

**Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 515/97 w sprawie wzajemnej pomocy między organami administracyjnymi państw członkowskich i współpracy między państwami członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego (COM(2006) 866 wersja ostateczna)**

(2007/C 94/02)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych<sup>(1)</sup>,

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych<sup>(2)</sup>, w szczególności jego art. 41,

uwzględniając wniosek w sprawie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 otrzymany od Komisji w dniu 4 stycznia 2007 r.;

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

#### WPROWADZENIE

1. Cel wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 515/97 z 13 marca w sprawie wzajemnej pomocy między organami administracyjnymi państw członkowskich i współpracy między państwami członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego<sup>(3)</sup> (zwanego dalej „wnioskiem”), jest dwojaki. Po pierwsze, wniosek ma na celu dostosowanie bieżącego rozporządzenia Rady (WE) nr 515/97 do nowych uprawnień Wspólnoty w dziedzinie wspólnotowej współpracy celnej. Po drugie, wniosek ma na celu zacieśnienie współpracy i wymiany informacji między państwami członkowskimi oraz między nimi a Komisją.
2. By osiągnąć te dwa cele, wniosek zakłada między innymi zwiększenie funkcjonalności bieżącego systemu informacji

celnej („SIC”) i tworzy dodatkowy europejski zbiór danych, który będzie obrazował przemieszczanie się kontenerów lub środków transportu, jak również odpowiednich towarów i osób („europejski zbiór danych”).

3. Ponadto wniosek wprowadza do prawa wspólnotowego identyfikującą bazę danych rejestru celnego (FIDE), pierwotnie utworzoną przez państwa członkowskie na mocy tytułu VI Traktatu o Unii Europejskiej<sup>(4)</sup>. Od chwili obecnej FIDE będzie mieściła się zarówno w zakresie działań Wspólnoty Europejskiej, jak i w ramach trzeciego filara, przy czym w każdej z tych sytuacji funkcjonowanie FIDE będzie regulował odpowiedni akt prawny. Ta sama sytuacja odnosi się do SIC<sup>(5)</sup>. W praktyce dokonuje się tego przez utworzenie dwóch baz danych, które udostępnia się różnym podmiotom w celu umożliwienia ich wykorzystania do różnych celów (pierwszy i trzeci filar).

#### I. Konsultacja z Europejskim Inspektorem Ochrony Danych

4. Komisja przesłała wniosek Europejskiemu Inspektorowi Ochrony Danych („EIOD”) w celu przeprowadzenia konsultacji zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 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 (dalej zwanym „rozporządzeniem (WE) nr 45/2001”). EIOD otrzymał wniosek w dniu 4 stycznia 2007 r.
5. Uwzględniając wiążący charakter art. 28 ust. 2 rozporządzenia (WE) nr 45/2001, niniejsza opinia powinna zostać wspomniana w preambule do wniosku przed motywami. W tym celu EIOD proponuje zastosowanie brzmienia wykorzystywanego w innych wnioskach legislacyjnych, odnoszącego się do opinii<sup>(6)</sup> EIOD, a które przedstawia się jak następuje: „po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych”.

<sup>(1)</sup> Dz.U. L 281 z 23.11.1995, str. 31.

<sup>(2)</sup> Dz.U. L 8 z 12.1.2001, str. 1.

<sup>(3)</sup> Dz.U. L 82 z 22.3.1997, str. 1.

<sup>(4)</sup> Protokół sporządzony zgodnie z art. 34 Traktatu o UE zmieniający w zakresie utworzenia identyfikacyjnej bazy danych Konwencję o wykorzystaniu technologii informatycznej dla potrzeb celnych oraz Konwencję o SIC. Rada przyjęła protokół w drodze aktu z dnia 8 maja 2003 r. (2003/C 139/01), C139/1 opublikowanego w dniu 13.6.2003.

<sup>(5)</sup> Podstawa prawna do międzyrządowej bazy danych jest konwencja o SIC, Konwencja sporządzona na podstawie Art. K3 Traktatu o Unii Europejskiej o wykorzystaniu technologii informatycznej dla potrzeb celnych, Dz.U. C 316 z 27.11.1995, str. 34.

<sup>(6)</sup> Patrz wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniający rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF).

## II. Znaczenie wniosku z punktu widzenia ochrony danych

6. Tworzenie i ulepszanie różnych aktów służących zacieśnianiu współpracy we Wspólnocie, tj. SIC, FIDE oraz europejskiego zbioru danych, pociąga za sobą zwiększenie ilości danych osobowych, które będą gromadzone i wymieniane między organami administracyjnymi państw członkowskich, a w niektórych przypadkach także między państwami trzecimi. Przetwarzane i przekazywane dane osobowe mogą zawierać informacje o rzekomym lub udowodnionym udziale danych osób w działaniach niedozwolonych w obszarze celnym lub rolnym. Z tego punktu widzenia wniosek ma znaczące skutki w zakresie ochrony danych osobowych. Ponadto jego znaczenie zwiększa się, jeśli wziąć pod uwagę rodzaj gromadzonych i przekazywanych danych, zwłaszcza podejrzania o udział danych osób w działaniach niedozwolonych, jak również ogólny cel i wyniki przetwarzania.
7. W świetle skutków wniosku dla ochrony danych osobowych EIOD uważa za stosowne przedstawienie niniejszej opinii analizującej wpływ wniosku na ochronę praw i swobód osób fizycznych w odniesieniu do przetwarzania danych osobowych.

## III. Główne elementy wniosku i uwagi wstępne

8. Główne elementy wniosku mające znaczenie z punktu widzenia ochrony danych to: (i) utworzenie europejskiego zbioru danych (art. 18a i 18b); (ii) przepisy aktualizujące zasady dotyczące SIC (art. 23–37), oraz (iii) zasady przedstawiające FIDE jako wspólnotową bazę danych (art. 41a–41d). Znaczenie również mają różne przepisy, w tym przepisy dotyczące nadzoru nad ochroną danych, które zostały zmienione, by uwzględnić przyjęcie rozporządzenia (WE) nr 45/2001 (art. 37, 42 i 43).
9. EIOD przypomina, że w swojej poprzedniej opinii na temat projektu rozporządzenia dotyczącego wzajemnej pomocy administracyjnej w celu ochrony interesów finansowych Wspólnoty przed nadużyciami finansowymi i wszelkimi innymi działaniami niezgodnymi z prawem<sup>(7)</sup> zwrócił uwagę na potrzebę dostosowania niektórych przepisów rozporządzenia Rady (WE) nr 515/97 w celu przystosowania go do nowych przepisów prawa w dziedzinie ochrony danych osobowych odnoszących się do instytucji UE, w szczególności do rozporządzenia (WE) nr 45/2001. EIOD jest zatem zadowolony z odpowiednich poprawek we wniosku.
10. Ponadto EIOD z zadowoleniem dostrzega, że przepisy przedstawiające europejski zbiór danych oraz aktualizujące zasady dotyczące SIC zawierają zabezpieczenia mające na

celu zapewnienie ochrony danych osobowych osób fizycznych oraz ich prywatności. EIOD z zadowoleniem przyjmuje także decyzję o wprowadzeniu FIDE do prawa wspólnotowego, obejmując ją zakresem rozporządzenia (WE) nr 45/2001.

11. EIOD dostrzega znaczenie celów, do których dąży wniosek, mianowicie zacieśnienie współpracy zarówno między samymi państwami członkowskimi, jak i między nimi a Komisją. Uznaje on także potrzebę utworzenia lub zaktualizowania instrumentów takich jak SIC i FIDE, aby te cele osiągnąć. Ponadto EIOD z zadowoleniem dostrzega, że wniosek, działając w tym kierunku, obejmuje zabezpieczenia uwzględniające obecne prawodawstwo w zakresie ochrony danych osobowych obowiązujące instytucje UE. EIOD uważa jednak, że istnieje możliwość poprawy, tak by zapewnić ogólną zgodność wniosku z istniejącymi ramami prawnymi dotyczącymi ochrony danych i skutecznej ochrony danych osobowych osób fizycznych. W tym celu EIOD przedstawia uwagi i propozycje zamieszczone w następującej części.

## ANALIZA WNIOSKU

### I. Utworzenie europejskiego zbioru danych

12. Zgodnie z art. 18a ust. 1 wniosku Komisja utworzy europejski zbiór danych i będzie nim zarządzała w celu „wykrywania przemieszczania się towarów mogących być przedmiotem działań sprzecznych z przepisami prawa celnego lub rolnego i środków transportu”. Komisja będzie uzyskiwała większość danych od publicznych lub prywatnych podmiotów świadczących usługi, działających w międzynarodowym łańcuchu logistycznym lub zajmujących się przewozem towarów. Zbiór może być wzbogacony o dane „z innych źródeł” na podstawie art. 18a ust. 2 lit. b). Art. 18a ust. 3 wyszczególnia dane, które mogą znaleźć się w zbiorze, między innymi dane osobowe<sup>(8)</sup>. Komisja będzie udostępniała dane ze zbioru właściwym organom w państwach członkowskich.
13. Wniosek stwierdza, że utworzenie zbioru będzie przydatne w wykrywaniu działań stanowiących ryzyko nieprawidłowości w zakresie przepisów prawa celnego i rolnego. EIOD uważa jednak, że — jak powinno być w każdym przypadku, gdy zostaje utworzona centralna baza danych zawierająca dane osobowe — należy odpowiednio i starannie oszacować potrzebę utworzenia takiej bazy danych, a gdy jest już ona utworzona, należy wprowadzić szczególnie zabezpieczenia na podstawie zasad ochrony danych. Celem tych działań jest uniknięcie wszelkich zdarzeń, które mogłyby w niewłaściwy sposób wpłynąć na ochronę danych osobowych.

<sup>(7)</sup> Opinia Europejskiego Inspektora Ochrony Danych Osobowych na temat projektu rozporządzenia Parlamentu Europejskiego i Rady dotyczącego wzajemnej pomocy administracyjnej w celu ochrony interesów finansowych Wspólnoty przed nadużyciami finansowymi i wszelkimi innymi działaniami niezgodnymi z prawem (COM(2004) 509 wersja ostateczna z dnia 20 lipca 2004 r.), Dz.U. C 301 z 7.12.2004, str. 4.

<sup>(8)</sup> W art. 18 ust. 3 lit. c) informacje odnoszące się do danych osobowych obejmują powyżej „nazwisko, nazwisko panięskie, imiona, pseudonimy, datę i miejsce urodzenia, narodowość, płeć oraz adres właścicieli, załadowców, odbiorców, pośredników przewozowych lub innych pośredników lub osoby zaangażowane w międzynarodowy łańcuch logistyczny i przewóz towarów.”

14. EIOD uważa, że wniosek nie przedstawia wystarczających argumentów na rzecz potrzeby utworzenia zbioru. W celu dopilnowania, aby tworzone były jedynie rzeczywiście potrzebne bazy danych, EIOD wzywa Komisję do dokonania odpowiedniej oceny potrzeby utworzenia zbioru i do przedstawienia sprawozdania z jej rezultatów.
15. Jeżeli chodzi o zabezpieczenia z zakresu ochrony danych, EIOD zauważa, że wniosek zakłada pewne zabezpieczenia; EIOD uważa jednak, że konieczne są dodatkowe środki.
19. EIOD przypomina, że Komisja, przestrzegając przepisów rozporządzenia (WE) nr 45/2001, będzie między innymi zobowiązana do informowania o tym fakcie osób, których nazwiska figurują w zbiorze<sup>(10)</sup>. W szczególności należy mieć na uwadze to, że prawo takie istnieje, nawet jeśli dane osobowe w zbiorze zostały pozyskane z publicznych źródeł. Ponadto, biorąc pod uwagę cel istnienia zbioru, Komisja będzie związana art. 27 rozporządzenia 45/2001, zgodnie z którym EIOD musi sprawdzić system przed jego uruchomieniem<sup>(11)</sup>.

#### I.1. Zastosowanie rozporządzenia (WE) nr 45/2001

16. EIOD zauważa, że biorąc pod uwagę fakt, iż Komisja utworzy europejski zbiór danych i będzie nim zarządzała oraz że zbiór będzie zawierał dane osobowe, ma do niego zastosowanie rozporządzenie nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych. Wobec tego Komisja, w ramach swoich kompetencji jako kontrolera danych zbioru<sup>(9)</sup>, musi zapewnić przestrzeganie wszystkich przepisów rozporządzenia.

17. Zważywszy, że wobec powyższego rozporządzenie (WE) nr 45/2001 ma zastosowanie *per se* do utworzenia zbioru i zarządzania nim, EIOD uważa, że z przyczyn spójności odpowiednie będzie wprowadzenie nowego ustępu przypominającego o zastosowaniu tego rozporządzenia. EIOD faktycznie odnotowuje, że art. 34 wniosku dotyczącego systemu informacji celnej (SIC) i identyfikującej bazy danych rejestru celnego („FIDE”) zawiera przepis przypominający o zastosowaniu rozporządzenia (WE) nr 45/2001. Aby być konsekwentnym w podejściu, należy wprowadzić podobny przepis dotyczący tego zbioru. EIOD proponuje zatem, aby art. 18 ust. 1 zawierał nowy ustęp o brzmieniu zapożyczonym z art. 34: „Komisja uważa europejski zbiór danych za system przetwarzania danych osobowych podlegający przepisom rozporządzenia (WE) nr 45/2001”.

18. EIOD odnotowuje, że art. 18a ust. 2 lit. b) wniosku potwierdza zastosowanie rozporządzenia (WE) nr 45/2001 do niektórych sposobów wykorzystania zbioru, zwłaszcza gdy Komisja wykorzystuje zbiór do „tworzenia zestawień udostępnionych danych...ich indeksowania, wzbogacania...”. O ile nie ma ogólnego stwierdzenia potwierdzającego zastosowanie rozporządzenia (WE) nr 45/2001 do zbioru jako całości, łącznie z działaniami przetwarzającymi wykonanymi od utworzenia zbioru do zarządzania nim, wszelkie inne działania/etapy nieokreślone wyraźnie w art. 18a ust. 2 lit. b) można uważać za nieobjęte rozporządzeniem (WE) nr 45/2001. Jest to kolejny powód uzasadniający wprowadzenie sformułowania proponowanego powyżej.

<sup>(9)</sup> Kontrolerzy danych są to osoby lub organy określające cele i sposoby przetwarzania danych zarówno w sektorze publicznym, jak i prywatnym.

#### I.2. Zastosowanie przepisów krajowych wdrażających dyrektywę 95/46/WE

20. Na mocy art. 18a ust. 2 lit. c) wniosku Komisja jest uprawniona do udostępniania danych właściwym organom państw członkowskich. EIOD zauważa, że podczas gdy przekazywanie danych regulowane jest rozporządzeniem (WE) nr 45/2001, kolejne przypadki korzystania z danych przez organy państw członkowskich są objęte dyrektywą 94/46/WE. Podczas gdy art. 18a ust. 2 lit. c) wydaje się w zamierzeniu przekazywać tę koncepcję, co zostało opisane poniżej, to jego brzmienie można by poprawić tak, by była ona bardziej widoczna.

21. Art. 18a ust. 2 lit. c) stanowi: „W ramach zarządzania zbiorem danych Komisja jest uprawniona do: [...] c) udostępnienia danych ze zbiorów innym właściwym organom, o których mowa w art. 1 ust. 1, wyłącznie dla osiągnięcia celów ustalonych w niniejszym rozporządzeniu, z zastrzeżeniem poszanowania przepisów krajowych wdrażających dyrektywę 95/46/WE”. W opinii EIOD art. 18a ust. 2 lit. c) nie odzwierciedla właściwie faktu, że dalsze wykorzystywanie danych osobowych przez organy państw członkowskich jest regulowane przez przepisy krajowe wdrażające dyrektywę 95/46/WE. W celu nadania tej kwestii większej jasności EIOD uważa, że końcowa część art. 18a ust. 2 lit. c) powinna być zmieniona jak następuje: „... wyłącznie do celów realizacji założeń niniejszego rozporządzenia. Dalsze wykorzystywanie danych osobowych przez te organy podlega przepisom krajowym wdrażającym dyrektywę 95/46/WE”. W każdym przypadku dalsze wykorzystywanie

<sup>(10)</sup> O ile podmiot świadczący usługi nie poinformował osób o tym wcześniej zgodnie z przepisami krajowymi wdrażającymi dyrektywę 95/46/WE.

<sup>(11)</sup> Działania z zakresu przetwarzania danych, które podlegają uprzedniemu sprawdzeniu przez EIOD, obejmują działania wyszczególnione w art. 27 rozporządzenia 45/2001, m.in. a) przetwarzanie danych odnoszących się do zdrowia i dotyczących podejrzeń o popełnienie przestępstwa, przestępstw, wyroków karnych lub środków bezpieczeństwa; b) operacje przetwarzania zmierzające do oceny aspektów osobistych odnoszących się do podmiotu danych, włącznie z jego możliwościami, wydajnością lub postępowaniem; c) operacje przetwarzania zezwalające na stworzenie powiązań między danymi przetwarzanymi dla różnych celów, nieuwzględnionymi w odpowiednim ustawodawstwie krajowym lub legislacji wspólnotowej; d) operacje przetwarzania w celu pozbawienia jednostki prawa, świadczenia lub wyłączenia jej z umowy.

danych na szczeblu krajowym będzie musiało odpowiadać celowi, do którego Komisja udostępnia te dane, chyba że zostaną spełnione szczególne warunki (patrz art. 6.1 lit.b)) i art. 13 ust. 1 dyrektywy 95/46/WE).

### I.3. Uwagi dodatkowe

22. EIOD zgadza się z podejściem obranym w art. 18 ust. 4 wniosku polegającym na ograniczeniu w Komisji liczby działów uprawnionych do przetwarzania danych osobowych zawartych w europejskim zbiorze danych. Jest to zgodne z art. 22 rozporządzenia (WE) nr 45/2001, które od kontrolerów danych wymaga między innymi wdrażania środków technicznych i organizacyjnych, takich jak pilnowanie, aby informacje były dostępne na zasadzie „ściślej potrzeby” w celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych.
23. Ostatni akapit art. 18 ust. 4 stwierdza, że z danych osobowych, które nie są potrzebne do celów, do których zostały pozyskane, należy usunąć czynniki identyfikacyjne. Akapit ten stanowi ponadto, że w każdym przypadku dane nie mogą być przechowywane dłużej niż jeden rok. EIOD z zadowoleniem przyjmuje zobowiązanie zgodne z art. 4 ust. 1 lit. e) rozporządzenia przewidujące, że dane osobowe mogą być przechowywane w formie, która pozwala na zidentyfikowanie osób, których dotyczą dane przez czas nie dłuższy niż jest to konieczne do celów, do których dane były gromadzone lub dalej przetwarzane.
24. Zgodnie z wymogiem art. 22 rozporządzenia (WE) nr 45/2001 zbiór musi być odpowiednio zabezpieczony. Zapewnienie utrzymania optymalnego poziomu bezpieczeństwa zbioru stanowi podstawowy wymóg ochrony danych osobowych przechowywanych w bazie danych. Podczas gdy przepisy regulujące system informacji celnej przewidują wprowadzenie konkretnych środków bezpieczeństwa, wniosek milczy w sprawie europejskiego zbioru danych. EIOD uważa, że sprawy bezpieczeństwa dotyczące zbioru powinny podlegać uzupełniającym przepisom administracyjnym przedstawiającym konkretne środki zapewniające poufność informacji. Należy skonsultować się z EIOD przy przyjmowaniu tych przepisów.

## II. Zmiany przepisów dotyczących systemu informacji celnej (SIC)

25. Art. 23–41 rozporządzenia Rady (WE) nr 515/97 przedstawiają przepisy ustanawiające system informacji celnej — bazę danych zarządzaną przez Komisję, dostępną dla państw członkowskich i Komisji, której celem jest wspomaganie ich w zapobieganiu działaniom sprzecznym z prawem celnym lub rolnym oraz w śledzeniu i ściganiu takich działań.

### II.1. Rozszerzanie możliwych sposobów wykorzystania danych osobowych przechowywanych w SIC

26. Wniosek zmienił niektóre pierwotne przepisy ustanawiające działanie i wykorzystanie SIC. W szczególności art. 25 poszerzył kategorie danych osobowych, które mogą być przechowywane w SIC, a art. 27 rozszerzył wykaz możliwych sposobów wykorzystania danych osobowych przechowywanych w SIC na analizy operacyjne umożliwiające między innymi „ocenę wiarygodności źródła informacji oraz samych informacji”, „formułowanie obserwacji, zaleceń (...) w celu wykrycia działań lub identyfikacji osób fizycznych lub prawnych”. Ponadto art. 35 ust. 3 stwarza możliwość kopiowania zawartości SIC do innych systemów przetwarzania danych w celu uczestniczenia w „systemach zarządzania ryzykiem używanych do kierowania krajowymi systemami kontroli lub w systemie analiz operacyjnych używanym do kierowania działaniami koordynacyjnymi na szczeblu Wspólnoty”.
27. Zgodnie z wnioskiem dodatkowe sposoby wykorzystania przedstawione powyżej są niezbędne, by wspomagać wykrywanie i ściganie działań sprzecznych z prawem celnym i rolnym. Chociaż EIOD nie kwestionuje istnienia takich potrzeb, uważa, że wniosek Komisji powinien być przedstawic pełniejsze informacje i racjonalne uzasadnienie dla takiej potrzeby.
28. EIOD z zadowoleniem dostrzega, że powyższym zmianom towarzyszą zabezpieczenia z zakresu ochrony danych osobowych. Wniosek faktycznie utrzymuje zamknięty wykaz danych osobowych, które można wprowadzić do SIC (na mocy art. 25 ust. 1); dane te wprowadzić jedynie wtedy, gdy istnieją „dowody” sugerujące, że dana osoba brała, bierze lub będzie brała udział w działaniach niedozwolonych (na mocy art. 27 ust. 2). Dodatkowo, zgodnie z art. 25 ust. 3 do SIC nie można wprowadzić danych wrażliwych<sup>(12)</sup>. Ponadto art. 35 ust. 3 ograniczył liczbę osób uprawnionych do kopiowania zawartości SIC do celów ustalonych w tym samym artykule i ograniczył czas zatrzymywania danych skopiowanych z SIC. Środki te są zgodne z zasadą jakości danych przedstawioną w art. 4 rozporządzenia (WE) nr 45/2001.

### II.2. Zakres zastosowania rozporządzenia (WE) nr 45/2001

29. Art. 34 wniosku uwzględnił przyjęcie rozporządzenia (WE) nr 45/2001 mającego zastosowanie do przetwarzania danych osobowych przez instytucje i organy wspólnotowe. Wymaga on zatem od Komisji wzięcia pod uwagę faktu, że rozporządzenie (WE) nr 45/2001 ma zastosowanie do SIC. EIOD potwierdza, że biorąc pod uwagę fakt, iż SIC zawiera dane osobowe i że Komisja ma dostęp do bazy danych, wobec której ma ona funkcję kontrolera danych, rozporządzenie (WE) nr 45/2001 z pewnością ma zastosowanie do tej bazy. Wobec tego EIOD z zadowoleniem przyjmuje zmiany uwzględniającą obecne ramy prawne dotyczące ochrony danych.

<sup>(12)</sup> Danych dotyczących pochodzenia rasowego lub etnicznego, opinii politycznych, poglądów religijnych lub filozoficznych, przynależności do związku zawodowych, oraz danych dotyczących zdrowia lub preferencji seksualnych.

30. EIOD przypomina, że w wyniku zastosowania art. 27 rozporządzenia (WE) nr 45/2001 i biorąc pod uwagę fakt, że cele SIC mogą być postrzegane jako przedstawiające szczególnie ryzyko dla praw i wolności podmiotu danych, EIOD musi wcześniej sprawdzić system.
31. Poza zastosowaniem rozporządzenia (WE) nr 45/2001, art. 34 wniosku utrzymuje jednocześnie zastosowanie przepisów krajowych wdrażających dyrektywę 95/46/WE. EIOD uważa to za właściwe podejście, o ile organy państw członkowskich mają dostęp do SIC oraz kompetencje do wprowadzenia i dalszego przetwarzania danych zawartych w SIC. Podsumowując, EIOD uważa, że kontrola nad SIC jest rozłożona między Komisję a państwa członkowskie, które działają jako współkontrolerzy danych w SIC.

### II.3. EIOD jako nadzorca SIC wraz z krajowymi organami ochrony danych

32. W wyniku zastosowania rozporządzenia (WE) nr 45/2001 Europejski Inspektor Ochrony Danych jest odpowiedzialny za zapewnianie stosowania rozporządzenia w odniesieniu do SIC. Podczas gdy niektóre artykuły wniosku uwzględniają kompetencje EIOD, inne tego nie robią. EIOD ubolewa w szczególności nad tym, że niektóre części art. 37 odnoszące się do nadzoru nie zostały odpowiednio zmienione i wzywa prawodawców do wprowadzenia poprawek określonych poniżej.
33. EIOD zauważa, że art. 37 ust. 1 wyraźnie uznaje kompetencje organów państw członkowskich w nadzorowaniu SIC. Art. 37 ust. 1 nie wspomina o podobnych kompetencjach EIOD na mocy rozporządzenia (WE) nr 45/2001. Problem ten jest jeszcze podkreślony w art. 37 ust. 3, który nie został zmieniony we wniosku. Art. 37 ust. 3 stanowi: „Komisja podejmuje wszelkie działania w swoich wydziałach w celu zapewnienia nadzoru nad ochroną danych osobowych, który daje zabezpieczenie na poziomie odpowiadającym wymogom określonym w ust. 1...”. Innymi słowy, art. 37 ust. 1 powierza nadzór nad ochroną danych „Komisji”. Jasne jest, że artykuł ten powinien być zostać zmieniony w celu uwzględnienia nowej, nadzorczej roli EIOD. Art. 37 ust. 3 w swojej obecnej postaci nie ma sensu. W celu rozwiązania tego problemu art. 37 ust. 3. powinien być zmieniony tak, aby stanowił, że „Europejski Inspektor Danych Osobowych będzie nadzorował zgodność SIC z rozporządzeniem (WE) nr 45/2001”.
34. Ponadto, jako że SIC jest regulowany nie tylko przez rozporządzenie (WE) nr 45/2001, lecz także przez przepisy krajowe wdrażające dyrektywę 95/46/WE, nadzór nad SIC spoczywa zarówno na EIOD, jak i na krajowych organach

ochrony danych. Na koniec, działania nadzorcze krajowych organów oraz EIOD powinny być do pewnego stopnia skoordynowane, tak aby zapewnić odpowiedni poziom spójności i ogólnej skuteczności. Jak stwierdzono w poprzednich opiniach EIOD dotyczących baz danych znajdujących się pod nadzorem państw członkowskich UE oraz EIOD „istnieje potrzeba ujednoliconego wdrażania rozporządzenia oraz potrzeba współpracy w celu wypracowania wspólnego podejścia do wspólnych problemów” <sup>(13)</sup>.

35. Niestety wniosek nie przewiduje procedury koordynacji w celu nadania struktury i zacieśnienia współpracy między EIOD a krajowymi organami ochrony danych. W celu rozwiązania tego problemu EIOD wymienia jako pierwszą możliwość wprowadzenie do art. 37 nowej sekcji, dotyczącej nadzoru nad ochroną danych, stanowiącej, że „Co najmniej raz w roku EIOD zwołuje spotkanie ze wszystkimi krajowymi organami nadzorczymi w celu zajęcia się kwestiami nadzoru dotyczącymi SIC. Członkowie krajowych organów ochrony danych oraz EIOD zwani są organami nadzorczymi”.
36. Lepszym rozwiązaniem odzwierciedlającym wielokierunkowe podejście do kwestii nadzoru byłoby — o czym wspomniano poprzednio — podzielenie przepisów dotyczących nadzoru (art. 37) na kilka pomniejszych, przy czym każdy z nich byłby poświęcony pewnemu poziomowi nadzoru, czego dokonano prawidłowo w niedawno przyjętych aktach prawnych ustanawiających system informacyjny Schengen (SIS II). W szczególności art. 44–46 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania systemu informacyjnego Schengen drugiej generacji (SIS II) <sup>(14)</sup> zakładają dobrze wyważony system nadzoru podzielony między szczeblami krajowym i europejskim, przy czym obydwa szczeble są skoordynowane. EIOD stanowczo sugeruje założenie tego samego systemu nadzoru (z pewnymi niewielkimi korektami) w odniesieniu do SIC. SIC i SIS II są w dużym stopniu porównywalne w zakresie struktury nadzoru.
37. Art. 43 ust. 5 przewiduje utworzenie w formie *ad hoc* komitetu, o którym mowa w art. 43 ust. 1 (dalej zwanego komitetem utworzonym w formie *ad hoc*), który będzie spotykał się okresowo w celu analizowania problemów z zakresu ochrony danych, związanych z SIC. EIOD uważa, że ten komitet utworzony w formie *ad hoc* nie powinien być uważany za organ właściwy do sprawowania nadzoru nad SIC, ponieważ leży to wyłącznie w gestii organów krajowych państw członkowskich oraz EIOD. Organ przedstawiony w art. 43 ust. 5 jest w rzeczywistości komitetem w ramach „komitologii”.

<sup>(13)</sup> Opinia z dnia 19 października 2005 r. w sprawie 3 wniosków dotyczących: Systemu Informacyjnego Schengen drugiej generacji (SIS II), (COM (2005) 230 wersja ostateczna, COM (2005) 236 wersja ostateczna, i COM (2005) 237 wersja ostateczna), Dz.U. C 91 z 19.4.2006, str. 38; opinia z dnia 23 marca 2005 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych między państwami członkowskimi na temat wiz krótkoterminowych, Dz.U. C 181 z 23.7.2005 str. 13.

<sup>(14)</sup> Dz. U. L 381 z 28.12.2006, str. 4-23.

38. EIOD uważa jednak, że komitet utworzony w formie *ad hoc* jest odpowiednim forum, na którym można analizować problemy z zakresu ochrony danych związane z działaniem SIC. W tym celu EIOD proponuje przeformułowanie art. 43 ust. 5 w celu uwzględnienia zadań i roli komitetu utworzonego w formie *ad hoc* na mocy tego artykułu: „Komitet, wraz z grupą nadzorczą, o której mowa w art... analizuje wszystkie problemy związane z działaniem SIC, jakie napotykają organy nadzorcze. Komitet utworzony w formie *ad hoc* spotyka się przynajmniej raz w roku.”
39. EIOD pragnie także zwrócić uwagę prawodawcy na kolejną cechę charakterystyczną, którą posiadają systemy SIC i SIS II, mianowicie fakt, że obydwa działają w ramach zarówno pierwszego, jak i trzeciego filara, co pociąga za sobą istnienie dwóch odrębnych podstaw prawnych dla każdego systemu. SIC w ramach trzeciego filara jest regulowany przez konwencję, o której mowa w punkcie 3 niniejszej opinii. Rodzi to liczne skutki, między innymi w zakresie struktury nadzoru: część SIC w ramach pierwszego filara będzie nadzorowana przez EIOD i krajowe organy ochrony danych, natomiast część w ramach trzeciego filara jest nadzorowana przez wspólny organ nadzorczy (składający się z przedstawicieli tychże organów krajowych). Stwarza to raczej niezręczny system nadzoru, który może powodować niespójność i może nie być zbyt skuteczny. Ilustruje to trudności stwarzane przez skomplikowane otoczenie prawne, takie jak tutaj opisywane.
40. Warto zauważyć, że w ramach SIS II prawodawca europejski zdecydował się na racjonalizację modelu nadzoru, stosując ten sam wielokierunkowy model, który został opisany powyżej zarówno w częściach systemu działających w ramach pierwszego filara, jak i tych działających w ramach trzeciego. Jest to podejście warte rozważenia i EIOD zaleca dalszą analizę dostarczanych przez nie sposobności wprowadzenia lepszego i bardziej konsekwentnego nadzoru.
- #### II.4. Prawa osób fizycznych
41. Prawa osób fizycznych w odniesieniu do wniosku, zwłaszcza prawo dostępu do danych, są regulowane w art. 36 i 37, które we wniosku zostały częściowo zmienione. EIOD pragnie zająć się trzema następującymi kwestiami związanymi z prawem dostępu: (i) obowiązującym prawem zgodnie z art. 36 ust. 1; (ii) granicami prawa dostępu zgodnie z art. 36 ust. 2 oraz (iii) procedurą, według której osoby fizyczne składają wnioski o dostęp zgodnie z art. 37 ust. 2 wniosku.
42. *Obowiązujące prawo*: art. 36 ust. 1, który we wniosku pozostał bez zmian uznaje przy okazji zastosowanie prawa osób fizycznych do ochrony danych i przewiduje, że prawo dostępu będzie regulowane przez przepisy prawa państw członkowskich lub przez przepisy o ochronie danych obowiązujące wobec Komisji, w zależności od tego, czy prawa takie zostały przywołane odpowiednio w państwach członkowskich, czy w instytucjach UE. Kryterium to odzwierciedla stwierdzenie przedstawione powyżej dotyczące art. 34 wniosku — zarówno Komisja, jak i państwa członkowskie są kontrolerami SIC. EIOD zgadza się z tym podejściem i wyraża zadowolenie, że wniosek utrzymał brzmienie art. 36 ust. 1. Jest jasne, że przepis ten odnosi się w domniemaniu do stosownego przepisu prawa krajowego wdrażającego dyrektywę 95/46/WE lub rozporządzenie (WE) nr 45/2001. W każdym przypadku obowiązujące prawo będzie zależało od miejsca wykonywania praw.
43. *Granice prawa dostępu*: art. 36 ust. 2 akapit drugi stanowi, że „dostęp nie zostanie udzielony w czasie, kiedy podejmowane jest działanie w celach zlokalizowania, sporządzania sprawozdań lub dochodzenia”. Z przyczyn przedstawionych poniżej EIOD opowiada się za poprawką brzmiącą „dostępu można nie udzielić” (w przeciwieństwie do brzmienia „dostęp nie zostanie udzielony”).
44. Na mocy rozporządzenia (WE) nr 45/2001, w ramach ogólnej zasady, osoby fizyczne są uprawnione do wykonywania prawa dostępu do ich danych osobowych. Art. 20 rozporządzenia (WE) nr 45/2001 uznaje jednak, że prawo to może zostać ograniczone, jeżeli ma zastosowanie jeden ze szczególnych warunków uzasadniających ograniczenie. Innymi słowy, osoby fizyczne mają zasadniczo prawo dostępu, ale dostęp ten może zostać ograniczony. Odwrotnie, brzmienie art. 36 ust. 2 „dostęp nie zostanie udzielony” nie daje możliwości oceny tego, czy dostęp może zostać udzielony, czy nie. Zasadniczo oznacza to, że osoby fizyczne przez pewien czas są pozbawione takiego prawa. Nie ma powodu, dla którego nie można byłoby zastosować w tym przypadku podejścia przedstawionego w rozporządzeniu (WE) nr 45/2001, zwłaszcza jeżeli art. 20 umożliwiłby ograniczenie dostępu w okresie przewidzianym w art. 36.2. Jeżeli Komisja rzeczywiście pragnęłaby uniemożliwić dostęp, mogłaby skorzystać z art. 20, zgodnie z którym można odmówić dostępu w celu zabezpieczenia dochodzenia.
45. EIOD uważa, że wniosek powinien być sformułowany w tym samym duchu co rozporządzenie (WE) nr 45/2001. Inne podejście byłoby sprzeczne z ogólnymi ramami przewidującymi prawo dostępu na mocy rozporządzenia (WE) nr 45/2001. Problem można rozwiązać poprzez zastąpienie sformułowania „nie zostanie udzielony” wyrażeniem „można udzielić”.
46. *Procedura składania wniosków o dostęp przez osoby fizyczne*: We wniosku wprowadzono zmianę w stosunku do dawnego artykułu 37 ust. 2 rozporządzenia (WE) nr 515/97 odnoszącego się do procedury składania wniosków o uzyskanie informacji, czy SIC zawiera dane osobowe konkretnej osoby. Nowy artykuł 37 ust. 2 przyznaje osobom fizycznym możliwość składania wniosków o dostęp Europejskiemu Inspektorowi Ochrony Danych oraz krajowym organom nadzoru, w zależności od tego, czy dane zostały wprowadzone do SIC przez Komisję czy przez państwo członkowskie.
47. EIOD z zadowoleniem przyjmuje tę zmianę, która dostosowuje omawianą procedurę do istniejących ram prawnych dotyczących ochrony danych. EIOD uważa jednak, że — z następujących przyczyn — kompetencje państw członkowskich ani Komisji nie powinny być zależne od podmiotu, który wprowadził dane do SIC: po pierwsze, EIOD zaznacza, że osoby fizyczne najprawdopodobniej nie wiedzą, jaki podmiot — Komisja czy państwo członkowskie — wprowadził informacje do SIC. Co za tym idzie, nie będą w stanie określić, który podmiot posiada kompetencje do rozpatrzenia ich wniosku. Procedura dotycząca wniosków o dostęp stanie się utrudniona, jeżeli osoby fizyczne

będą zmuszone najpierw określić, kto wprowadził dane do systemu. Po drugie, EIOD uważa, że ten przepis zaprzecza kryteriom określonym w art. 36 ust. 1, zgodnie z którymi prawo dostępu do danych będzie podlegać prawu państw członkowskich lub przepisom dotyczącym ochrony danych mającym zastosowanie do Komisji, zależnie od tego, czy takie prawa zostały przywołane odpowiednio w państwach członkowskich, czy w instytucjach UE. Zatem — co najmniej w celu zachowania zgodności z art. 36 — kompetencje dotyczące wniosków o dostęp powinny zależeć od tego, czy wniosek o dostęp został złożony krajowym organom nadzoru, czy też EIOD.

48. By rozwiązać ten problem, należy zastąpić sformułowanie „zależnie od tego, czy dane zostały wprowadzone do SIC przez państwo członkowskie, czy też przez Komisję” sformułowaniem „zależnie od tego, czy prawa takie zostały przywołane odpowiednio w krajowych organach nadzorczych, czy w urzędzie EIOD”. Jeżeli zastosowanie zostanie takie podejście, pełny sens otrzyma także następujące zdanie z art. 37 ust. 2: „Jeżeli dane zostały umieszczone przez inne państwo członkowskie lub przez Komisję, sprawdzenie odbywa się w ścisłej współpracy z krajowym organem nadzorczym w tym innym państwie członkowskim lub z Europejskim Inspektorem Ochrony Danych.”

#### II.5. Wymiana danych

49. Wniosek nie dodaje nowych elementów odnośnie do wymiany danych osobowych z organami państw trzecich. Kwestię tę ujęto w art. 30 ust. 4 wniosku. EIOD uważa, że ten artykuł należy zmienić, by objąć potrzebę przedsięwzięcia przez Komisję (nie zaś tylko przez państwa członkowskie) szczególnych środków zapewniających bezpieczeństwo danych podczas ich przesyłania lub przekazywania ośrodkom znajdującym się w państwach trzecich. Ponadto art. 30 ust. 4 należy zmienić, aby zapewnić jego zgodność z prawodawstwem mającym zastosowanie do przesyłania danych osobowych do państw trzecich.

### III. Identyfikująca baza danych rejestru celnego („FIDE”)

50. Art. 41a, b, c i d wniosku ustanawiają zasady funkcjonowania identyfikującej bazy danych rejestru celnego. FIDE umożliwi właściwym organom sprawdzenie, czy osoba lub przedsiębiorstwo były przedmiotem postępowania karnego w którymkolwiek państwie członkowskim.
51. FIDE istnieje już jako narzędzie stosowane przez państwa członkowskie w ramach trzeciego filaru<sup>(15)</sup>. Celem art. 41 jest zatem zapewnienie podstawy prawnej dla FIDE wspólnotowego, co EIOD przyjmuje z zadowoleniem.
52. Jako że wszystkie przepisy mające zastosowanie do SIC mają zastosowanie również do FIDE na mocy art. 41a, wszystkie uwagi poczynione w sekcji II powyżej mają zastosowanie do FIDE *mutatis mutandis*.

<sup>(15)</sup> Utworzona aktem Rady z dnia 8 maja 2003 r. ustalającym Protokół zmieniający Konwencję o wykorzystaniu technologii informatycznej do potrzeb celnych

#### III.1. Zastosowanie rozporządzenia (WE) nr 45/2001

53. EIOD zauważa, że uwzględniając, iż Komisja posiada kompetencje do przetwarzania danych zawartych w FIDE, powinno być jasne, że rozporządzenie (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ma zastosowanie również do FIDE. EIOD uważa, że właściwe byłoby, by w art. 41 przywołać zastosowanie rozporządzenia (WE) nr 45/2001 do FIDE oraz kompetencje EIOD jako organu nadzoru do monitorowania i zapewniania spójności z przepisami tego rozporządzenia.
54. EIOD przypomina, że w wyniku zastosowania art. 27 rozporządzenia (WE) nr 45/2001 i biorąc pod uwagę fakt, że cele FIDE oraz charakter zawartych w niej danych mogą być postrzegane jako przedstawiające szczególne ryzyko dla praw i wolności podmiotu danych, EIOD musi wcześniej sprawdzić system.

#### III.2. Zatrzymywanie danych

55. Art. 41d określa szczegółowo okresy zatrzymywania danych. EIOD uważa, że terminy przewidziane w art. 41d są zasadne.
56. Nie jest pewny związek tego przepisu z art. 33 w odniesieniu do SIC. Przyjmuje się, że art. 41d ma pierwszeństwo przed przepisem dotyczącym tej samej kwestii w odniesieniu do SIC, ale nie zostało to jednoznacznie stwierdzone w omawianym wniosku. Pożyteczne byłoby dodanie przepisu wyjaśniającego tę kwestię.

#### III.3. Aktualizacja informacji zawartych w FIDE.

57. Zasada jakości danych (art. 4 rozporządzenia (WE) 45/2001) wymaga, by dane osobowe były prawidłowe, stosowne oraz nienadmierne w stosunku do celu, dla którego są gromadzone. Jest jasne, że jakość danych osobowych można zapewnić jedynie pod warunkiem regularnej i właściwej kontroli ich prawidłowości. EIOD również przyjmuje z zadowoleniem przepisy art. 41 d, które wymagają, by dane zostały bezzwłocznie usunięte, gdy tylko dana osoba zostanie oczyszczona od podejrzeń zgodnie z prawem ustawowym i wykonawczym oraz procedurami państwa przekazującego dane.
58. Z drugiej strony, by zagwarantować, że zbędne dane nie pozostają w FIDE, EIOD proponuje zastosowanie do FIDE niektórych przepisów dotyczących ochrony danych określonych dla SIC w art. 33. W szczególności EIOD proponuje zastosowanie do FIDE przepisów art. 33 ust. 1, zgodnie z którymi potrzeba zatrzymywania danych powinna być poddawana przez stronę przekazującą dane corocznemu przeglądowi. W tym celu EIOD proponuje dodanie po art. 41d ust. 2 następującego sformułowania: „Potrzeba zatrzymywania danych powinna być przynajmniej co rok poddawana przeglądowi przez państwo członkowskie przekazujące dane”.

## WNIOSKI

59. EIOD z zadowoleniem przyjmuje prośbę o wydanie opinii w sprawie wniosku, który przewiduje stworzenie lub aktualizację kilku systemów zawierających dane osobowe: europejskiego zbioru danych, systemu informacji celnej (SIC) i identyfikującej bazy danych rejestru celnego („FIDE”) w celu wzmocnienia współpracy i wymiany informacji zarówno pomiędzy państwami członkowskimi, jak i między nimi a Komisją.
60. Odnośnie do **treści** EIOD wyciąga następujące wnioski:
- Wniosek nie przedstawia wystarczających argumentów za potrzebą stworzenia **europejskiego zbioru danych**. EIOD wzywa Komisję do przeprowadzenia właściwej oceny konieczności tworzenia tego zbioru danych i przedstawienia sprawozdania z wyników tej oceny.
  - Do art. 18a ust. 1 należy dodać nowy akapit przywołujący zastosowanie rozporządzenia (WE) nr 45/2001 do europejskiego zbioru danych zawierający następującą treść: „Komisja uznaje europejski zbiór danych za system przetwarzania danych osobowych objęty rozporządzeniem (WE) nr 45/2001.”
  - Należy wyjaśnić, że krajowe przepisy wdrażające dyrektywę 95/46/WE mają zastosowanie do wykorzystywania europejskiego zbioru danych przez państwa członkowskie; EIOD proponuje zatem następującą zmianę art. 18a ust. 2 lit. c): „W ramach zarządzania zbiorem danych Komisja jest uprawniona do: c) udostępnienia danych ze zbiorów innym właściwym organom, o których mowa w art. 1 ust. 1, wyłącznie do celów realizacji założeń niniejszego rozporządzenia. Dalsze wykorzystywanie danych osobowych przez te organy podlega przepisom krajowym wdrażającym dyrektywę 95/46/WE.”
  - Wniosek nie wypowiada się na temat środków bezpieczeństwa dotyczących europejskiego zbioru danych. EIOD uważa, że właściwe byłoby dodanie do art. 18a ust. 2 nowego akapitu przewidującego przyjęcie uzupełniających przepisów administracyjnych ustalających konkretne środki gwarantujące poufność informacji. Podczas przyjmowania tych przepisów należy skonsultować się z EIOD.
  - We wniosku nie uznano w pełni roli EIOD jako organu nadzoru w odniesieniu do **systemu informacji celnej (SIC)**. Aby rozwiązać ten problem należy zmienić art. 37 ust. 3, by określał on, że „Europejski Inspektor Danych Osobowych będzie nadzorował zgodność SIC z rozporządzeniem (WE) nr 45/2001.”
  - Działalność nadzorcza krajowych organów nadzorczych i EIOD powinna być do pewnego stopnia skoordynowana, aby zapewnić dostateczny poziom spójności i ogólnej skuteczności nadzoru nad SIC. W tym celu EIOD proponuje jako wariant pierwszy dodanie do art. 37 nowej sekcji stanowiącej, że: „Co najmniej raz w roku EIOD zwołuje spotkanie ze wszystkimi krajowymi organami nadzorczymi w celu zajęcia się kwestiami nadzoru dotyczącymi SIC. Członkowie krajowych organów ochrony danych oraz EIOD zwani są organami nadzorczymi”. Lepszym rozwiązaniem byłoby jednak zastosowanie bardziej rozwiniętego modelu, przyjętego niedawno dla systemu informacyjnego Schengen drugiej generacji (SIS II). Zgodnie z tym podejściem w każdym przypadku należy wprowadzić do art. 43 ust. 5 następującą zmianę: „Komitet, wraz z grupą nadzorczą, o której mowa w art... analizuje wszystkie problemy związane z działaniem SIC, jakie napotykają organy nadzorcze, o których mowa w art. 37. Komitet utworzony w formie ad hoc spotyka się przynajmniej raz w roku.”
  - Na mocy art. 36 ust. 2 akapit drugi dotyczący dostępu do danych osobowych przechowywanych w SIC „dostęp nie zostanie udzielony w czasie, kiedy podejmowane jest działanie w celach zlokalizowania, sporządzania sprawozdań lub dochodzenia” Aby zapewnić spójność z rozporządzeniem (WE) nr 45/2001, EIOD preferowały zmianę o brzmieniu „dostęp można odmówić”.
  - W odniesieniu do procedury wnoszenia o dostęp, niezależnie od tego, czy wniosek należy składać EIOD, czy też krajowym organom nadzoru, EIOD uważa, że proponowany w art. 37 ust. 2 system, w którym określenie kompetentnego organu zależy od tego, czy dane zostały wprowadzone do SIC przez państwo członkowskie, czy też przez Komisję, jest bardzo niezręczny. Pozostaje on również w sprzeczności z innymi artykułami wniosku. By rozwiązać ten problem, należy zastąpić sformułowanie „zależnie od tego, czy dane zostały wprowadzone do SIC przez państwo członkowskie, czy też przez Komisję” w art. 37 ust. 2 sformułowaniem „zależnie od tego, czy prawa takie zostały przywołane w krajowych organach nadzorczych, czy w urzędzie EIOD.”
  - EIOD uważa, że właściwe byłoby, by w art. 41a przywołać zastosowanie rozporządzenia (WE) nr 45/2001 **do identyfikującej bazy danych rejestru celnego (FIDE)** oraz kompetencje EIOD jako organu nadzoru do monitorowania i zapewniania spójności z przepisami tego rozporządzenia.
61. Aby zagwarantować usuwanie zbędnych danych osobowych z FIDE, EIOD proponuje dodanie po art. 41d ust. 2 następującego tekstu: „Potrzeba zatrzymywania danych powinna być przynajmniej co rok poddawana przeglądowi przez państwo członkowskie przekazujące dane.”



62. Co do **procedury**, EIOD:

- zaleca umieszczenie w preambule do wniosku wyrażonego odniesienia do niniejszej opinii w brzmieniu: „po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych”,
- przypomina, że ze względu na to, iż działania przetwarzające w ramach europejskiego zbioru danych, systemu informacji celnej (SIC) i identyfikującej bazy danych rejestru celnego (FIDE) przedstawiają szczególne ryzyko dla praw i wolności osoby, której dotyczą dane, ze

względu na cel bazy danych i charakter tych danych, zgodnie z art. 27 rozporządzenia (WE) nr 45/2001 EIOD musi uprzednio sprawdzić te trzy systemy.

Sporządzono w Brukseli, dnia 22 lutego 2007 r.

Peter HUSTINX

*Europejski Inspektor Ochrony Danych*

---