Opinia Europejskiego Inspektora Ochrony Danych w sprawie: zmienionego wniosku dotyczącego rozporządzenia Rady zmieniającego rozporządzenie (WE, Euratom) nr 1605/2002 w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich (COM (2006) 213 wersja ostateczna) oraz w sprawie wniosku dotyczącego rozporządzenia Komisji (WE, Euratom) zmieniającego rozporządzenie (WE, Euratom) nr 2342/2002 ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE, Euratom) nr 1605/2002 w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich (SEC(2006) 866 wersja ostateczna)

(2007/C 94/03)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

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

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

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

uwzględniając wnioski o wydanie opinii przesłane przez Komisję 18 maja 2006 r. (w sprawie zmienionego wniosku dotyczącego rozporządzenia finansowego) i 4 lipca 2006 r. (w sprawie wniosku dotyczącego zasad wykonawczych) zgodnie z art. 28 rozporządzenia (WE) nr 45/2001,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WSTĘP**

1. Rozporządzenie Rady (WE, Euratom) nr 1605/2002 z dnia 25 czerwca 2002 r. w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich ([3]) (zwane dalej „RF") ustanawia prawne podstawy reformy zarządzania finansami. W grudniu 2002 roku, po zakończeniu szeroko zakrojonych konsultacji z instytucjami, Komisja przyjęła zasady wykonawcze do RF (zwane dalej „ZW"). Obydwa rozporządzenia, mające zastosowanie do wszystkich instytucji, weszły w życie w dniu 1 stycznia 2003 r.

2. Zmieniony wniosek dotyczący rozporządzenia Rady zmieniającego rozporządzenie (WE, Euratom) nr 1605/2002 w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich ([4]) (zwany dalej „wnioskiem dotyczącym RF") przyjęty w 2006 roku przedłożono w celu wykonania przepisów art. 184 RF, który przewiduje przegląd rozporządzenia finansowego co trzy lata lub w każdym przypadku, gdy okaże się to niezbędne. Głównym celem wniosku dotyczącego RF jest poprawa skuteczności i przejrzystości przepisów poprzez lepsze zrównoważenie kosztów kontroli i ponoszonego ryzyka finansowego, przy jednoczesnym utrzymaniu wysokiego poziomu ochrony środków finansowych Wspólnoty. Zmieniony wniosek dotyczący RF został uzgodniony w drodze procedury pojednawczej między Parlamentem Europejskim a Radą pod koniec listopada 2006 roku. Tekst ten uwzględniono w niniejszej opinii ([5]).

3. Aby przyspieszyć proces legislacyjny, Komisja z własnej inicjatywy przedstawiła wniosek dotyczący rozporządzenia Komisji (WE, Euratom) zmieniającego rozporządzenie (WE, Euratom) nr 2342/2002 ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE, Euratom) nr 1605/2002 z dnia 25 czerwca 2002 r. w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich ([6]) (zwany dalej „wnioskiem dotyczącym ZW"). Zasięgnięto opinii EIOD w sprawie tych dwóch wniosków.

4. EIOD uważa, że analiza wniosków jest istotna, ponieważ wpłyną one na sposób postępowania z niektórymi danymi osobowymi osób fizycznych związanymi z działalnością finansową. Jednym z głównych punktów wniosków jest to, że przewidują one utworzenie przez Komisję centralnej, wspólnej dla wszystkich instytucji i organów, bazy danych kandydatów i oferentów, którzy znajdują się w określonych sytuacjach wykluczających ich w związku z oszustwami finansowymi, oraz zarządzanie tą bazą oraz że pozwalają one na wymianę informacji zawartych w bazie danych z władzami na różnych szczeblach. EIOD podkreśla, że przewidywana centralna baza danych, która zawierałaby dane kandydatów i oferentów znajdujących się w jednej z sytuacji określonych w art. 93, 94 oraz art. 96 ust. 1 lit. b) i ust. 2 lit. a) rozporządzenia finansowego, istniała już przed zmianą rozporządzenia finansowego ([7]). Istniejąca baza danych działa z wykorzystaniem ostrzeżeń na różnych poziomach (1, 2, 3, 4, 5a i 5b) w zależności od skutków, jakie mają dla kandydatów i oferentów. Istniejąca baza danych, utworzona na poziomie instytucjonalnym przez Komisję, ma jednak szerszy zakres niż baza przewidziana we wniosku dotyczącym rozporządzenia finansowego (obejmująca jedynie ostrzeżenia na poziomie 5). Wspomniana centralna baza danych i inne aspekty wniosków wymagają uważnej analizy z punktu widzenia ochrony danych.

([1]) Dz.U. L 281 z 23.11.1995, str. 31.
([2]) Dz.U. L 8 z 12.1.2001, str. 1.
([3]) Dz.U. L 248 z 16.9.2002, str. 1.
([4]) Dok. COM(2006) 213 wersja ostateczna — 2005/0090 (CNS)
([5]) W zmienionym wniosku skreślono art. 95 ust. 3 pkt 2, co oznacza poprawę tekstu z punktu widzenia ochrony danych.
([6]) Dok. SEC(2006) 866 wersja ostateczna
([7]) Na temat analizy aktualnej sytuacji — zob. opinię z kontroli wstępnej EIOD na temat systemu wczesnego ostrzegania Komisji z dnia 6 grudnia 2006 r., dostępną pod adresem: www.edps.europa.eu

Konsultacje z Europejskim Inspektorem Ochrony Danych

5. Komisja przesłała wnioski dotyczące RF i ZW do 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 (zwanego dalej „rozporządzeniem nr 45/2001"). Uwzględniając wiążący charakter art. 28 ust. 2 rozporządzenia nr 45/2001, EIOD z zadowoleniem przyjmuje wyraźne odniesienie do tej konsultacji w preambule do wniosków.

II. **ANALIZA WNIOSKÓW**

6. Komisja, odpowiedzialna za wykonanie budżetu ogólnego Unii Europejskiej i wszelkich innych środków finansowych zarządzanych przez Wspólnoty, ma obowiązek przeciwdziałać oszustwom finansowym i wszelkim innym nielegalnym działaniom mającym wpływ na interesy finansowe Wspólnot. Wnioski dotyczące RF i ZW określają nowe obowiązki Komisji w zakresie udzielania zamówień i przyznawania dotacji stronom trzecim w kontekście zarządzania środkami finansowymi Wspólnoty. Uwzględniając fakt, że wnioski ustanawiają przepisy, których należy przestrzegać w celu zapewnienia ochrony interesów finansowych Wspólnot, niezbędne jest przy tym odpowiednie zagwarantowanie ochrony danych i prawa do prywatności osób przy przetwarzaniu ich danych osobowych.

II.1. **Przejrzystość**

7. EIOD uznaje, że we wnioskach propaguje się ważne zasady dotyczące należytego zarządzania finansami, a także wprowadza się lub wzmacnia nowe zasady. EIOD odnotowuje, na przykład, że motyw 1 wniosku dotyczącego RF przewiduje, że: *„w szczególności należy zwiększyć przejrzystość poprzez zapewnienie informacji o beneficjentach wspólnotowych środków finansowych*". Zasadę tę rozwinięto w art. 30 ust. 3 i art. 53 RF.

8. Przepisy te, dotyczące zasady przejrzystości, wprowadzają obowiązek publikowania wykazu beneficjentów środków finansowych pochodzących z budżetu. EIOD popiera wprowadzenie tej zasady, z należytym poszanowaniem przepisów dyrektywy 95/46/WE i rozporządzenia 45/2001, ale pragnie podkreślić, że należy przestrzegać proaktywnego podejścia do praw podmiotów danych ([8]), ponieważ zostaną ujawnione dane osobowe. To proaktywne podejście mogłoby polegać na wcześniejszym informowaniu podmiotów danych, w momencie gromadzenia danych osobowych, że dane te mogą zostać podane do wiadomości publicznej, oraz na zapewnieniu poszanowania prawa podmiotu danych do dostępu do jego danych oraz jego prawa do sprzeciwu. Zasada ta powinna mieć również zastosowanie do publikacji *ex post* wykazu beneficjentów (art. 169 zasad wykonawczych).

II.2. **Centralna baza danych systemu wczesnego ostrzegania (EWS)**

9. Art. 95 wniosku dotyczącego RF stanowi, że Komisja utworzy centralną bazę danych zawierającą stosowne szczegółowe informacje o kandydatach i oferentach znajdujących się w jednej z sytuacji prowadzących do ich wykluczenia, o których mowa w art. 93, 94 ([9]), 96 ust. 1 lit. b) i ust. 2 lit. a), i będzie nią zarządzać zgodnie ze wspólnotowymi przepisami dotyczącymi przetwarzania danych osobowych. Jak wspomniano we wstępie, nowa wersja art. 95, podkreślająca pierwszoplanową rolę Komisji, nie zmienia w istotny sposób dotychczasowej praktyki (tj. art. 95 RF stwierdza, że każda instytucja ma swoją własną centralną bazę danych). Obecnie instytucje ([10]) nie mają oddzielnych baz danych, ale korzystają ze skomputeryzowanej bazy danych Komisji Europejskiej i wymieniają z nią informacje ([11]). Ta baza danych funkcjonuje zgodnie z procedurą przewidzianą w decyzji Komisji w sprawie systemu wczesnego ostrzegania (EWS) ([12]). Komisja centralizuje wszystkie istotne informacje i odgrywa rolę centralnego punktu dostępu między wszystkimi instytucjami uczestniczącymi w tym systemie.

10. Art. 95 RF stwierdza również, że baza danych jest wspólna dla instytucji, agencji wykonawczych oraz organów, o których mowa w art. 185 RF. W uzgodnionej wersji rozporządzenia finansowego art. 95 stwierdza dalej, że władze państw członkowskich i państw trzecich, jak również organy uczestniczące w wykonaniu budżetu przekazują właściwemu intendentowi informacje o kandydatach i oferentach, którzy znajdują się w jednej z sytuacji, o których mowa w art. 93 ust. 1 lit. e) (tj. wobec których wydany został prawomocny wyrok). Informacje te przekazuje się, jeżeli dany podmiot postępował ze szkodą dla interesów finansowych Wspólnot (art. 95 ust. 2). Konsekwencje związane z działalnością tych podmiotów zostaną przeanalizowane poniżej.

([8]) Zob. art. 11-13 i art. 18 rozporządzenia 45/2001. Na temat pojęcia proaktywnego podejścia — zob. dokument pt. *EDPS Background paper: public access to documents and data protection*, z dnia 12 lipca 2005 r. dostępny pod adresem: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/21

([9]) Art. 93 i 94 (rozważane łącznie z art. 114 ust. 2) ustanawiają obowiązek wykluczenia stron trzecich z udziału w procedurze udzielania zamówień lub przyznawania dotacji, jeżeli znajdują się one w jednej z sytuacji wymienionych w art. 93 RF, lub zakazują udzielenia zamówienia lub przyznania dotacji stronom trzecim, które znajdują się w sytuacji konfliktu interesów lub są winne wprowadzenia w błąd przy dostarczaniu informacji wymaganych przez instytucję zamawiającą jako warunek udziału w procedurze udzielania zamówień lub przyznawania dotacji.

([10]) Art. 1 RF: Do celów RF Komitet Ekonomiczno-Społeczny, Komitet Regionów, Rzecznika Praw Obywatelskich oraz Europejskiego Inspektora Ochrony Danych traktuje się jako instytucje wspólnotowe.

([11]) Zob. Opinia EIOD z kontroli wstępnej dotyczącej systemu wczesnego ostrzegania Europejskiego Trybunału Sprawiedliwości, która zostanie opublikowana na stronie internetowej EIOD.

([12]) C(2004) 193/3 wraz ze sprostowaniem C(2004)517, ostatnio zmieniona przepisami wewnętrznymi z 2006 roku — zob.: http://ec.europa.eu/budget/library/sound_fin_mgt/ews_decision_en.pdf .

11. EIOD zgadza się z zasadą centralnej bazy danych kandydatów i oferentów, którzy znaleźli się w jednej z sytuacji, o których mowa w art. 93, 94 i 96 ust. 1 lit. b) i ust. 2 lit. a), w świetle celów przetwarzania danych przewidzianych w RF. Celami tymi jest zwiększenie efektywności, poprawa ochrony interesów finansowych Wspólnot i zapewnienie przepływu informacji zastrzeżonych dotyczących stron trzecich.

12. Ponieważ jednak centralne bazy danych i systemy na wielką skalę są obecnie coraz powszechniej stosowane, EIOD uważa, że w każdym przypadku należy właściwie i ostrożnie ocenić potrzebę ustanowienia takiej bazy danych, a kiedy baza danych zostanie utworzona, należy wdrożyć określone zabezpieczenia w świetle zasad ochrony danych. Celem tych działań jest uniknięcie wszelkich zdarzeń, które mogłyby w niewłaściwy sposób wpłynąć na ochronę danych osobowych. Zdaniem EIOD, każdy wniosek przewidujący stworzenie centralnego repozytorium danych osobowych musi być zgodny z ramami regulacyjnymi europejskiej ochrony danych i w konkretny sposób wprowadzać je w życie. Na przykład art. 4 (Jakość danych), 5 (Legalność przetwarzania) i 10 (Przetwarzanie szczególnych kategorii danych) rozporządzenia 45/2001 mają bardzo duże znaczenie dla przetwarzania danych osobowych przez instytucje europejskie.

13. EIOD podkreśla ponadto, że dane osobowe powinny być gromadzone do zgodnych z prawem celów (art. 4 ust. 1 lit. b) rozporządzenia 45/2001). W tym kontekście EIOD uważa, że o ile w uzasadnionym interesie instytucji i organów leży utworzenie systemu w celu ochrony interesów finansowych i dobrego imienia Wspólnot, wprowadzenie ostrzeżenia o osobie może mieć poważne negatywne skutki dla podmiotu danych i z tego powodu muszą być dostępne określone zabezpieczenia w celu ochrony uzasadnionych interesów podmiotu danych. Kwestię tych zabezpieczeń rozwinięto w kolejnych punktach.

II.2.a. *Zainteresowane podmioty danych*

14. Baza danych EWS oparta jest na zatwierdzanych centralnie „aktach dotyczących osób prawnych" (zwanych dalej „LEF" — *legal entity file*) i korzysta z zawartych w niej danych. LEF jest ogólną bazą danych obejmującą osoby prawne lub fizyczne, które kiedykolwiek miały stosunki umowne lub finansowe z jedną ze służb Komisji: usługodawców, pracowników, ekspertów, beneficjentów dotacji. Art. 95 wniosku dotyczącego RF odnosi się jedynie do kandydatów i oferentów i nie ma zastosowania do członków personelu, ponieważ nie mogą oni być jednocześnie kandydatami lub oferentami. W tym względzie EIOD sugeruje doprecyzowanie definicji kandydatów i oferentów we wniosku dotyczącym ZW w celu uniknięcia nieporozumień co do podmiotów objętych bazą danych.

15. Ponadto EIOD sugeruje, by w art. 134a wniosku dotyczącego ZW jaśniej określić kategorie podmiotów, których dotyczy baza danych.Art. 134a obejmuje strony trzecie, zwane także w LEF podmiotami prawnymi, które są osobami fizycznymi lub prawnymi. Poza tym wniosek przewiduje trzecią kategorię w tym sensie, że informacje mogą również dotyczyć osób fizycznych upoważnionych do reprezentowania danych osób prawnych, podejmowania w ich imieniu decyzji bądź sprawowania nad nimi kontroli. A zatem, w tym ostatnim przypadku, system obejmuje również osoby fizyczne w takim zakresie, w jakim mają one upoważnienie do reprezentowania innych podmiotów. Zgodnie z obecną praktyką osoby te dołącza się do bazy danych jako nowy, odrębny wpis. Korzystne będzie jaśniejsze określenie powiązań i różnic między osobami prawnymi a osobami fizycznymi upoważnionymi do reprezentowania danych osób prawnych, podejmowania w ich imieniu decyzji bądź sprawowania nad nimi kontroli.

II.2.b. *Aktualizacja informacji zapisanych w bazie danych*

16. Zasada jakości danych (art. 4 rozporządzenia 45/2001) wymaga, by dane były prawidłowe, stosowne oraz nienadmierne w stosunku do celów, dla których są gromadzone ([13]). Jest jasne, że jakość danych osobowych można zapewnić jedynie pod warunkiem regularnej i właściwej kontroli ich prawidłowości. Zgodnie z procedurą przewidzianą obecnie w art. 134a ust. 2 wniosku dotyczącego ZW Komisja poprzez zabezpieczony protokół dostarcza regularnie zweryfikowane dane figurujące w bazie danych wyznaczonym osobom w instytucjach, agencjach wykonawczych oraz organach, o których mowa w ust. 1. Zaproponowany harmonogram jest niejasny. EIOD zdaje sobie sprawę z tego, że rozważane są inne rozwiązania, w tym stałe dostarczanie danych. Nie byłoby to jednak wystarczające. Zdaniem EIOD, aktualizacja centralnej bazy danych musi być częsta, a częstotliwość musi być usystematyzowana i zgodna z określonym harmonogramem (comiesięczne lub cotygodniowe przesyłanie danych pomogłoby zapewnić ich prawidłowość i odpowiednio szybką aktualizację).

II.2.c. *Zarządzanie i bezpieczeństwo*

17. Centralna baza danych musi być odpowiednio chroniona. Zarządzanie optymalnym poziomem bezpieczeństwa centralnej bazy danych i przestrzeganie tego poziomu stanowi podstawowy wymóg zapewniający odpowiednią ochronę i aktualizację danych osobowych przechowywanych w bazie danych. W celu osiągnięcia tego satysfakcjonującego poziomu ochrony należy wdrożyć odpowiednie zabezpieczenia, dzięki którym będzie można zarządzać potencjalnym ryzykiem związanym z infrastrukturą systemu i z osobami go obsługującymi.

([13]) W systemie EWS zawarte są następujące informacje: Imię i nazwisko oraz adres osoby — Rodzaj ostrzeżenia EWS — Data początkowa — Data końcowa aktywnego ostrzeżenia — Służba Komisji, która wystąpiła z wnioskiem o wystosowanie ostrzeżenia EWS.

18. W tym względzie EIOD uważa, że konieczne jest wprowadzenie spójnego systemu selekcji intendentów, aby umożliwić odpowiednią ochronę informacji przechowywanych w centralnej bazie danych i jej integralności. Chociaż art. 134a przewiduje selekcję i określenie zadań intendenta właściwego do złożenia wniosku o umieszczenie wpisu w bazie danych i do otrzymania zatwierdzonych danych z tej bazy, procedura ta jest przewidziana jedynie dla instytucji, agencji wykonawczych lub organów, o których mowa w art. 185 RF, i stosowana w odniesieniu do Komisji w ramach decyzji Komisji o systemie wczesnego ostrzegania. Nie przewidziano żadnych szczegółowych zasad w odniesieniu do sytuacji państw członkowskich, państw trzecich lub organizacji międzynarodowych. Sytuacja ta może spowodować brak spójności w ochronie udostępnianych danych.

19. EIOD zaleca umieszczenie w uzupełniających zasadach administracyjnych przepisów dotyczących sposobu udostępniania danych władzom i organom państw członkowskich, państw trzecich i organizacji międzynarodowych, jak również ilości danych, jaką można udostępnić. EIOD uważa, że istotne jest nie tylko zapewnienie bezpieczeństwa informacji przechowywanych w bazie danych, ale także przesyłania informacji do właściwych i uprawnionych organów, a wewnątrz tych organów — wyłącznie do odpowiednich urzędników.

II.2.d *Wymiana danych*

20. EIOD przyjmuje z uznaniem utworzenie jednego, centralnego punktu dostępu do bazy danych, koordynowanego przez Komisję. Ponadto wniosek dotyczący RF rozszerza obecny zakres EWS, ponieważ przewiduje dostęp dla większej liczby władz i organów niż w poprzedniej wersji. Ponadto wniosek dotyczący RF przewiduje różne sytuacje dotyczące dostępu do informacji. Sytuacje te dotyczą różnych władz i organów i muszą być analizowane osobno. Z perspektywy ochrony danych EIOD zauważa, że prawo dostępu do bazy danych, przyznane różnym organom, prowadzi do przekazywania danych do każdego z zainteresowanych organów, pomimo faktu, że dane te są przechowywane przez Komisję. Analizę należy zatem przeprowadzić w świetle art. 7, 8 i 9 rozporządzenia 45/2001, które dotyczą przekazywania danych.

21. Wniosek dotyczący RF rozróżnia dwa przypadki przekazywania danych. Pierwszy z nich dotyczy przekazywania danych wewnątrz instytucji i organów wspólnotowych lub między nimi. Drugi odnosi się do prawa dostępu państw członkowskich i państw trzecich lub organów międzynarodowych. Do celów niniejszej opinii EIOD dokonuje odrębnej analizy sytuacji państw członkowskich oraz sytuacji państw trzecich lub organów międzynarodowych, gdyż te dwie sytuacje podlegają odrębnym przepisom rozporządzenia 45/2001.

22. Pierwsza sytuacja podlega przepisom art. 95 ust. 1 wniosku dotyczącego RF, który stanowi, że centralna baza danych utworzona i zarządzana przez Komisję jest wspólna dla instytucji, agencji wykonawczych oraz organów, o których mowa w art. 185 RF. EIOD podkreśla, że jeżeli przewidziane jest przekazywanie danych wewnątrz instytucji lub organów wspólnotowych albo między nimi, zastosowanie ma art. 7 rozporządzenia 45/2001. EIOD przypomina w związku z tym, że odbiorca danych przetwarza je jedynie do celów, dla których zostały one przesłane.

23. Dostęp państw członkowskich, państw trzecich i organizacji międzynarodowych podlega przepisom art. 95 ust. 2 akapit drugi wniosku dotyczącego RF. Mają one dostęp do informacji zawartych w bazie danych oraz, w stosownych przypadkach i na ich własną odpowiedzialność, mogą je brać pod uwagę przy udzielaniu zamówień związanych z wykonaniem budżetu. Wniosek przewiduje zatem automatyczny dostęp do bazy danych w ramach udzielania zamówień związanych z wykonaniem budżetu.

24. EIOD podkreśla, że jeżeli odbiorcami danych są państwa członkowskie, zastosowanie ma art. 8 rozporządzenia 45/2001. Artykuł ten dotyczy przekazywania danych osobowych odbiorcom, innym niż instytucje i organy wspólnotowe, podlegającym dyrektywie 95/46/WE. W tym przypadku art. 8 lit. a) jest prawdopodobnie przestrzegany, biorąc pod uwagę fakt, że „konieczny" charakter danych w celu wypełnienia zadań wykonywanych przez odbiorców związany jest z wybranym przez Komisję sposobem wykonania budżetu. Ponadto wszystkie te organy działają na mocy prawa krajowego wprowadzającego w życie dyrektywę 95/46 w celu wykonania budżetu europejskiego.

25. Jeżeli chodzi o państwa trzecie i organizacje międzynarodowe, zastosowanie ma art. 9 rozporządzenia 45/2001 ([14]). Art. 9 ust. 1 ustanawia zakaz przekazywania danych osobowych odbiorcom, innym niż instytucje i organy wspólnotowe, które nie podlegają prawu krajowemu przyjętemu na mocy dyrektywy 95/46/WE, chyba że w państwie odbiorcy lub w organizacji międzynarodowej będącej odbiorcą zapewniony jest odpowiedni poziom ochrony, a dane przekazywane są wyłącznie w celu umożliwienia wykonania zadań należących do kompetencji administratora danych. Rozporządzenie 45/2001 przewiduje odstępstwa, które obejmują sytuację udzielania zamówień związanych z wykonaniem budżetu. EIOD podkreśla jednak, że odstępstwa te należy interpretować w sposób zawężający. Preferowane jest zapewnienie odpowiednich zabezpieczeń w przypadku przekazywania o charakterze strukturalnym. W kontekście przekazywania danych z centralnej bazy danych, przekazywanie to ma charakter strukturalny, i dlatego potrzeba zabezpieczeń, takich jak klauzule umowne w umowie o przyznaniu środków finansowych UE, powinna zostać ustanowiona w zasadach wykonawczych.

([14]) Art. 9 jest porównywalny do art. 25 i 26 dyrektywy 95/46/WE.

26. Poza tym, państwom trzecim dostarczane są nie tylko dane z centralnej bazy danych, zgodnie z art. 95 RF. Art. 134a ZW przewiduje również otrzymywanie danych od państw trzecich i organizacji międzynarodowych, i w tym zakresie zaświadczają one Komisji, że informacje zostały zebrane i przekazane stosowanie do przepisów dotyczących ochrony danych osobowych. W tym kontekście EIOD podkreśla znaczenie zasady jakości danych podczas międzynarodowego przekazywania danych. Należy zapewnić przestrzeganie przepisów rozporządzenia 45/2001 dotyczących prawidłowości i aktualizacji danych dostarczanych Komisji i umieszczanych w bazie danych. Przy zawieraniu umów w sprawie finansowania ważne będzie zatem określenie objętych nimi danych i gwarancji związanych z jakością danych. Zapis na temat konieczności tych zabezpieczeń powinien znaleźć się również w zasadach wykonawczych.

II.2.e. *Prawa kandydatów i oferentów*

27. Kandydaci i oferenci zarejestrowani w centralnej bazie danych korzystają z zabezpieczeń dotyczących zarządzania ich danymi osobowymi w tej bazie. Zabezpieczenia te powinny obejmować przede wszystkim prawa podmiotu danych do bycia informowanym i do otrzymania dostępu do dotyczących go danych.

28. Prawo do bycia informowanym jest zawarte w art. 134a ust. 1 akapit trzeci wniosku dotyczącego ZW. EIOD uważa jednak, że brzmienie tego akapitu powinno zostać zmienione i interpretowane w następujący sposób: „Instytucje, agencje wykonawcze oraz organy, o których mowa w art. 95 ust. 1 i 2 rozporządzenia finansowego, zaświadczają Komisji, że informacje te zostały zebrane i przekazane stosownie do przepisów dotyczących ochrony danych osobowych, oraz że dana osoba trzecia została poinformowana o przekazaniu tych informacji." EIOD podkreśla, że rozporządzenie 45/2001 ma zastosowanie do instytucji, agencji wykonawczych i organów, ale że ustawodawstwo krajowe wprowadzające w życie dyrektywę 95/46/WE będzie miało zastosowanie w państwach członkowskich. Problemy mogą pojawić się jednak na szczeblu krajowym, kiedy państwo trzecie nie zapewni swoim obywatelom prawa do bycia informowanym. EIOD uważa, że Komisja powinna zapewnić mechanizm pozwalający kandydatom i oferentom na otrzymanie informacji o ich umieszczeniu w centralnej bazie danych.

29. EIOD zgadza się ponadto z proaktywnym podejściem do prawa do informacji ([15]). W sprawie będącej przedmiotem kontroli wstępnej, dotyczącej wdrożenia systemu wczesnego ostrzegania Trybunału Sprawiedliwości ([16]), EIOD z zadowoleniem przyjmuje fakt, że wszystkie strony trzecie informowane są wcześniej o tym, że ich dane osobowe mogą być użyte przez Trybunał nie tylko do celów wewnętrznych związanych z procedurą udzielania zamówień, ale także przekazane innym instytucjom w kontekście art. 93 i 94 RF w celu umieszczenia ich w bazie danych Komisji przewidzianej w art. 95 RF. W takich przypadkach strona trzecia jest już poinformowana o możliwości wykluczenia jej z udziału w procedurze udzielania zamówień lub z udzielenia zamówienia, jeżeli jej dane są umieszczone w bazie danych Komisji. Na tej samej zasadzie EIOD uznaje również starania poczynione na rzecz zapewnienia dodatkowych praw do informacji. Na przykład, motyw 36 wniosku dotyczącego RF dotyczy prawa do informacji, jakie mają być przekazywane oferentom, których oferty odrzucono, już po udzieleniu zamówienia. Jak już podkreślono w niniejszej opinii, EIOD proponuje, by stosowano tę procedurę we wszystkich zainteresowanych instytucjach, władzach i organach i aby zalecono ją we wniosku dotyczącym ZW.

30. Art. 13 rozporządzenia 45/2001 ustanawia prawo dostępu podmiotu danych do informacji przetwarzanych przez administratorów danych. Aby wprowadzić w życie to prawo, należy zatem stwierdzić w zasadach wykonawczych, że każda strona trzecia umieszczona w bazie danych ma prawo dostępu do dotyczących jej danych oraz że prawa tego nie należy ograniczać z powodów innych niż te wymienione w art. 20 rozporządzenia 45/2001. Ponadto prawo dostępu jest ściśle związane ze wspomnianym wyżej podejściem proaktywnym w takim sensie, że osoba nieświadoma tego, iż jej dane zostały umieszczone w bazie danych, w rezultacie nie będzie w stanie skorzystać ze swojego prawa dostępu.

II.2.f. *Potrzeba kontroli wstępnej*

31. Zgodnie z art. 27 ust. 2 lit. b) rozporządzenia 45/2001 operacje przetwarzania zmierzające do oceny aspektów osobistych odnoszących się do podmiotu danych, włącznie z jego możliwościami, wydajnością lub postępowaniem, mogą stworzyć określone zagrożenia wobec praw podmiotów danych. Ponadto podobnie jest w przypadku danych związanych z operacjami przetwarzania w celu pozbawienia jednostki prawa, świadczenia lub wyłączenia jej z umowy (art. 27 ust. 2 lit. d)).

32. W dniu przyjęcia niniejszej opinii zarówno Komisja Europejska, jak i Europejski Trybunał Sprawiedliwości, zgłosiły EIOD wniosek o przeprowadzenie kontroli wstępnej systemu wczesnego ostrzegania na podstawie istniejącej wersji RF. Ponieważ w nowej wersji RF wprowadzono zmiany dotyczące zarządzania bazą danych w odniesieniu do utworzenia i funkcjonowania wspólnej bazy danych, do której będą miały dostęp i do której będą przesyłać dane państwa członkowskie, państwa trzecie i organizacje międzynarodowe, EIOD uważa to za istotną zmianę podlegającą przepisom art. 27 rozporządzenia 45/2001. A zatem, kiedy Komisja podejmie kroki w celu wdrożenia nowych ram prawnych, EIOD przeprowadzi kontrolę wstępną systemu.

III. **TERMINY DOTYCZĄCE PRZECHOWYWANIA DANYCH I KONTROLI BUDŻETOWEJ**

33. EIOD chciałby skorzystać z tej okazji i zwrócić uwagę na przepis, który analizował przy okazji wcześniejszych kontroli wstępnych związanych z kwestiami budżetowymi, chociaż przepis ten nie jest objęty obecnymi zmianami zawartymi we wnioskach.

([15]) Na temat zasady przejrzystości — zob. powyżej.
([16]) Wkrótce zostanie opublikowana pod adresem: www.europa.edps.eu

Istniejące ramy

34. Art. 49 obecnych ZW dotyczący przechowywania dokumentów towarzyszących przez intendentów stanowi, że: „systemy i procedury zarządzania dotyczące zachowania oryginalnych dokumentów towarzyszących przewidują, że: (...) d) dokumenty takie mają być przechowywane przez co najmniej pięć lat od dnia, w którym Parlament Europejski udzielił absolutorium za rok budżetowy, do którego odnoszą się te dokumenty. Dokumenty odnoszące się do operacji niezamkniętych ostatecznie przechowywane są przez okres dłuższy niż przewidziany w akapicie pierwszym lit. d), to znaczy do końca roku następującego po roku, w którym operacje zostały zamknięte".

35. Ustanowiona w ZW zasada dotycząca przechowywania dokumentów towarzyszących przewiduje zatem możliwość ich przechowywania przez okres do 7 lat w celu udzielenia absolutorium budżetowego ze sprawozdań finansowych instytucji i organów europejskich.

36. Dokumenty towarzyszące przechowywane przez intendentów mogą zawierać dane osobowe i w tym zakresie zasady dotyczące przechowywania danych osobowych ustanowione w rozporządzeniu 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych również mają zastosowanie.

37. Art. 4. ust. 1 lit. c) rozporządzenia 45/2000 przewiduje co do zasady, że dane osobowe muszą być prawidłowe, stosowne oraz nienadmierne w stosunku do celów, dla których są gromadzone lub dalej przetwarzane. Art. 4 ust. 1 lit. e) rozporządzenia przewiduje ponadto, że dane osobowe mogą być przechowywane w formie, która pozwala na zidentyfikowanie podmiotów danych przez czas nie dłuższy niż jest to konieczne do celów, dla których dane były gromadzone lub dalej przetwarzane.

38. Art. 37 rozporządzenia przewiduje szczegółowe zasady dotyczące przechowywania danych o połączeniach i danych billingowych w kontekście wewnętrznych sieci komunikacyjnych. Sieci takie zdefiniowane są w art. 34 jako „sieci telekomunikacyjne lub urządzenia końcowe działające pod kontrolą instytucji lub organu Wspólnoty". Artykuł ten ma zatem zastosowanie do danych o połączeniach i danych billingowych gromadzonych przez wewnętrzne sieci instytucji lub organów Wspólnoty.

39. Zgodnie z art. 37 ust. 1 dane o połączeniach, które są przetwarzane i przechowywane w celu ustanowienia połączeń telefonicznych i innych połączeń dokonywanych przez sieć telekomunikacyjną, zostają usunięte lub stają się anonimowe po zakończeniu połączenia telefonicznego lub innego połączenia. Zasadą jest zatem usuwanie danych kiedy tylko przestaną być one potrzebne do ustanowienia połączenia telefonicznego lub innego połączenia.

40. Artykuł 37 ust. 2 przewiduje jednak, że dane o połączeniu ([17]), wskazane w wykazie uzgodnionym przez EIOD, mogą być przetwarzane w celu zarządzania budżetem i połączeniami, włącznie ze sprawdzaniem uprawnionego korzystania z systemów telekomunikacyjnych. Dane te należy usunąć lub uczynić anonimowymi tak szybko, jak to jest możliwe, i nie później niż w sześć miesięcy po ich zgromadzeniu, o ile nie muszą być one przechowywane przez czas dłuższy w celu ustalenia, wykonania lub obrony prawa w ramach postępowania sądowego. Jeżeli przed upływem sześciomiesięcznego okresu nie zostanie wszczęte postępowanie, dane o połączeniu należy usunąć bądź powinny one stać się anonimowe. Jeżeli przed upływem tego okresu wszczęto postępowanie, bieg przewidzianego okresu zostaje wstrzymany na czas postępowania, a następnie na czas okresu przewidzianego na wszelkie odwołania lub na przeprowadzenie postępowania odwoławczego, w zależności od przypadku. Przechowywanie danych o połączeniu i danych billingowych po upływie wspomnianego sześciomiesięcznego okresu może być uzasadnione jedynie na podstawie art. 20.

41. Art. 20 rozporządzenia 45/2001 stanowi, że można wprowadzić zwolnienia i ograniczenia względem przepisu o natychmiastowym usuwaniu danych o połączeniu przewidzianym w art. 37 ust. 1 w pewnej ograniczonej liczbie przypadków wymienionych w tym pierwszym artykule. Możliwe jest w szczególności zachowanie danych o połączeniu jeżeli działanie to jest niezbędne do ochrony zapobiegania przestępstwom, dochodzenia w ich sprawie oraz ich wykrywania i karania; ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Wspólnot Europejskich, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi; bądź też ochrony podmiotu danych lub praw i wolności innych osób. Art. 20, jako wyjątek od zasad ochrony danych przewidzianych w rozporządzeniu, należy interpretować w sposób zawężający i ma on zastosowanie tylko w odniesieniu do indywidualnych przypadków. Ponadto art. 20 przewiduje jedynie wyjątki od zasady natychmiastowego usunięcia danych o połączeniu ustanowionej w art. 37 ust. 1, a nie od sześciomiesięcznego terminu przewidzianego w art. 37 ust. 2. Art. 20 nie może zatem służyć jako uzasadnienie przechowywania danych o połączeniu powyżej sześciu miesięcy do ogólnych celów kontroli, jak przewidziano w art. 49 ZW.

Konieczność przeglądu

42. EIOD zaleca zatem, by dokonano przeglądu przepisów ZW dotyczących przechowywania dokumentów towarzyszących, tak by zapewnić przestrzeganie zasad regulujących ochronę danych osobowych.

43. Aby zapewnić przestrzeganie tych zasad, informacje zawarte w dokumentach towarzyszących należy zweryfikować. Dokumenty towarzyszące zawierają różne poziomy informacji: ogólne informacje mające znaczenie dla udzielenia absolutorium z wykonania budżetu, w tym ewentualne informacje dotyczące kontroli, oraz informacje szczegółowe, które same w sobie nie są niezbędne do kontroli budżetowej.

44. Ogólna zasada powinna przewidywać, że jeżeli dokumenty towarzyszące zawierają dane osobowe, to przetworzone mogą zostać jedynie dane osobowe niezbędne do celów udzielenia absolutorium z wykonania budżetu. O ile jest to możliwe, dokumenty zawierające dane osobowe, które nie są niezbędne do tego celu, powinny zostać usunięte. Istotne dane można przechowywać jedynie przez okres niezbędny do udzielenia absolutorium z wykonania budżetu. Okres 5-7 lat ustanowiony w art. 49 ZW należy w każdym razie uznać za maksymalny okres przechowywania dokumentów towarzyszących.

([17]) Dane billingowe nie są wyraźnie wymienione w art. 37 ust. 2, ale w sposób domyślny można je włączyć do jego zakresu.

45. Jeżeli chodzi o przechowywanie dokumentów towarzyszących zawierających szczegółowe informacje, takie jak dane o połączeniu, powinna obowiązywać zasada, że takie dane o połączeniu należy usunąć, gdyż nie są one niezbędne do celów udzielenia absolutorium z wykonania budżetu. Jeżeli dokumenty towarzyszące zawierają różne poziomy informacji, to najniższy i najbardziej szczegółowy poziom informacji, do których mogą należeć dane o połączeniu, nie jest niezbędny i nie należy go przechowywać do celów udzielenia absolutorium z wykonania budżetu. Jeżeli dokumenty towarzyszące nie zawierają różnych poziomów informacji, należy rozważyć częściowe przetworzenie danych zawartych w dokumentach, pod warunkiem że nie wymaga to podjęcia niewspółmiernych wysiłków.

46. Dla zilustrowania tej kwestii, EIOD chciałby posłużyć się przykładem budżetu na telefonię stacjonarną w instytucjach. Jeżeli chodzi o telefonię stacjonarną, zasada ustanowiona w art. 37 implikuje, że dane o połączeniu, takie jak numer przychodzący, numer wybierany oraz długość połączenia, mogą być przechowywane w celu zarządzania połączeniami i zarządzania budżetem, w tym w celu sprawdzenia uprawnionego korzystania z systemu komunikacji przez okres do 6 miesięcy. Po należytym sprawdzeniu uprawnionego korzystania z narzędzi komunikacji wszelkie dane o połączeniu należy usunąć lub uczynić anonimowymi. Jeżeli konieczne jest przechowanie danych do celów kontroli kosztów komunikacji zgodnie z ZW, nie ma potrzeby przechowywania szczegółowych danych o połączeniu. Jedynymi istotnymi danymi, które można przechowywać do celów budżetowych, są dane dotyczące kosztów komunikacji nieujawniające związanych z nimi danych o połączeniu ([18]).

Sugerowane zmiany w art. 49

47. Aby uwzględnić omówioną kwestię zgodności, EIOD sugeruje dodanie w art. 49 ZW akapitu w brzmieniu: „*Dane osobowe zawarte w dokumentach towarzyszących należy usunąć o ile to możliwe, jeżeli dane te nie są niezbędne do celów udzielenia absolutorium z wykonania budżetu. W każdym przypadku należy przestrzegać przepisów art. 37 ust. 2 rozporządzenia (WE) 45/2001 w odniesieniu do przechowywania danych o połączeniu*".

IV. **WNIOSKI**

EIOD z zadowoleniem przyjmuje decyzję o zasięgnięciu jego opinii w sprawie przedmiotowych wniosków, które przewidują należyte i bardziej przejrzyste zarządzanie środkami finansowymi Wspólnoty. Przy tej okazji EIOD pragnie również zwrócić uwagę na pewne szczegółowe aspekty ochrony danych związane z wprowadzeniem w życie tych wniosków, szczególnie w kontekście systemu wczesnego ostrzegania.

Co do treści EIOD zaleca, co następuje:

— w zasadach wykonawczych należy umieścić odniesienia do proaktywnego podejścia (wcześniejsze informowanie i informacje zwrotne), które powinno być powszechnie stosowane przez wszystkie zainteresowane instytucje, władze i organy w świetle zasady przejrzystości;

— w momencie utworzenia centralnej bazy danych należy wprowadzić konkretne zabezpieczenia w świetle zasad ochrony danych;

— w art. 134a zasad wykonawczych należy sprecyzować pojęcia kandydatów i oferentów, jak również kategorie podmiotów, których dotyczy baza danych;

— w zasadach wykonawczych należy umieścić dokładne ramy czasowe dotyczące aktualizacji informacji zawartych w bazie danych;

— w celu uniknięcia niespójności — należy wprowadzić system selekcji intendentów w państwach członkowskich, władzach i organach; zasady ich dostępu do informacji, jak również zakres udostępnianych im danych zgodnie z art. 95 ust. 2 należy określić w uzupełniających przepisach administracyjnych;

— w kontekście przekazywania danych osobowych z centralnej bazy danych w zasadach wykonawczych należy ustanowić zabezpieczenia, takie jak klauzule umowne, w związku z tym, że takie przekazywanie ma charakter strukturalny;

— w kontekście otrzymywania danych z państw trzecich i organizacji międzynarodowych ważne będzie określenie zakresu danych, których to dotyczy, oraz gwarancji związanych z jakością, a potrzeba takich zabezpieczeń powinna zatem zostać ujęta w zasadach wykonawczych;

— należy zmienić brzmienie art. 134a ust. 1 akapit trzeci zasad wykonawczych, tak by odnosił się on do instytucji, agencji wykonawczych, władz i organów, o których mowa w art. 95 ust. 1 i 2 rozporządzenia finansowego;

— w odniesieniu do prawa dostępu kandydatów i oferentów należy umieścić odniesienie do art. 13 rozporządzenia 45/2001;

— EIOD sugeruje dodanie ustępu do art. 49 ZW w celu uwzględnienia kwestii zgodności z art. 37 rozporządzenia 45/2001.

Co do procedury, EIOD:

— zaleca umieszczenie w preambule do wniosku wyraźnego odniesienia do niniejszej opinii;

— przypomina, że w związku z wprowadzeniem przez przewidziane operacje przetwarzania znacznych zmian do zarządzania bazą danych, przez co podlegać będą one przepisom art. 27 rozporządzenia 45/2001, EIOD ma obowiązek przeprowadzić wstępną kontrolę systemu przed jego wdrożeniem.

Sporządzono w Brukseli, dnia 12 grudnia 2006 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

([18]) Wyraźną ilustrację tego przypadku można znaleźć w opinii EIOD w sprawie procedury TOP 50 Parlamentu Europejskiego (sprawa 2004-0126).