniałyby żadne zabezpieczenia: paradoksalnie dane osobowe mogłyby być przekazywane do państw trzecich — bez względu na jakąkolwiek odpowiednią ochronę danych osobowych — „łatwiej" niż do innych państw członkowskich. Mogłoby to doprowadzić do powstania możliwości „prania informacji". Właściwe organy państw członkowskich mogłyby obchodzić surowe normy w zakresie ochrony danych poprzez przekazywanie danych państwom trzecim lub organizacjom międzynarodowym, w przypadku gdyby mogły one być dostępne dla właściwych organów innego państwa członkowskiego lub nawet z powrotem przesyłane do takiego organu.

102. Wobec powyższego EIOD zaleca zmianę obecnego wniosku tak, aby zapewnić stosowanie art. 15 do wymiany *wszystkich* danych osobowych z państwami trzecimi. Zalecenie to nie odnosi się do art. 15 ust. 1 lit. c), który ze względu na swój charakter może jedynie odnosić się do danych osobowych wymienianych z innymi państwami członkowskimi.

Wyjątkowe przekazywanie danych do krajów niezapewniających odpowiedniego poziomu ochrony danych

103. Art. 15 ustanawia zestaw warunków dla przekazywania danych właściwym organom w państwach trzecich lub międzynarodowym organizacjom porównywalnych z warunkami określonymi w art. 25 dyrektywy 95/46/WE. Jednak art. 15 ust. 6 ustanawia możliwość przekazywania danych państwom trzecim lub organizacjom międzynarodowym, które nie zapewniają odpowiedniego poziomu ochrony danych, o ile przekazywanie danych jest absolutnie konieczne w celu zabezpieczenia podstawowych interesów państwa członkowskiego lub dla zapobieżenia bliskiemu poważnemu zagrożeniu bezpieczeństwa publicznego lub wobec określonej osoby lub osób.

104. Stosowanie wyjątku ustanowionego w ust. 6 powinno zostać wyjaśnione. Wobec powyższego EIOD zaleca:

— wyjaśnienie, że wyjątek ten ustanawia jedynie odstępstwo od warunku „odpowiedniej ochrony", ale nie narusza innych warunków, o których mowa w pierwszym akapicie art. 15;

— dodanie, że przekazy danych prowadzone zgodnie z tym wyjątkiem powinny podlegać odpowiednim warunkom (takim jak wyraźny warunek mówiący o tym, że dane są przetwarzane jedynie czasowo i dla szczególnych celów) oraz że właściwy organ nadzoru będzie powiadamiany.

Przetwarzanie danych osobowych otrzymywanych z państw trzecich

105. W kontekście wzrastającej wymiany danych osobowych z organami policyjnymi i sądowymi państw trzecich należy również zwrócić szczególną uwagę na dane osobowe „importowane" z tych państw trzecich, które nie zapewniają odpowiednich norm poszanowania praw człowieka, a w szczególności ochrony danych osobowych.

([1]) Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, został podpisany 8 listopada 2001 r. i wszedł w życia 1 lipca 2004 r. Ten wiążący instrument prawa międzynarodowego został dotychczas podpisany przez 11 państw (z których 9 jest państwami członkowskimi UE). Art. 2.1 protokołu ustanawia ogólną zasadę: „Każda Strona zapewni, że przekazanie danych osobowych do odbiorcy podlegającego jurysdykcji państwa lub organizacji niebędącej Stroną konwencji nastąpi tylko wtedy, gdy to państwo lub organizacja zapewni wystarczający poziom ochrony danych, które mają zostać przekazane".

106. W szerszej perspektywie EIOD uważa, że prawodawca powinien zapewnić, aby dane osobowe otrzymane z państw trzecich były zgodne przynajmniej z międzynarodowymi normami odnoszącymi się do poszanowania praw człowieka. Na przykład, dane zgromadzone przy zastosowaniu tortur lub w wyniku naruszenia praw człowieka, czarne listy oparte jedynie na poglądach politycznych lub preferencjach seksualnych nie powinny być przetwarzane ani też organy porządku publicznego i organy sądowe nie powinny się na nich opierać, chyba że w interesie osoby, której dane dotyczą. Wobec tego EIOD zaleca wyjaśnienie powyższego przynajmniej w motywie wniosku, w miarę możliwości poprzez odniesienie do odpowiednich instrumentów międzynarodowych ([1]).

107. Przyglądając się bliżej ochronie danych osobowych, EIOD stwierdza, że w przypadku gdy dane osobowe są przekazywane z krajów nie mających odpowiednich norm i gwarancji w zakresie ochrony danych osobowych, możliwy brak danych wysokiej jakości jest należycie oceniany w celu uniknięcia błędnego oparcia się na takich informacjach przez organy porządku publicznego UE i oraz zapobieżenia poniesienia uszczerbku przez osoby, których dane dotyczą.

108. Wobec powyższego EIOD zaleca dodanie do art. 9 wniosku przepisu stwierdzającego, że jakość danych osobowych przekazywanych z państw trzecich powinna być szczególnie oceniana, gdy tylko dane te zostaną otrzymane, oraz należy wskazać stopień ścisłości i wiarygodności tych danych.

IV.9 **Wymiana danych osobowych z podmiotami prywatnymi i organami innymi niż organy porządku publicznego**

109. Art. 13 i 14 wniosku ustanawiają zestaw wymogów, które mają być spełnione w przypadkach, gdy dane osobowe są dalej przekazywane podmiotom prywatnym i organom innym niż organy porządku publicznego. Jak to wcześniej wskazano, artykuły te uzupełniają bardziej ogólne zasady ustanowione w rozdziale II, których w każdym przypadku należy przestrzegać.

110. EIOD uważa, że powinny mieć zastosowanie szczególne i surowe warunki, ponieważ w szczególnych przypadkach do celów zapobiegania i zwalczania przestępczości może być konieczne przekazywanie danych podmiotom prywatnym i innym organom publicznym. Jest to zgodne z punktem widzenia wyrażonym przez europejskich inspektorów ochrony danych w dokumencie określającym stanowisko sporządzonym w Krakowie ([2]).

111. W tej perspektywie EIOD uważa, że dodatkowe warunki ustanowione w art. 13 i 14 mogą być uznane za satysfakcjonujące, jeżeli są stosowane razem z zasadami ogólnymi określonymi w rozdziale II, włączając w to kompleksowe stosowanie zasad dotyczących dalszego przetwarzania (patrz pkt IV.2 powyżej). Jednak obecny wniosek ogranicza stosowanie art. 13 i 14 w odniesieniu do danych otrzymanych lub udostępnianych przez właściwe organy innego państwa członkowskiego.

112. Ogólne stosowanie tych ostatnich warunków jest nawet bardziej istotne, jeżeli rozważy się rosnącą wymianę danych pomiędzy organami porządku publicznego i innymi organami lub podmiotami prywatnymi również w państwach członkowskich. Za przykład może posłużyć partnerstwo publiczno-prywatne w działaniach w zakresie ochrony porządku publicznego ([3]).

113. Wobec powyższego EIOD zaleca zmianę obecnego wniosku tak, aby zapewnić stosowanie art. 13 i 14 do wymiany *wszystkich* danych osobowych, także tych nieprzekazywanych lub nieudostępnianych przez inne państwo członkowskie. Zalecenie to nie odnosi się do art. 13 lit. c) ani do art. 14 lit. c).

Dostęp i dalsze wykorzystani danych osobowych kontrolowanych przez podmioty prywatne

114. Wymiana danych osobowych z podmiotami prywatnymi odbywa się w dwóch kierunkach: oznacza również przekazywanie lub udostępnianie danych osobowych przez podmioty prywatne organom porządku publicznego i sądowym.

115. W tym przypadku dane osobowe gromadzone do celów komercyjnych (transakcje handlowe, marketing, świadczenie usług, itd.) oraz zarządzane przez prywatnych kontrolerów są osiągane, a następnie wykorzystywane przez organy publiczne do bardzo różnych celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania. Ponadto ścisłość i wiarygodność danych przetwarzanych do celów komercyjnych jest uważnie oceniana, gdy dane te są wykorzystywane do celów ochrony porządku publicznego ([4]).

([1]) Konwencja NZ w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania podpisana przez wszystkie państwa członkowskie UE, która weszła w życie dnia 26 czerwca 1987 r. W szczególności art. 15 stwierdza, że „Każde Państwo Strona zapewni, aby jakiekolwiek oświadczenie, które, jak ustalono, zostało złożone w wyniku zastosowania tortur, nie zostało wykorzystane w charakterze dowodu w postępowaniu, z wyjątkiem wypadku, gdy jest ono wykorzystywane przeciwko osobie oskarżonej o stosowanie tortur, jako dowód na to, że oświadczenie zostało złożone".

([2]) Dokument przedstawiający stanowisko w sprawie egzekwowania prawa i wymiany informacji w UE, przyjęty na wiosennej konferencji europejskich organów ochrony danych w Krakowie w dniach 25-26 kwietnia 2005 r.

([3]) Patrz Program legislacyjny i program prac Komisji na 2006 r. COM(2005) 531 wersja ostateczna

([4]) Na przykład, rachunek telefoniczny będzie wiarygodny do celów komercyjnych, o ile prawidłowo określa, które rozmowy telefoniczne zostały wykonane; w każdym razie organy porządku publicznego nie mogą opierać się na tym samym rachunku telefonicznym, ponieważ brak jest rozstrzygających dowodów określających, kto wykonał daną rozmowę.

116. Niedawny i ważny przykład dostępu do prywatnych baz danych do celów ochrony porządku publicznego znajduje się w zatwierdzonym tekście dyrektywy w sprawie zatrzymywania danych w zakresie łączności (patrz pkt 16-18), zgodnie z którą dostawcy publicznie dostępnych usług łączności elektronicznej lub operatorzy publicznych sieci łączności będą musieli przechowywać do dwóch lat pewne dane związane z łącznością elektroniczną w celu zapewnienia dostępności tych danych do celów dochodzenia, wykrywania i ścigania poważnych przestępstw. Według zatwierdzonego tekstu kwestie dotyczące dostępu do tych danych wykraczają poza prawo wspólnotowe i nie mogą być regulowane przez samą dyrektywę. Natomiast te ważne zagadnienia mogą być przedmiotem prawa krajowego lub działań zgodnych z tytułem VI TUE ([1]).

117. W opinii w sprawie wniosku dotyczącego tej dyrektywy EIOD wystąpił w obronie szerszej wykładni traktatu WE, ponieważ ograniczenie dostępu jest niezbędne dla zapewnienia odpowiedniej ochrony osoby, której dane dotyczą i której dane w zakresie łączności elektronicznej muszą być zatrzymane. Niestety prawodawca europejski nie ujął w wyżej wymienionej dyrektywie zasad dotyczących dostępu.

118. W obecnej opinii EIOD ponownie podkreśla swoją wolę, aby prawo UE zapewniało wspólne normy dotyczące dostępu i dalszego wykorzystywania danych przez organy porządku publicznego. Jeżeli pierwszy filar nie zajmuje się konieczną ochroną, to instrument trzeciego filaru mógłby przewidzieć postanowienia jej dotyczące. To stanowisko EIOD jest odzwierciedleniem ogólnego wzrostu wymiany danych pomiędzy państwami członkowskimi i niedawnego wniosku w sprawie zasady dostępności. Różne zasady krajowe dotyczące zakresu i dalszego wykorzystywania danych nie byłyby zgodne z wnioskowanym „swobodnym przepływem" w całej UE informacji w zakresie ochrony porządku publicznego, który obejmuje również dane z prywatnych baz danych.

119. Wobec powyższego, EIOD uważa, że powinny mieć zastosowanie wspólne normy dotyczące dostępu przez organy porządku publicznego do danych znajdujących się w posiadaniu podmiotów prywatnych tak, aby umożliwić dostęp jedynie na podstawie dobrze zdefiniowanych warunków i ograniczeń. W szczególności należy zezwolić na dostęp przez właściwe organy jedynie w konkretnych przypadkach, na szczególnych warunkach, do szczególnych celów i pod sądową kontrolą państw członkowskich.

IV.10 **Prawa osób, których dane dotyczą**

120. Rozdział IV określa prawa osób, których dane dotyczą, w sposób, który jest w zasadzie zgodny z obecnym prawodawstwem w zakresie ochrony danych i z art. 8 Karty Praw Podstawowych UE.

121. EIOD z zadowoleniem przyjmuje te przepisy, ponieważ przewidują one zharmonizowany zestaw praw osób, których dane dotyczą, uwzględniając cechy charakterystyczne przetwarzania danych przez organy porządku publicznego i sądowe. Jest to istotna poprawa, ponieważ obecna sytuacja charakteryzuje się dużą różnorodnością zasad i praktyk, szczególnie dotyczących prawa dostępu. Niektóre państwa członkowskie nie zezwalają na dostęp osoby, której dane dotyczą, do jej danych, lecz wprowadzają system „dostępu pośredniego" (realizowanego przez krajowy organ ochrony danych w imieniu osoby, której dane dotyczą).

122. Zgodnie z wnioskiem, możliwe odstępstwa od bezpośredniego prawa dostępu są zharmonizowane. Jest to niezwykle ważne, aby zezwolić obywatelom, których dane są w coraz większej ilości przetwarzane i wymieniane przez właściwe organy różnych państw członkowskich UE, na skorzystanie jako osoby, których dane dotyczą, ze zharmonizowanego zestawu praw, bez względu na to, w którym państwie członkowskim dane są gromadzone i przetwarzane ([2]).

123. EIOD uznaje możliwość ograniczenia praw osób, których dane dotyczą, w przypadkach, gdy jest to konieczne do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania. W każdym razie z tego względu że ograniczenia te muszą być uznane za wyjątki od podstawowych praw osób, których dane dotyczą, należy zastosować surowy test proporcjonalności. Oznacza to, że należy ograniczyć i dobrze zdefiniować wyjątki oraz że ograniczenia powinny, w miarę możliwości, być częściowe i ograniczone w czasie.

124. W tej perspektywie EIOD pragnie zwrócić uwagę prawodawcy szczególnie na literę a) ustępu 2 artykułów 19, 29 i 21, które ustanawiają bardzo szeroki i niezdefiniowany wyjątek od prawa osób, których dane dotyczą, poprzez stwierdzenie, że prawa te mogą być ograniczone, jeśli jest to konieczne, „aby kontroler danych mógł w sposób właściwy wypełnić swoje zgodne z prawem obowiązki". Ponadto wyjątek ten częściowo pokrywa się z przepisem lit. b), który zezwala na ograniczenia praw osób, których dane dotyczą, jeżeli jest to konieczne, „aby uniknąć

([1]) Zgodnie z motywami dyrektywy: „Kwestie dotyczące dostępu krajowych organów publicznych do danych zatrzymywanych na mocy niniejszej dyrektywy do celów działań, o których mowa w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46/WE, wychodzą poza zakres zastosowania prawa wspólnotowego. Mogą one być jednak przedmiotem prawa krajowego lub działania na mocy tytułu VI Traktatu o Unii Europejskiej, przy czym należy zawsze odnotować, że takie prawa lub działania muszą w pełni szanować prawa podstawowe, ponieważ wynikają one ze wspólnych tradycji konstytucjonalnych państw członkowskich i są gwarantowane przez EKPC. Art. 8 EKPC, w wykładni Europejskiego Trybunału Praw Człowieka…"

([2]) W szczególności rozdział IV określa prawo do informacji (art. 19 i 20) oraz prawo dostępu do danych oraz do ich sprostowania, usunięcia lub zablokowania (art. 21). Generalnie artykuły te zapewniają osobom, których dane dotyczą wszelkie prawa, które są zwykle gwarantowane przez prawo UE w zakresie ochrony danych, a ponadto ustanawiają zestaw wyjątków mających na celu uwzględnienie szczególnych cech trzeciego filaru. W szczególności ograniczenia praw osób, których dane dotyczą są dozwolone na mocy prawie identycznych przepisów ustanowionych w odniesieniu do zarówno prawa do informacji (art. 19 ust. 2 i art. 20 ust. 2) i prawa dostępu (art. 21 ust. 2).

negatywnego wpływu na toczące się dochodzenie lub postępowanie lub na wypełnianie zgodnych z prawem obowiązków właściwych organów". Podczas gdy ten drugi wyjątek może być uznany za uzasadniony, to ten pierwszy wydaje się nakładać nieproporcjonalne ograniczenie na prawa osoby, której dane dotyczą. Wobec powyższego EIOD zaleca skreślenie lit. a) w ust. 2 art. 19, 20 i 21.

125. Ponadto, EIOD zaleca poprawę art. 19, 20 i 21 w następujący sposób:

— określenie, że ograniczenia praw podmiotu danych są nieobowiązkowe, nie mają zastosowania na czas nieokreślony i są dozwolone „wyłącznie" w szczególnych przypadkach wymienionych w artykułach,

— uwzględnienie, że kontroler dostarcza informacje autonomicznie, a nie na podstawie wniosku osoby, której dane dotyczą,

— dodanie w art. 19 ust. 1 lit. c), że informacje powinny być również dostarczane „w terminach przewidzianych dla przechowywania danych",

— zapewnienie (zmieniając art. 20 ust. 1) zgodnie z innymi instrumentami UE w zakresie ochrony danych), aby informacje — jeżeli dane nie zostały uzyskane od osoby, której dane dotyczą lub zostały uzyskane od tej osoby bez jej wiedzy — były tej osobie dostarczane „najpóźniej w terminie, gdy dane są ujawniane po raz pierwszy",

— zapewnienie, że mechanizm odwołania od decyzji odmownej lub ograniczające prawa osoby, której dane dotyczą, ma zastosowanie do przypadków ograniczenia prawa do informacji oraz odpowiednio zmienić ostatnie zdanie art. 19 ust. 4.

Zautomatyzowane decyzje indywidualne

126. EIOD żałuje, że wniosek w ogóle nie zajmuje się ważnymi zagadnieniami zautomatyzowanych decyzji indywidualnych. Rzeczywiście doświadczenie wskazuje, że organy porządku publicznego coraz częściej wykorzystują zautomatyzowane przetwarzanie danych mające na celu ocenę pewnych osobistych aspektów osób, w szczególności w celu oceny ich wiarygodności i postępowania.

127. EIOD — uznając, że te systemy mogą być konieczne w pewnych przypadkach w celu zwiększenia skuteczności działań w zakresie ochrony porządku publicznego — zauważa, że decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu danych powinny podlegać bardzo surowym warunkom i zabezpieczeniom, jeżeli mają skutki prawne dla danej osoby lub istotnie wpływają na tę osobę. Powyższe jest nawet jeszcze ważniejsze w kontekście trzeciego filaru, ponieważ w tym przypadku właściwe organy posiadają kompetencje w zakresie publicznych środków przymusu i przez to ich decyzje lub działania mogą wpływać na daną osobę lub mogą być bardziej naruszające niż byłyby normalnie, gdyby takie decyzje/działania były podjęte przez podmioty prywatne.

128. W szczególności i zgodnie z ogólnymi zasadami ochrony danych, takie decyzje lub działania powinny być dozwolone wyłącznie, gdy zezwala na nie prawo lub właściwy organ nadzoru, a ponadto powinny podlegać odpowiednim środkom mającym na celu zabezpieczenie zgodnych z prawem interesów osoby, której dane dotyczą. Ponadto osobie, której dane dotyczą powinno się szybko udostępnić środki umożliwiające przedstawienie punktu widzenia tej osoby, a ponadto powinna mieć możliwość poznania logiki decyzji, jeżeli nie jest to sprzeczne z celem, dla którego dane są przetwarzane.

129. Wobec powyższego EIOD zaleca wprowadzenie szczególnego przepisu dotyczącego zautomatyzowanych decyzji indywidualnych, zgodnego z obecnym prawodawstwem UE w zakresie ochrony danych.

IV.11 **Bezpieczeństwo przetwarzania danych**

130. W odniesieniu do przetwarzania danych, art. 24 ustanawia dla kontrolera obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które są zgodne z przepisami zawartymi w innych instrumentach UE dotyczących ochrony danych. Ponadto w ust. 2 przedstawiono szczegółową i kompleksową listę środków, które należy wdrożyć w odniesieniu do zautomatyzowanego przetwarzania danych.

131. EIOD z zadowoleniem przyjmuje ten przepis, ale proponuje, w celu ułatwienia organom nadzorczym skutecznej kontroli, dodanie następującego środka uzupełniającego do wykazu środków ustanowionych w ust. 2: *„k) wdrożenia środków w celu systematycznego monitorowania i składania sprawozdań w zakresie skuteczności tych środków bezpieczeństwa (systematyczny audyt własny środków bezpieczeństwa)"* [1].

Odnotowywanie danych

132. Art. 10 stwierdza, że każdorazowe zautomatyzowane przekazanie lub otrzymanie danych osobowych zostaje odnotowane (w przypadku zautomatyzowanego przekazania) lub udokumentowane (w przypadku niezautomatyzowanego przekazania) w celu zapewnienia późniejszej weryfikacji zgodności z prawem przekazania i przetwarzania danych. Informacje takie są dostępne, na wniosek, dla właściwego organu nadzoru.

[1] Patrz opinia EIOD w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego I Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, COM(2004) 835 wersja ostateczna, opublikowana na stronie

133. EIOD z zadowoleniem przyjmuje ten przepis. Jednak EIOD zauważa, że w celu zapewnienia kompleksowego nadzoru i sprawdzenia właściwego wykorzystania danych osobowych, również „dostęp" do danych będzie odnotowywany lub dokumentowany. Informacje te są niezbędne, ponieważ skuteczne monitorowanie właściwego przetwarzania danych osobowych musi koncentrować się nie tylko na zgodności z prawem przekazywania danych osobowych pomiędzy organami, ale również na zgodności z prawem dostępu do danych przez te organy ([1]). Wobec powyższego, EIOD zaleca zmianę art. 10 tak, aby zapewnić również odnotowanie lub dokumentowanie dostępu.

V.12 **Środki odwoławcze, odpowiedzialność i sankcje**

134. Rozdział VI wniosku obejmuje środki prawne (art. 27), odpowiedzialność (art. 28) i sankcje (art. 29). Przepisy są generalnie spójne z obecnym prawodawstwem UE w zakresie ochrony danych.

135. W szczególności w zakresie sankcji EIOD przyjmuje z zadowoleniem określenie, że w przypadku naruszenia przepisów ustanowionych zgodnie z decyzją ramową, sankcje będą musiały być skuteczne, odpowiednie i odstraszające. Ponadto sankcje karne w przypadku umyślnie popełnionych przestępstw wiążących się z poważnymi naruszeniami przepisów — szczególnie w zakresie poufności i bezpieczeństwa przetwarzania danych — zapewnią lepszy skutek odstraszający dla poważniejszych naruszeń prawa ochrony danych.

IV.13 **Zadania związane z kontrolą, nadzorem i doradztwem**

136. Przepisy wniosku, które odnoszą się do kontroli i nadzoru przetwarzania danych, a także konsultacji w zakresie kwestii dotyczących przetwarzania danych są w dużej mierze podobne do przepisów zawartych w dyrektywie 95/46/WE. EIOD z zadowoleniem przyjmuje fakt, że Komisja w swoim wniosku opowiedziała się za już przetestowanymi i dobrze funkcjonującymi mechanizmami oraz podkreśla w szczególności wprowadzenie (obowiązkowego) systemu kontroli wstępnej. System taki jest nie tylko przewidziany w dyrektywie 95/46/WE, ale jest również włączony do rozporządzenia 45/2001/WE; system ten wykazał, że jest skutecznym instrumentem nadzoru przetwarzania danych przez instytucje i organy Wspólnot Europejskich znajdującym się w gestii EIOD.

137. Innym instrumentem kontroli i nadzoru przetwarzania danych, który wykazał się skutecznością, jest mianowanie inspektorów ochrony danych przez kontrolera. Instrument ten funkcjonuje w kilku państwach członkowskich. Jest on ustanowiony w rozporządzeniu 45/2001/WE jako obowiązkowy instrument i odgrywa kluczową rolę na szczeblu Wspólnot Europejskich. Inspektorzy ochrony danych są administratorami w organizacji, która zapewnia w sposób niezależny wewnętrzne zastosowanie przepisów w zakresie ochrony danych.

138. EIOD zaleca dodanie do wniosku przepisów w zakresie inspektorów ochrony danych. Przepisy te mogłyby być podobne do przepisów art. 24 rozporządzenia 45/2001/WE.

139. Wniosek dotyczący decyzji ramowej jest skierowany do państw członkowskich. Zatem logiczne jest, aby art. 30 wniosku przewidywał nadzór prowadzony przez niezależne organy nadzoru. Artykuł ten jest sformułowany w podobny sposób jak art. 28 dyrektywy 95/46/WE. Te organy krajowe powinny współpracować między sobą, ze wspólnymi organami nadzoru ustanowionymi w tytule VI traktatu o UE oraz z EIOD. Ponadto art. 31 wniosku przewiduje ustanowienie grupy roboczej, która musi odgrywać podobną rolę do tej, jaką odgrywa Grupa Robocza Art. 29 w zakresie zagadnień związanych z pierwszym filarem. Wszystkie istotne podmioty w obszarze ochrony danych są wymienione w art. 31 wniosku.

140. Nie zostało wskazane, że we wniosku, który przewiduje poprawę współpracy policyjnej i sądowej pomiędzy państwami członkowskimi, istotną rolę odgrywa współpraca pomiędzy wszystkimi istotnymi podmiotami w obszarze ochrony danych. Wobec powyższego EIOD z zadowoleniem przyjmuje podkreślenie roli współpracy pomiędzy organami nadzoru we wniosku.

141. Ponadto EIOD podkreśla wagę spójnego podejścia w zakresie zagadnień ochrony danych, które mogłoby zostać wzmocnione poprzez wspieranie komunikacji pomiędzy istniejącą Grupą Roboczą Art. 29 a grupą roboczą ustanowioną na mocy obecnego wniosku dotyczącego decyzji ramowej. EIOD zaleca zmianę art. 31 ust. 2 wniosku tak, aby dać prawo przewodniczącemu Grupy Roboczej Art. 29 do udziału lub bycia reprezentowanym na posiedzeniach nowej grupy roboczej.

142. Tekst art. 31 obecnego wniosku zawiera jedną istotną różnicę w stosunku do art. 29 dyrektywy 95/46/WE. EIOD jest pełnoprawnym członkiem Grupy Roboczej art. 29. Członkostwo to oznacza również prawo głosu. Obecny wniosek również wyznacza EIOD na członka grupy roboczej (w oparciu o art. 31), ale nie przewiduje prawa głosu dla EIOD. Nie są jasne przyczyny, dla których obecny wniosek odchodzi od art. 29 dyrektywy 95/46/WE. Według EIOD wnioskowany tekst jest dwuznaczny co do roli EIOD; może to zmniejszyć skuteczność zaangażowania EIOD w prace grupy roboczej. Wobec powyższego EIOD zaleca zachowanie spójności z tekstem dyrektywy.

([1]) Jest to zgodne z przepisami ustanowionymi w art. 18 wniosku, zgodnie z którymi organ przekazujący zostanie poinformowany, na wniosek, w kwestii dalszego przetwarzania danych osobowych przekazywanych lub udostępnianych oraz z przepisami ustanowionymi w art. 24 wykonującym środki bezpieczeństwa, także w świetle wnioskowanego systematycznego audytu własnego tych środków.

IV.14 **Pozostałe przepisy**

143. Rozdział VIII wniosku zawiera niektóre końcowe przepisy zmieniające konwencję z Schengen i inne instrumenty dotyczące przetwarzania i ochrony danych osobowych.

Konwencja z Schengen

144. Art. 33 wniosku przewiduje, że art. 126-130 konwencji z Schengen zostaną zastąpione decyzją, o której mowa w zakresie zagadnień objętych zakresem Traktatu o UE. Art. 126-130 konwencji z Schengen zawierają ogólne zasady dotyczące przetwarzanie danych przekazywane zgodnie z konwencją (ale poza Systemem Informacyjnym Schengen).

145. EIOD z zadowoleniem przyjmuje to zastąpienie, ponieważ poprawia ono spójność systemu ochrony danych w trzecim filarze i stanowi w pewnych aspektach istotną poprawę ochrony danych osobowych, na przykład poprzez zwiększenie kompetencji organów nadzoru. Jednakże w pewnych punktach zastąpienie to wywiera niezamierzony — i niefortunny — skutek obniżenia poziomu ochrony danych. Niektóre przepisy konwencji z Schengen są rzeczywiście surowsze niż przepisy decyzji ramowej.

146. EIOD szczególnie przywołuje art. 126 ust. 3 lit. b) konwencji z Schengen, który stwierdza, że dane mogą być wykorzystywane jedynie przez organy sądowe oraz służby i organy wykonujące zadania lub obowiązki w związku z celami określonymi w konwencji. Przepis ten wydaje się wyłączać przekazywanie danych podmiotom prywatnym, podczas gdy byłoby to dozwolone na mocy wnioskowanej decyzji ramowej. Kolejnym punktem jest to, że przepisy w zakresie ochrony danych konwencji z Schengen mają również zastosowanie do *wszystkich* danych przekazywanych z *niezautomatyzowanego* pliku oraz włączonych do *niezautomatyzowanego* pliku danych (art. 127), przy czym pliki nieustrukturalizowane są wyłączone z zakresu wnioskowanej decyzji ramowej.

Konwencja o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej

147. Art. 34 stwierdza, że art. 23 Konwencji o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej zostaje zastąpiony decyzją ramową. EIOD zauważa, że chociaż to zastąpienie generalnie zapewniłoby lepszą ochronę danych osobowych wymienianych w ramach konwencji, to mogłoby również spowodować powstanie pewnych problemów związanych ze spójnością tych dwóch instrumentów.

148. W szczególności konwencja obejmuje również wzajemną pomoc odnoszącą się do przechwyceń w zakresie telekomunikacji. W tym przypadku państwo członkowskie, do którego skierowano wniosek może wyrazić zgodę — na przechwycenie lub przekazanie zapisu telekomunikacyjnego — z uwzględnieniem wszelkich warunków, jakich należy przestrzegać w podobnych przypadkach na szczeblu krajowym. Zgodnie z art. 23 ust. 4 Konwencji, w przypadku gdy te dodatkowe warunki odnoszą się do wykorzystania danych osobowych, będą one miały pierwszeństwo nad zasadami dotyczącymi ochrony danych określonymi w art. 23. Podobnie art. 23 ust. 5 określa pierwszeństwo dodatkowych zasad dotyczących zabezpieczenia informacji gromadzonych przez wspólne zespoły dochodzeniowe. EIOD zauważa, że jeżeli art. 23 zostanie zastąpiony przez obecny wniosek, to będzie niejasne, czy wyżej wymienione dodatkowe zasady będą nadal miały zastosowanie. Wobec powyższego EIOD zaleca wyjaśnienie tego punktu w celu dogłębnej oceny skutków pełnego zastąpienia art. 23 konwencji przez decyzję ramową, o której mowa.

Konwencja Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych

149. Art. 34 ust. 2 stwierdza, że wszelkie odniesienia do konwencji Rady Europy nr 108 należy rozumieć jako odniesienia do decyzji ramowej, o której mowa. Wykładnia i konkretne stosowanie tego przepisy nie są jasne. W każdym razie EIOD stwierdza, że przepis ten ma zastosowanie jedynie w zakresie *ratione materiae* decyzji ramowej, o której mowa.

Zagadnienia końcowe

150. W odniesieniu do systematycznej spójności tekstu, EIOD zauważa, że niektóre artykuły mogłyby zostać lepiej umiejscowione w tekście wniosku.

Wobec powyższego EIOD proponuje:

1. przeniesienie art. 16 („Komitet") z rozdziału III („Szczególne formy przetwarzania") do nowego rozdziału;

2. przeniesienie art. 25 („Rejestr") i art. 26 („Kontrola wstępna") z rozdziału V („Poufność i bezpieczeństwo przetwarzania danych") do nowego rozdziału

V. **WNIOSKI**

Istotny krok do przodu

a) Przyjęcie omawianego wniosku stanowiłoby znaczący krok w zakresie ochrony danych osobowych w ważnej dziedzinie, która szczególnie wymaga spójnego i skutecznego mechanizmu ochrony danych osobowych na szczeblu Unii Europejskiej.

b) Skuteczna ochrona danych osobowych ma znaczenie nie tylko dla osób, których dane dotyczą, ale ma również korzystny wpływ na skuteczność samej współpracy policyjnej i sądowej. Pod wieloma względami interesy te są zbieżne.

Wspólne normy

c) Według EIOD nowe ramy ochrony danych powinny nie tylko być zgodne z zasadami ochrony danych — należy zagwarantować spójność ochrony danych w ramach Unii Europejskiej — ale również określić zestaw dodatkowych zasad uwzględniających szczególny charakter dziedziny ochrony porządku publicznego.

d) Obecny wniosek spełnia te warunki: zapewnia, stosowanie istniejących zasad ochrony danych ustanowione w dyrektywie 95/46/WE w obszarze trzeciego filaru, ponieważ większość przepisów wniosku odzwierciedla instrumenty prawne UE w zakresie ochrony danych osobowych i jest spójna z tymi instrumentami prawnymi. Ponadto przewiduje wspólne normy określające te zasady, mając na uwadze ich zastosowanie w tej dziedzinie, które są generalnie rzecz ujmując satysfakcjonujące dla zapewnienia odpowiednich zabezpieczeń ochrony danych w trzecim filarze.

Stosuje się do wszelkiego rodzaju przetwarzania danych

e) Istotnym czynnikiem umożliwiającym osiągnięcie celu decyzji ramowej jest, by jej zakres obejmował wszystkie dane policyjne i sądowe, nawet jeżeli nie są one przekazywane ani udostępniane przez właściwe organy innych państw członkowskich.

f) Art. 30 ust. 1 lit. b) i art. 31 ust. 1 lit. c) TUE stanowią podstawę prawną zasad ochrony danych, która nie ogranicza się do ochrony danych osobowych faktycznie wymienianych pomiędzy właściwymi organami państw członkowskich, ale dotyczy także sytuacji krajowych.

g) Wniosek nie ma zastosowania do przetwarzania danych w ramach drugiego filaru traktatu o UE (wspólna polityka zagraniczna i bezpieczeństwa) ani też do przetwarzania danych przez służby wywiadowcze oraz dostępu tych służb do tych danych, gdy są one przetwarzane przez właściwe organy lub inne strony (wynika to z art. 33 TUE). W tych dziedzinach prawo krajowe powinno zapewniać odpowiednią ochronę osób, których dane dotyczą. Ta luka w zakresie ochrony na szczeblu UE wymaga jeszcze skuteczniejszej ochrony w dziedzinach, które wniosek obejmuje.

h) EIOD z zadowoleniem przyjmuje fakt, że wniosek rozszerza swój zakres o dane osobowe przetwarzane przez organy sądowe.

W odniesieniu do innych instrumentów prawnych

i) W przypadku gdy jakikolwiek inny szczególny instrument prawny na podstawie tytułu VI traktatu o UE przewiduje bardziej szczegółowe warunki lub ograniczenia dla przetwarzania lub dostępu do danych, zastosowanie powinny mieć przepisy szczególnego instrumentu prawnego, jako *lex specialis*.

j) Omawiany wniosek dotyczący decyzji ramowej Rady w sprawie ochrony danych jest ważny sam w sobie, a jego przyjęcie jest niezbędne nawet w przypadku braku instrumentu prawnego dotyczącego dostępności (zgodnie z wnioskiem Komisji z dnia 12 października 2005 r.)

k) W związku z zatwierdzeniem przez Parlament Europejski dyrektywy w sprawie zatrzymywania danych w zakresie łączności kwestia ustanowienia ram prawnych dla ochrony danych w ramach trzeciego filaru staje się jeszcze pilniejsza.

Struktura wniosku

l) Dodatkowe zasady określone w rozdziale II (oprócz ogólnych zasad zawartych w dyrektywie 95/46/WE) powinny zapewniać dodatkową ochronę osobom, których dane dotyczą, w związku z szczególnym kontekstem trzeciego filaru, ale nie mogą one prowadzić do niższego poziomu ochrony.

m) Rozdział III dotyczący szczególnych form przetwarzania (do którego włączono trzecią warstwę ochrony) nie może naruszać przepisów rozdziału II. Przepisy rozdziału III powinny zapewniać dodatkową ochronę osobom, których dane dotyczą, w sytuacjach, gdy dotyczy to właściwych organów więcej niż jednego państwa członkowskiego, przy czym przepisy te nie mogą prowadzić do niższego poziomu ochrony.

n) Przepisy dotyczące weryfikacji jakości danych (art. 9 ust. 1 i 6) oraz regulujące dalsze przetwarzanie danych osobowych (art. 11 ust.1) powinny zostać przeniesione do rozdziału II i stosowane do wszystkich rodzajów przetwarzania danych przez organy porządku publicznego, nawet jeśli dane osobowe nie zostały przekazane ani udostępnione przez inne państwo członkowskie. Jest to w szczególności niezbędne — zarówno w interesie osób, których dane dotyczą, jak i właściwych organów — dla zapewnienia, że właściwa weryfikacja jakości dotyczy wszystkich danych osobowych.

Ograniczenie celu

o) Wniosek nie określa w sposób zadowalający pewnej sytuacji, która może wydarzyć się podczas pracy policji: a mianowicie, potrzeby dalszego wykorzystywania danych do celów uznanych za niezgodne z celem, dla które zostały zebrane.

p) Zgodnie z prawem UE dotyczącym ochrony danych, dane osobowe muszą być gromadzone do określonych i wyraźnych celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Trzeba zezwolić na pewną elastyczność w odniesieniu do dalszego wykorzystania. Jest bardziej prawdopodobne, że ograniczenie dotyczące gromadzenia danych jest faktycznie przestrzegane, jeżeli organy odpowiedzialne za wewnętrzne bezpieczeństwo wiedzą, że mogą polegać, przy odpowiednich zabezpieczeniach, na odstępstwie od ograniczenia w odniesieniu do dalszego wykorzystania.

q) Decyzja ramowa powinna określać w rozdziale II, że państwom członkowskim powinno się zezwolić na przyjęcie środków legislacyjnych w celu umożliwienia dalszego przetwarzania, gdy środek taki jest konieczny do zabezpieczenia:

— zapobiegania zagrożeniom bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego;

— ochrony ważnego interesu gospodarczego lub finansowego państwa członkowskiego.

— ochrona osoby, której dane dotyczą.

Do tych kompetencji państw członkowskich może należeć również przetwarzanie naruszające prywatność i wobec tego muszą mu towarzyszyć surowe warunki.

Konieczność i proporcjonalność

r) Zasady konieczność i proporcjonalności wniosku powinny w pełni odzwierciedlać orzecznictwo Europejskiego Trybunału Praw Człowieka poprzez zapewnienie, że przetwarzanie danych osobowych uważane jest za konieczne jedynie w przypadku, gdy właściwe organu mogą wykazać jego wyraźną potrzebę oraz o ile nie są dostępne środki mniej naruszające prywatność.

Wymiana danych osobowych z państwami trzecimi

s) Przekazywanie państwom trzecim danych bez zapewnienia ochrony osób, których dane dotyczą, poważnie naruszyłoby ochronę danych przewidzianą w obecnym wniosku na terytorium Unii Europejskiej. EIOD zaleca zmianę obecnego wniosku tak, aby zapewnić stosowanie art. 15 do wymiany *wszystkich* danych osobowych z państwami trzecimi. Zalecenie to nie odnosi się do art. 15 ust. 1 lit. c).

t) W przypadku gdy dane osobowe są przekazywane z krajów trzecich, ich jakość powinna być przed ich wykorzystaniem uważnie oceniana w świetle poszanowania praw człowieka i norm ochrony danych.

Wymiana danych osobowych z podmiotami prywatnymi i organami innymi niż organy porządku publicznego

u) Powinny mieć zastosowanie szczególne i surowe warunki, ponieważ w szczególnych przypadkach do celów zapobiegania i zwalczania przestępczości może być konieczne przekazywanie danych podmiotom prywatnym i innym organom publicznym. EIOD zaleca zmianę obecnego wniosku tak, aby zapewnić stosowanie art. 13 i 14 do wymiany *wszystkich* danych osobowych, także tych niepotrzymanych lub nieudostępnianych przez inne państwo członkowskie. Zalecenie to nie odnosi się do art. 13 lit. c) ani do art. 14 lit. c).

v) Powinny mieć zastosowanie wspólne normy dotyczące dostępu przez organy porządku publicznego do danych znajdujących się w posiadaniu podmiotów prywatnych tak, aby umożliwić dostęp jedynie na podstawie dobrze zdefiniowanych warunków i ograniczeń.

Szczególne kategorie danych

w) Szczególne zabezpieczenia powinno się przewidzieć w szczególności w celu zagwarantowania, aby:

— dane biometryczne i profile DNA były wykorzystane jedynie na podstawie dobrze określonych i interoperacyjnych norm technicznych,

— ich stopień ścisłości był uważnie uwzględniony i mógł być podważony przez osobę, której dane dotyczą przy pomocy dostępnych sposobów, oraz

— było w pełni zapewnione poszanowanie godności osób.

Rozróżnienie na różne kategorie danych

x) Dane osobowe dotyczące różnych kategorii osób (podejrzany, skazany, ofiara, świadek, itd.) powinny być przetwarzane zgodnie z różnymi odpowiednimi warunkami i zabezpieczeniami. Wobec powyższego EIOD proponuje dodanie nowego ustępu do art. 4, który zawierałby następujące elementy:

— obowiązek państw członkowskich określenia konsekwencji prawnych rozróżnienia, które zostanie dokonane na dane osobowe różnej kategorii osób;

— dodatkowe przepisy ograniczające cel przetwarzania, określające dokładne terminy i ograniczające dostęp do danych, w przypadku gdy jest mowa o osobach niebędących podejrzanymi.

Zautomatyzowane decyzje indywidualne

y) Decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu danych powinny podlegać bardzo surowym warunkom, jeżeli mają skutki prawne dla danej osoby lub istotnie wpływają na tę osobę. W tym przypadku EIOD zaleca wprowadzenie szczególnych przepisów dotyczących zautomatyzowanych decyzji indywidualnych, podobnych do przepisów dyrektywy 95/46/WE.

Zestawienie innych zaleceń

z) EIOD zaleca:

— przeformułowanie pierwszego tiret art. 4 ust. 4 tak, aby zapewnić poszanowanie orzecznictwa w zakresie art. 8 EKPC, ponieważ wnioskowane sformułowanie art. 4 ust. 4 nie spełnia kryteriów określonych w orzecznictwie Europejskiego Trybunału Praw Człowieka odnoszącym się do art. 8 EKPC;

— usunięcie ogólnego odstępstwa, o którym mowa w art. 7 ust. 1 lub przynajmniej wyraźne ograniczenie interesów publicznych uzasadniających korzystanie z tego odstępstwa przez państwa członkowskie;

— zmianę art. 10 tak, aby zapewnić również odnotowanie lub dokumentowanie dostępu do danych;

— skreślenie lit. a) w ust. 2 art. 19, 20 i 21;

— dodanie do wniosku przepisów w zakresie inspektorów ochrony danych; Przepisy te mogłyby być podobne do przepisów art. 24-26 rozporządzenia 45/2001/WE.

— zmianę art. 31 ust. 2 wniosku tak, aby dać prawo przewodniczącemu Grupy Roboczej art. 29 do udziału lub bycia reprezentowanym na posiedzeniach nowej grupy roboczej.

Sporządzono w Brukseli dnia 19 grudnia 2005 r.,

Peter HUSTINX

Europejski Inspektor Ochrony Danych