# Sprawozdanie roczne

# 2006

Europejski Inspektor
Ochrony Danych

# Sprawozdanie roczne

# 2006

Europejski Inspektor
Ochrony Danych

Adres do korespondencji: EDPS, rue Wiertz 60, B-1047 Bruxelles
Siedziba: rue Montoyer 63, Bruxelles
E-mail: edps@edps.europa.eu
Internet: http://edps.europa.eu
Tel. (32-2) 283 19 00
Faks (32-2) 283 19 50



Wiele informacji o Unii Europejskiej znajduje się w Internecie w portalu Europa (http://europa.eu).

Dane katalogowe znajdują się na końcu niniejszej publikacji.

Luksemburg: Urząd Oficjalnych Publikacji Wspólnot Europejskich, 2007

ISBN 978-92-95030-26-8

# Spis treści

# Podręcznik użytkownika

Bezpośrednio po tekście niniejszego podręcznika zamieszczone jest określenie misji i przedmowa przygotowana przez Petera Hustinxa, Europejskiego Inspektora Ochrony Danych (EIOD).

Rozdział 1 – **Bilans i perspektywy** przedstawia ogólny przegląd działań EIOD. Rozdział ten prezentuje również wyniki osiągnięte w 2006 roku i przedstawia cele na 2007 rok.

Rozdział 2 – **Nadzór** obszernie opisuje działania realizowane w celu zapewnienia wykonywania przez instytucje i organy WE obowiązków związanych z ochroną danych oraz monitorowania tych instytucji i organów. Po ogólnym przeglądzie przedstawiono rolę urzędników ds. ochrony danych (DPO) w administracji UE. Ten rozdział obejmuje analizę kontroli wstępnych, skarg i postępowań wyjaśniających oraz porad dotyczących środków administracyjnych, którymi zajmowano się w 2006 roku. Ustosunkowuje się również do protokołu ustaleń podpisanego z Europejskim Rzecznikiem Praw Obywatelskich i przedstawia działania podjęte w następstwie opublikowanego w lipcu 2005 roku dokumentu na temat przejrzystości i publicznego dostępu. Ponadto zawiera sekcję dotyczącą e-monitoringu oraz aktualizację informacji na temat nadzoru nad systemem Eurodac.

Rozdział 3 – **Konsultacje** obejmuje działania EIOD dotyczące jego funkcji doradczej, koncentrując się na opiniach wydawanych na temat wniosków prawodawczych i dokumentów pokrewnych, jak również na wpływie, jaki wywierają one w coraz liczniejszych dziedzinach. Rozdział ten zawiera także analizę tematów horyzontalnych i wprowadza pewne nowe zagadnienia technologiczne, takie jak rola technologii wspomagających oraz badań i rozwoju dla ochrony prywatności i danych.

Rozdział 4 – **Współpraca** opisuje działania realizowane w ramach kluczowych forów, takich jak grupa robocza art. 29, w ramach wspólnych organów nadzoru „trzeciego filaru", a także podczas Europejskiej oraz Międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych.

Rozdział 5 – **Komunikacja** przedstawia „inicjatywę londyńską" i stanowi przegląd wykorzystania różnych narzędzi komunikacji, takich jak strona internetowa, biuletyny, służba prasowa i przemówienia.

Rozdział 6 – **Administracja**, **budżet i personel** obejmuje główne zagadnienia organizacyjne, w tym kwestie budżetowe, kwestie związane z zasobami ludzkimi i porozumienia administracyjne.

Sprawozdanie uzupełniają **załączniki**, które zawierają przegląd stosownych ram prawnych, fragmenty rozporządzenia (WE) nr 45/2001, wykaz skrótów, statystyki dotyczące kontroli wstępnych, wykaz urzędników ds. ochrony danych w poszczególnych instytucjach i organach, skład sekretariatu EIOD itp.

Opublikowano odrębne **streszczenie** dla osób, które preferują krótkie przedstawienie rozwoju wydarzeń w 2006 roku.

Osoby, które chcą uzyskać więcej informacji na temat EIOD, zachęca się do odwiedzenia naszej strony internetowej, która pozostaje głównym narzędziem komunikacji: www.edps.europa.eu. Strona internetowa umożliwia również subskrypcję ukazującego się co dwa miesiące biuletynu.

Papierowe kopie sprawozdania rocznego, jak również jego streszczenia, można zamówić bezpłatnie; dane kontaktowe znajdują się na naszej stronie internetowej.

# Określenie misji

Misją Europejskiego Inspektora Ochrony Danych (EIOD) jest zapewnienie poszanowania podstawowych praw i wolności osób fizycznych – w szczególności ich prywatności – w trakcie przetwarzania ich danych osobowych przez instytucje i organy WE. EIOD jest odpowiedzialny za:

– monitorowanie i zapewnienie przestrzegania przepisów rozporządzenia (WE) nr 45/2001, jak również innych wspólnotowych aktów w sprawie ochrony podstawowych praw i wolności, w trakcie przetwarzania danych osobowych przez instytucje i organy WE („nadzór");
– doradzanie instytucjom i organom WE we wszystkich sprawach związanych z przetwarzaniem danych osobowych. Obejmuje to konsultacje w sprawie wniosków prawodawczych i monitorowanie nowych wydarzeń, które mają wpływ na ochronę danych osobowych („konsultacje");
– współpraca z krajowymi instytucjami nadzoru oraz organami nadzoru w ramach „trzeciego filaru" UE z myślą o poprawie spójności w dziedzinie ochrony danych osobowych („współpraca").

Zgodnie z powyższym EIOD ma na celu prowadzenie strategicznych działań służących:

– promowaniu „kultury ochrony danych" w instytucjach i organach, przyczyniając się w ten sposób również do poprawy dobrego zarządzania;
– włączeniu poszanowania zasad ochrony danych do prawodawstwa i polityk WE, we wszystkich stosownych przypadkach;
– poprawie jakości polityk UE we wszelkich sytuacjach, kiedy skuteczna ochrona danych stanowi podstawowy warunek ich powodzenia.

# Przedmowa

Mam przyjemność przedłożyć Parlamentowi Europejskiemu, Radzie i Komisji Europejskiej trzecie roczne sprawozdanie z moich działań w charakterze Europejskiego Inspektora Ochrony Danych (EIOD), zgodnie z rozporządzeniem (WE) nr 45/2001 Parlamentu Europejskiego i Rady oraz z art. 286 Traktatu WE.

Niniejsze sprawozdanie obejmuje 2006 rok, drugi pełny rok działalności EIOD jako nowego, niezależnego organu nadzoru mającego za zadanie zapewnienie poszanowania przez instytucje i organy wspólnotowe podstawowych praw i wolności osób fizycznych, w szczególności ich prywatności, w odniesieniu do przetwarzania danych osobowych.

Po pierwszych krokach w budowaniu nowej instytucji i rozwoju jej funkcji na poziomie wspólnotowym, w celu monitorowania i zapewnienia stosowania prawnych zabezpieczeń ochrony danych osobowych obywateli Unii Europejskiej, nadszedł czas oceny wyników.

Niniejsze sprawozdanie dowodzi, że w 2006 roku osiągnięto znaczne postępy w różnych dziedzinach. EIOD został uznany za nowy widoczny autorytet w bardzo istotnym obszarze. Większość instytucji i organów UE jest na najlepszej drodze do wprowadzenia zasad ochrony danych do codziennej praktyki. Coraz częściej przywołuje się doradczą rolę EIOD, a jej wpływ zaczyna przynosić pozytywne rezultaty.

Przed nami wciąż co najmniej dwa wyzwania. Pierwsze obejmuje wdrożenie zasad i przepisów w zakresie ochrony danych w *całej* administracji UE oraz rozwój „kultury ochrony danych" jako elementu „dobrych rządów". EIOD rozpocznie podsumowywanie postępów osiągniętych we wszystkich instytucjach i organach począwszy od wiosny 2007 roku i zapewni stosowne informacje na ten temat.

Drugim wyzwaniem jest pełne włączenie zasad ochrony danych do prawodawstwa wspólnotowego oraz poprawa jakości polityk UE we wszystkich sytuacjach, kiedy skuteczna ochrona danych stanowi podstawowy warunek ich powodzenia. Oczywiście obejmuje to również skuteczne włączenie aspektów prywatności w pewnych obszarach – takich jak polityki związane z bezpieczeństwem publicznym i egzekwowaniem prawa – które czasami wydają się zmierzać w innym kierunku.

Chciałbym zatem skorzystać z okazji, by ponownie podziękować wszystkim tym w Parlamencie Europejskim, Radzie i Komisji, którzy nadal wspierają nasze działania, a także wielu innym osobom w różnych instytucjach i organach, które są w bardziej bezpośredni sposób odpowiedzialne za metody realizacji ochrony danych w praktyce. Chciałbym również skierować słowa zachęty do wszystkich tych, którzy będą podejmować stojące przed nami wyzwania.

Wreszcie, chciałbym wyrazić szczególne podziękowanie – również w imieniu Joaquína Bayo Delgado, zastępcy inspektora ochrony danych – członkom personelu uczestniczącym w realizacji naszej misji. Nieprzeciętne zalety personelu walnie przyczyniają się do rosnącej skuteczności naszych działań.

*Peter Hustinx*
*Europejski Inspektor Ochrony Danych*

# 1. Bilans i perspektywy

## 1.1. Ogólny przegląd 2006 roku

Ramy prawne, w obrębie których działa Europejski Inspektor Ochrony Danych (EIOD) ([1]), przewidują wiele zadań i uprawnień umożliwiających podstawowe rozróżnienie trzech głównych funkcji. Funkcje te nadal służą jako strategiczne platformy działań EIOD i są odzwierciedlone w określeniu jego misji:

- funkcja **nadzorcza** polegająca na monitorowaniu i zapewnianiu poszanowania przez instytucje i organy wspólnotowe ([2]) istniejących zabezpieczeń prawnych podczas przetwarzania danych osobowych;
- funkcja **konsultacyjna** polegająca na udzielaniu instytucjom i organom wspólnotowym porad we wszystkich stosownych kwestiach, w szczególności w sprawie wniosków prawodawczych mających wpływ na ochronę danych osobowych;
- funkcja **współpracy** z krajowymi instytucjami nadzoru oraz organami nadzoru w ramach „trzeciego filaru" UE obejmująca współpracę policyjną i sądową w sprawach karnych z myślą o poprawie spójności w dziedzinie ochrony danych osobowych.

Funkcje te zostaną szerzej omówione w rozdziałach 2, 3 i 4 niniejszego sprawozdania rocznego, w których przedstawiono główne działania EIOD i postępy osiągnięte w 2006 roku. Kluczowe znaczenie informacji na temat tych działań oraz przekazywania tych informacji zostało podkreślone osobno w rozdziale 5, dotyczącym **komunikacji**. Większość tych działań opiera się na skutecznym zarządzaniu **zasobami** finansowymi, ludzkimi i innymi, co zostanie omówione w rozdziale 6.

EIOD świadomie postanowił połączyć kwestię „ochrony danych" z innymi stosownymi tematami i wynikami praktycznymi. To dlatego od samego początku podkreślano, że wiele polityk UE jest uzależnionych od **zgodnego z prawem przetwarzania danych osobowych** oraz że **skuteczną ochronę danych osobowych**, jako podstawową wartość leżącą u podstaw polityk UE, należy postrzegać jako **warunek ich powodzenia**. EIOD będzie nadal działać w takim duchu ogólnym i ze swej strony oczekuje pozytywnych reakcji.

W 2006 roku w różnych istotnych obszarach osiągnięto znaczne postępy przybliżające realizację tej perspektywy. W 2007 roku i w latach późniejszych trzeba jednak, idąc w tym samym kierunku, osiągnąć bardziej konkretne postępy, żeby w pełni stała się ona rzeczywistością. EIOD rozpocznie podsumowywanie osiągniętych postępów, czemu będą towarzyszyć różnego rodzaju kontrole we wszystkich instytucjach i organach, począwszy od wiosny 2007 roku. Zadba również o przekazywanie odpowiednich informacji zwrotnych.

## 1.2. Wyniki w 2006 roku

W sprawozdaniu rocznym za 2005 rok wspomniano, że na 2006 rok wybrano następujące cele główne. Większość z tych celów została zrealizowana.

- **Wsparcie sieci DPO**

Liczba urzędników ds. ochrony danych (DPO) wzrosła po opublikowaniu dokumentu EIOD przedstawia-

([1]) Zob. przegląd ram prawnych w załączniku A i wyciąg z rozporządzenia (WE) nr 45/2001 w załączniku B.

([2]) Pojęcia „instytucje" i „organy" pojawiające się w rozporządzeniu (WE) nr 45/2001 stosowane są w całym sprawozdaniu. Obejmuje to również agencje wspólnotowe. Pełny wykaz można znaleźć pod adresem: http://europa.eu/agencies/community_agencies/index_en.htm.

jącego stanowisko w sprawie roli DPO w zapewnianiu skutecznego stosowania rozporządzenia (WE) nr 45/2001. EIOD w dalszym ciągu udzielał silnego wsparcia sieci DPO i zorganizował warsztaty dla nowych DPO. Regularnie mają miejsce dwustronne oceny postępów w zakresie powiadomień w dużych instytucjach.

- **Kontynuacja kontroli wstępnych**

Liczba kontroli wstępnych istniejących operacji przetwarzania danych również znacznie wzrosła i obejmuje obecnie zarówno kategorie priorytetowe, jak i inne. Opinie są publikowane na stronie internetowej. Informacje na temat stosownych polityk i głównych zagadnień będących przedmiotem działań są przekazywane DPO podczas regularnych spotkań, a przedmiotowe polityki i zagadnienia zostały także opisane w niniejszym sprawozdaniu rocznym. W związku z tym nie wydano odrębnego dokumentu strategicznego.

- **E-monitoring i dane o połączeniach**

Końcowa wersja dokumentu zawierającego wytyczne na temat przetwarzania danych osobowych odnoszących się do wykorzystania sieci łączności elektronicznej została przygotowana do publikacji na początku 2007 roku. Zostały już wydane pierwsze opinie na temat kontroli wstępnych w tej dziedzinie. EIOD rozpocznie procedury służące ocenie wykazów zatrzymywanych danych, kiedy zostaną one przedłożone.

- **Wytyczne dotyczące akt osobowych**

EIOD rozpoczął badanie w zakresie aktualnych praktyk dotyczących akt osobowych personelu w instytucjach i organach. Na podstawie jego wyników i analizy kontroli wstępnych w dziedzinach pokrewnych w przygotowaniu znajduje się dokument zawierający stosowne wytyczne. Przeanalizowano przechowywanie danych dotyczących środków dyscyplinarnych i na tej podstawie zostaną wydane zalecenia do ogólnego stosowania.

- **Przekazywanie państwom trzecim**

Przekazywanie danych państwom trzecim i organizacjom międzynarodowym zostało przeanalizowane w dokumencie roboczym i omówione z OLAF. Uwzględniono zarówno potrzebę podejścia strukturalnego zgodnie z rozporządzeniem (WE) nr 45/2001, jak i wykorzystanie protokołów ustaleń i innych elastycznych mechanizmów. Wzięto również pod uwagę stanowisko innych organów UE.

- **Nadzór nad systemem Eurodac**

Obecnie przeprowadzany jest szczegółowy audyt bezpieczeństwa dotyczący centralnej bazy danych Eurodac, a jego wyniki są oczekiwane do połowy 2007 roku. EIOD rozwija ścisłą współpracę z krajowymi organami ds. ochrony danych w zakresie systemu wspólnego nadzoru z myślą o zgromadzeniu i wymianie doświadczeń na potrzeby innych dużych baz danych. Pierwsze wspólne sprawozdanie jest oczekiwane w połowie 2007 roku.

- **Doradcza rola w kwestii prawodawstwa**

Założenia zawarte w dokumencie strategicznym z 2005 roku na temat doradczej funkcji EIOD w zakresie wniosków prawodawczych są realizowane. Liczba wydawanych opinii podwoiła się, a wachlarz tematów, jaki one obejmują, jest szeroki. Pierwszy spis stosownych tematów na 2007 rok opublikowano na stronie internetowej. W następstwie wydawanych opinii systematycznie podejmuje się dalsze działania.

- **Interwencje w sprawach sądowych**

EIOD otrzymał prawo interweniowania w trzech sprawach przed Sądem Pierwszej Instancji dotyczących publicznego dostępu i ochrony danych, wziął również udział w przesłuchaniu publicznym w ramach jednej z nich. Zwrócił się również o interwencję w sprawie przed Trybunałem Sprawiedliwości dotyczącej ważności dyrektywy 2006/24/WE odnoszącej się do zatrzymywania danych. Sprawy sądowe powiązane z kwestiami interpretacji zasad ochrony danych są uważnie monitorowane.

- **Druga wersja strony internetowej**

W styczniu 2007 roku uruchomiono całkowicie zmienioną stronę internetową. Dostęp on-line do rejestru powiadomień dotyczących kontroli wstępnych i kilka innych funkcji zostanie dodanych wiosną 2007 roku. Strona internetowa odzwierciedla obecnie strukturę głównych funkcji EIOD i zapewnia lepszy dostęp do stosownych informacji o poszczególnych dziedzinach działalności.

- **Rozwój zasobów**

EIOD w dalszym ciągu rozwijał niezbędne zasoby i infrastrukturę w celu zapewnienia skutecznego wykonywania powierzonych mu zadań. Porozumienie administracyjne zawarte w 2004 roku z Komisją, Parlamentem i Radą zostało przedłużone na kolejne trzy lata. Powierzchnia biurowa została powiększona i obecnie biura zajmują jeszcze jedną kondygnację. Komitet personelu bierze czynny udział w dyskusjach.

## 1.3. Cele na 2007 rok

Na 2007 rok wybrano następujące główne cele. Wyniki osiągnięte w trakcie ich realizacji zostaną przedstawione w sprawozdaniu w przyszłym roku.

- **Rozmiar sieci DPO**

Sieć urzędników ds. ochrony danych powinna osiągnąć stan docelowy i objąć działaniami wszystkie instytucje i organy. EIOD nadal będzie udzielać silnego wsparcia rozwojowi funkcji DPO i ukierunkowywać ten rozwój, będzie również zachęcać do wymiany najlepszych praktyk.

- **Kontynuacja kontroli wstępnych**

EIOD zamierza zakończyć kontrole wstępne istniejących operacji przetwarzania danych dla wszystkich stosownych kategorii. Szczególna uwaga zostanie zwrócona na systemy międzyinstytucjonalne i inne sytuacje, w których instytucje i organy wspólnie korzystają z określonych zasobów, z myślą o usprawnieniu i uproszczeniu procedur. Wyniki kontroli wstępnych zostaną przekazane DPO i innym stosownym podmiotom.

- **Inspekcje i kontrole**

EIOD rozpocznie mierzenie postępów w wykonywaniu rozporządzenia (WE) nr 45/2001, czemu będą towarzyszyć różnego rodzaju kontrole we wszystkich instytucjach i organach, w tym kontrole na miejscu, począwszy od wiosny 2007 roku. Uwaga zostanie zwrócona na powiadomienia i kontrole wstępne, a także na realizację zaleceń wynikających z wydanych uprzednio opinii w sprawach objętych kontrolą wstępną. EIOD opracuje również i opublikuje bardziej ogólną strategię dotyczącą kontroli.

- **Nadzór wideo**

EIOD opracuje i wyda wytyczne dotyczące nadzoru wideo prowadzonego przez instytucje i organy, z uwzględnieniem ewentualnego wpływu na prywatność personelu i gości. Wytyczne te obejmować będą wykorzystanie nadzoru wideo jako takiego oraz warunki procedur związanych z nadzorem wideo zgodnych z zasadami poszanowania prywatności.

- **Zagadnienia horyzontalne**

Opinie na temat kontroli wstępnych i decyzje w sprawie skarg dotyczyły wielu kwestii wspólnych, równie użyteczne dla instytucji i organów innych niż te, których dane sprawy dotyczą. EIOD opracuje dokumenty dotyczące takich zagadnień horyzontalnych i udostępni je powszechnie jako wytyczne dla wszystkich instytucji i organów.

- **Konsultacje w sprawie prawodawstwa**

EIOD nadal będzie wydawał opinie na temat wniosków dotyczących nowego prawodawstwa i zapewniał odpowiedni monitoring. Ta doradcza funkcja obejmie szerszy zakres tematyczny, a jej podstawą będzie systematyczny spis i wybór stosownych tematów i priorytetów. Szczególna uwaga zostanie zwrócona na odnośne wnioski dotyczące decyzji wykonawczych.

- **Ochrona danych w trzecim filarze**

EIOD nadal będzie zwracał szczególną uwagę na opracowanie i terminowe przyjęcie ogólnych ram ochrony danych w trzecim filarze. Będzie również uważnie obserwował wnioski dotyczące wymiany danych osobowych między poszczególnymi państwami lub zapewnienia dostępu do danych z sektora prywatnego lub publicznego do celów egzekwowania prawa.

- **Przekazywanie informacji na temat ochrony danych**

EIOD będzie udzielać silnego wsparcia działaniom podejmowanym w następstwie tzw. inicjatywy londyńskiej (zob. pkt 5.1), mającej na celu „przekazywanie informacji na temat ochrony danych i zwiększanie jej efektywności". Obejmuje to działania związane zarówno ze zwiększaniem świadomości, lepszym wykonaniem, jak i skutecznym egzekwowaniem zasad ochrony danych.

- **Regulamin wewnętrzny**

Korzystając z uzyskanej perspektywy i dotychczasowych doświadczeń, EIOD przyjmie i szeroko udostępni regulamin wewnętrzny obejmujący jego poszczególne funkcje i działania. Regulamin ten zostanie uzupełniony praktycznymi informacjami i narzędziami przeznaczonymi dla zainteresowanych stron, takich jak osoby rozważające złożenie skargi lub wniosku o poradę, a także instytucje lub organy podlegające kontroli.

- **Zarządzanie zasobami**

EIOD będzie w dalszym stopniu udoskonalać zarządzanie zasobami finansowymi i ludzkimi, w drodze odnowienia struktury budżetowej, przyjęcia wewnętrznych procedur w stosownych obszarach, takich jak ocena personelu, oraz opracowania polityki szkoleń. Różne udoskonalenia zostaną również wprowadzone w wewnętrznym środowisku biurowym, w tym w zakresie zarządzania pocztą elektroniczną i bezpieczeństwa informacji.

# 2. Nadzór

## 2.1. Wprowadzenie

Zadaniem Europejskiego Inspektora Ochrony Danych (EIOD) jest niezależny nadzór nad operacjami przetwarzania danych przeprowadzanymi przez instytucje lub organy wspólnotowe, które w całości lub częściowo wchodzą w zakres prawa wspólnotowego (z wyjątkiem Trybunału Sprawiedliwości działającego w ramach swych kompetencji sądowych). Rozporządzenie określa i przyznaje szereg obowiązków i uprawnień umożliwiających EIOD sprawowanie nadzoru.

Kontrole wstępne pozostały głównym aspektem nadzoru w 2006 roku. Zadanie to obejmuje analizę działań instytucji i organów w dziedzinach, które mogą stwarzać szczególne zagrożenia dla podmiotów danych, zgodnie z art. 27 rozporządzenia (WE) nr 45/2001. Jak wyjaśniono poniżej, kontrolowanie obecnie przeprowadzanych operacji przetwarzania danych, w połączeniu z planowanymi operacjami, zapewnia dokładny obraz przetwarzania danych osobowych w instytucjach i organach. Opinie EIOD umożliwiają administratorom danych dostosowywanie wykonywanych przez nich operacji przetwarzania danych do wytycznych EIOD, w szczególności w przypadkach, gdy nieprzestrzeganie zasad ochrony danych może stwarzać poważne zagrożenie dla praw osób fizycznych. EIOD dysponuje również innymi metodami, takimi jak rozpatrywanie skarg i zapytań.

Jeśli chodzi o uprawnienia nadane EIOD, jak dotąd nie wydano żadnego nakazu, ostrzeżenia ani zakazu. Dotychczas wyrażanie przez EIOD opinii w postaci zaleceń okazywało się wystarczające (zarówno w kontekście kontroli wstępnych, jak i skarg). Administratorzy danych wykonywali te zalecenia lub wyrażali zamiar ich wykonania i podejmowali niezbędne kroki. Szybkość reakcji różni się w poszczególnych przypadkach. EIOD opracował systematyczny monitoring wykonywania zaleceń.

## 2.2. Urzędnicy ds. ochrony danych

Rozporządzenie przewiduje, że należy wyznaczyć co najmniej jedną osobę jako urzędnika ds. ochrony danych (DPO) (art. 24 ust. 1). Niektóre instytucje wyznaczają również zastępcę DPO. Komisja wyznaczyła także DPO dla Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF, jedna z dyrekcji generalnych Komisji) oraz koordynatora ds. ochrony danych (DPC) w każdej z pozostałych dyrekcji generalnych w celu koordynowania wszystkich aspektów ochrony danych w danej dyrekcji.

Od kilku lat DPO spotykają się regularnie w celu wymiany doświadczeń i omawiania zagadnień horyzontalnych. Ta nieformalna sieć okazała się pożyteczna z punktu widzenia współpracy. Funkcjonowała ona także w 2006 roku.

**Zastępca inspektora Joaquín Bayo Delgado podczas zebrania z personelem.**

**EIOD na zebraniu urzędników ds. danych osobowych (DPO) w Lizbonie, Portugalia.**

EIOD uczestniczył w każdym z posiedzeń z udziałem DPO zorganizowanych w marcu (Trybunał Sprawiedliwości, Luksemburg), czerwcu (Europejskie Centrum Monitorowania Narkotyków i Narkomanii, Lizbona) i w październiku (EIOD, Bruksela). Posiedzenia te stanowiły dla EIOD dobrą sposobność do przekazania DPO aktualnych informacji na temat działań, które prowadzi, oraz do omówienia zagadnień będących przedmiotem zainteresowania obu stron. EIOD wykorzystał to forum do wyjaśnienia i omówienia procedury kontroli wstępnych oraz niektórych najważniejszych aspektów rozporządzenia, istotnych z punktu widzenia procedury przeprowadzania kontroli wstępnych (np. administrator danych, operacje przetwarzania danych). Forum to dało również EIOD okazję do nakreślenia postępów osiągniętych w dziedzinie spraw dotyczących kontroli wstępnych oraz do przekazania szczegółowych informacji na temat ustaleń będących wynikiem przeprowadzania kontroli wstępnych (zob. pkt 2.3 poniżej). W ten sposób współpraca pomiędzy EIOD a DPO w dalszym ciągu bardzo korzystnie się rozwijała.

Wraz z czerwcowym posiedzeniem w Lizbonie, z pomocą kilku doświadczonych DPO, EIOD zorganizował warsztaty dla nowych DPO. Przeanalizowano najważniejsze punkty rozporządzenia, koncentrując się w głównej mierze na kwestiach praktycznych mogących pomóc nowym DPO w wykonywaniu powierzonych im zadań.

W listopadzie 2006 roku rozpoczęło działalność nowe forum współpracy między EIOD a DPO: ustanowiono mianowicie grupę roboczą ds. terminów przechowywania danych, ds. blokowania i ds. usuwania danych. Zastępca EIOD, dwóch członków personelu oraz kilku DPO spotyka się regularnie w celu sporządzenia dokumentu, który będzie mógł stanowić praktyczny przewodnik po tych tematach dla administratorów danych i ekspertów IT.

W 2006 roku EIOD kładł nacisk na wynikający z przepisów prawa obowiązek wyznaczenia DPO przez wszystkie instytucje i organy, wskazał także kluczowe przesłania zawarte w wydanym przez siebie w 2005 roku dokumencie przedstawiającym stanowisko na temat DPO. W wyniku tych działań mianowano 7 nowych DPO ([3]). W tym kontekście należy przypomnieć, że samo mianowanie nie jest jeszcze wystarczające i nie oznacza automatycznie pełnej zgodności z przepisami rozporządzenia. DPO pracujący w niepełnym wymiarze godzin muszą poświęcić wystarczająco dużo czasu kwestiom ochrony danych, a wszyscy DPO muszą dysponować wystarczającymi zasobami, aby wykonywać swoje obowiązki. Muszą być oni również powiadamiani w bardziej właściwy sposób o przetwarzaniu danych osobowych w obrębie swojej instytucji lub organu, a w stosownych przypadkach oni z kolei muszą powiadomić EIOD o wszelkich operacjach przetwarzania danych, wiążących się ze szczególnym zagrożeniem dla osób, których te dane dotyczą, i które to operacje muszą w związku z tym zostać poddane kontroli wstępnej.

([3]) Nie licząc wakatów na istniejących stanowiskach, np. z powodu zmiany stanowiska.

## 2.3. Kontrole wstępne

### 2.3.1. Podstawa prawna

**Zasada ogólna: art. 27 ust. 1**

Artykuł 27 ust. 1 rozporządzenia przewiduje, że wszelkie „operacje przetwarzania, mogące ze swej natury przez swój zakres lub swoje cele stworzyć konkretne zagrożenia dla praw i wolności podmiotów danych" podlegają kontroli wstępnej przez EIOD. Artykuł 27 ust. 2 rozporządzenia zawiera wykaz operacji przetwarzania danych, które mogą stworzyć takie zagrożenia. Wykaz ten nie jest wyczerpujący. Inne niewymienione przypadki mogą stanowić szczególne zagrożenie dla praw i wolności podmiotów danych, uzasadniają zatem przeprowadzenie kontroli wstępnej przez EIOD. Na przykład każda operacja przetwarzania danych osobowych, która ma związek z zasadą poufności określoną w art. 36, wiąże się ze szczególnymi zagrożeniami, które uzasadniają przeprowadzenie kontroli wstępnej przez EIOD. Kolejnym kryterium, przyjętym w 2006 roku, jest obecność pewnych danych biometrycznych poza samymi zdjęciami, jako że charakter biometrii, możliwe powiązania i stan zaawansowania narzędzi technicznych mogą przynieść podmiotom danych nieoczekiwane lub niepożądane rezultaty.

**Przypadki wymienione w art. 27 ust. 2**

Artykuł 27 ust. 2 zawiera wykaz kilku operacji przetwarzania danych, które mogą stworzyć szczególne zagrożenia dla praw i wolności podmiotów danych:

a) *przetwarzanie danych odnoszących się do zdrowia i dotyczących podejrzeń o popełnienie przestępstwa, przestępstw, wyroków karnych lub środków bezpieczeństwa* („sûreté" w wersji francuskiej, tj. środki przyjęte w ramach postępowania prawnego);
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 do różnych celów nieuwzględnionymi w odpowiednim ustawodawstwie krajowym lub legislacji wspólnotowej;*
d) *operacje przetwarzania w celu pozbawienia jednostki prawa, świadczenia lub wyłączenia jej z umowy.*

Kryteria opracowane w poprzednich dwóch latach ([4]) nadal były stosowane przy interpretacji tego przepisu zarówno przy podejmowaniu decyzji, zgodnie z którą dane powiadomienie od DPO nie podlega kontroli wstępnej, jak i przy doradzaniu w sprawie konsultacji odnośnie do potrzeby przeprowadzenia kontroli wstępnej (zob. także pkt 2.3.6).

### 2.3.2. Procedura

**Powiadomienie/konsultacja**

EIOD musi przeprowadzać kontrole wstępne po otrzymaniu powiadomienia ze strony DPO.

**Termin, zawieszenie i przedłużenie**

EIOD musi wydać opinię w terminie dwóch miesięcy od otrzymania stosownego powiadomienia. W przypadku gdy EIOD zwraca się z wnioskiem o dostarczenie dalszych informacji, bieg tego dwumiesięcznego okresu ulega zwykle zawieszeniu do momentu uzyskania takich informacji przez EIOD. Taki okres zawieszenia obejmuje czas (zwykle 7 dni kalendarzowych), jaki DPO danej instytucji lub organu otrzymuje na przedstawienie uwag – i dalszych informacji w razie potrzeby – na temat projektu końcowego.

Jeśli wymaga tego złożony charakter sprawy, początkowy dwumiesięczny okres może również zostać przedłużony o kolejne dwa miesiące w drodze decyzji EIOD, o której należy poinformować administratora danych przed upływem początkowego dwumiesięcznego okresu. Jeżeli do końca dwumiesięcznego okresu lub jego przedłużenia nie zostanie wydana żadna decyzja, przyjmuje się, że opinia EIOD jest pozytywna. Jak dotąd, taka sytuacja nie miała miejsca.

**Rejestr**

Artykuł 27 ust. 5 rozporządzenia przewiduje, że EIOD musi prowadzić rejestr wszystkich operacji przetwarzania, o których został powiadomiony w celu przeprowadzenia kontroli wstępnej. Rejestr ten musi zawierać informacje, o których mowa w art. 25, i być ogólnodostępny.

([4]) Zob. sprawozdanie roczne za 2005 rok, pkt 2.3.1.

Podstawą takiego rejestru jest formularz powiadomienia wypełniany przez DPO i przesyłany EIOD. W ten sposób w możliwie największym stopniu zmniejsza się zapotrzebowanie na dalsze informacje.

Do celów przejrzystości wszystkie informacje są zawarte w publicznym rejestrze (z wyjątkiem środków bezpieczeństwa, które nie są wymieniane w rejestrze) i są ogólnodostępne.

Po wydaniu opinii przez EIOD jest ona podawana do wiadomości publicznej. Następnie w skróconej formie przedstawiane są zmiany wprowadzone przez administratora danych w świetle opinii EIOD. W ten sposób realizowany jest dwojaki cel: z jednej strony informacje na temat danej operacji przetwarzania danych są stale uaktualniane, a z drugiej strony przestrzegana jest zasada przejrzystości.

Wszystkie te informacje będą udostępniane na nowej stronie internetowej EIOD wraz ze streszczeniem danej sprawy.

**Opinie**

Zgodnie z art. 27 ust. 4 rozporządzenia końcowe stanowisko EIOD przyjmuje postać opinii, o której należy powiadomić administratora danej operacji przetwarzania oraz DPO zainteresowanej instytucji lub organu.

Struktura opinii jest następująca: opis postępowania, zwięzłe przedstawienie stanu faktycznego, analiza prawna, wnioski.

Analiza prawna rozpoczyna się od zbadania, czy dana sprawa faktycznie kwalifikuje się do przeprowadzenia kontroli wstępnej. Jak wspomniano powyżej, jeżeli dana sprawa nie mieści się w zakresie spraw wymienionych w art. 27 ust. 2, EIOD ocenia szczególne zagrożenie dla praw i wolności podmiotu danych. Kiedy dana sprawa zostanie zakwalifikowana do przeprowadzenia kontroli wstępnej, zasadniczym punktem analizy prawnej jest zbadanie, czy dana operacja przetwarzania jest zgodna ze stosownymi przepisami rozporządzenia. W razie potrzeby wydawane są zalecenia służące zapewnieniu przestrzegania przepisów rozporządzenia. We wnioskach EIOD zwykle stwierdzał do tej pory, że przetwarzanie nie wydaje się powodować naruszenia żadnego przepisu rozporządzenia, pod warunkiem uwzględnienia wydanych zaleceń. W dwóch opiniach wydanych w 2006 roku (2006-301 i 2006-142) wnioski były odmienne: operacje przetwarzania stanowiły naruszenie przepisów rozporządzenia i należało wykonać pewne zalecenia, aby odpowiednio dostosować te operacje.

Opracowano podręcznik rozpatrywania spraw, aby zagwarantować, podobnie jak w innych obszarach, że cały zespół pracuje na takiej samej podstawie oraz że opinie EIOD są przyjmowane po kompletnej analizie wszystkich istotnych informacji. Na podstawie zgromadzonych doświadczeń praktycznych nadaje on opiniom strukturę i jest stale aktualizowany. Zawiera on również listę kontrolną.

Istnieje także system przepływu pracy, który ma zapewnić wykonywanie wszystkich zaleceń w danej sprawie, a w stosownych przypadkach – przestrzeganie wszystkich decyzji wykonawczych (zob. pkt 2.3.7).

### 2.3.3. Analiza ilościowa

**Rozróżnienie spraw *ex post* i właściwych spraw dotyczących kontroli wstępnej**

Rozporządzenie weszło w życie 1 lutego 2001 roku. Artykuł 50 przewiduje, że instytucje i organy wspólnotowe musiały dopilnować, aby operacje przetwarzania będące wówczas w toku zostały doprowadzone do zgodności z rozporządzeniem w terminie roku od tej daty (tj. do 1 lutego 2002 roku). Mianowanie EIOD i jego zastępcy nabrało mocy 17 stycznia 2004 roku.

Kontrole wstępne dotyczą nie tylko operacji, które jeszcze się nie rozpoczęły („właściwe" kontrole wstępne), ale także operacji przetwarzania, które rozpoczęły się przed 17 stycznia 2004 roku lub przed wejściem rozporządzenia w życie (kontrole wstępne *ex post*). W takich sytuacjach kontrola na mocy art. 27 nie mogłaby mieć charakteru „wstępnego" w ścisłym tego słowa znaczeniu, ale należy ją potraktować na zasadzie *ex post.* Przyjmując takie pragmatyczne podejście, EIOD ma pewność, że w obszarze operacji przetwarzania stwarzających szczególne zagrożenia art. 50 rozporządzenia jest przestrzegany.

Aby rozwiązać problem zaległych spraw mogących podlegać kontroli wstępnej, EIOD zwrócił się do DPO o przeanalizowanie sytuacji w ich odnośnych instytucjach w zakresie operacji przetwarzania objętych art. 27. Po otrzymaniu informacji od wszystkich DPO sporządzono, a następnie poprawiono wykaz spraw podlegających kontroli wstępnej.

W wyniku tego spisu określono pewne kategorie występujące w większości instytucji i organów, a w związku z tym uznano, że powinny być one przedmiotem bardziej systematycznego nadzoru. Aby umożliwić najbardziej efektywne wykorzystanie dostępnych zasobów ludzkich, EIOD określił priorytety pracy nad sprawami dotyczącymi kontroli wstępnej *ex post,* ustalając następujące kategorie priorytetowe:

1) akta medyczne (zarówno *sensu stricto,* jak i akta zawierające dane dotyczące zdrowia)
2) ocena personelu (w tym również przyszłego personelu [rekrutacja])
3) postępowania dyscyplinarne
4) usługi socjalne
5) e-monitoring

**Powyższe kryteria dotyczące priorytetów mają zastosowanie wyłącznie do spraw *ex post***, ponieważ właściwe sprawy dotyczące kontroli wstępnej muszą być rozpatrywane przed wykonaniem danej operacji przetwarzania, zgodnie z planami stosownej instytucji lub organu.

**Opinie na temat spraw dotyczących kontroli wstępnej wydane w 2006 roku**

W 2006 roku wydano **54 opinie** ([5]) dotyczące powiadomień o przeprowadzeniu kontroli wstępnej.

| | |
|---|---|
| Rada | 13 spraw (12 opinii)) |
| Komisja | 12 spraw |
| Europejski Bank Centralny | 5 spraw (4 opinie) |
| Trybunał Sprawiedliwości | 5 spraw |
| Europejski Bank Inwestycyjny | 5 spraw |
| Parlament | 4 sprawy (3 opinie) |
| CdT ([6]) | 3 sprawy |
| EPSO ([7]) | 3 sprawy |
| Trybunał Obrachunkowy | 2 sprawy |
| Komitet Regionów | 1 sprawa |
| Europejski Komitet Ekonomiczno-Społeczny | 1 sprawa |
| EUMC ([8]) | 1 sprawa |
| OHIM ([9]) | 1 sprawa |
| OLAF ([10]) | 1 sprawa |

Tych 57 spraw stanowi wzrost o 67,6% w porównaniu z liczbą przeprowadzanych kontroli wstępnych w 2005 roku. Obciążenie pracą niewątpliwie wzrośnie w 2007 roku (zob. poniżej).

([5]) EIOD otrzymał 57 powiadomień, ale z przyczyn praktycznych oraz z uwagi na fakt, że niektóre sprawy były powiązane z tymi samymi celami, 6 powiadomień (2 z EBC, 2 z Rady i 2 z Parlamentu) zostało rozpatrzonych wspólnie. Dlatego wydano 54 opinie, choć otrzymano 57 powiadomień.
([6]) Centrum Tłumaczeń dla Organów Unii Europejskiej.
([7]) Europejskie Biuro Doboru Kadr (wchodzące w zakres działalności DPO Komisji).
([8]) Europejskie Centrum Monitorowania Rasizmu i Ksenofobii.
([9]) Urząd Harmonizacji w ramach Rynku Wewnętrznego.
([10]) Europejski Urząd ds. Zwalczania Nadużyć Finansowych.

Z tych 57 spraw dotyczących kontroli wstępnej (54 opinie) tylko 5 to właściwe sprawy dotyczące kontroli wstępnej, tzn. zainteresowane instytucje (Trybunał Obrachunkowy w jednym przypadku, Komisja w trzech i Parlament w jednym) zastosowały procedurę obowiązującą w razie przeprowadzania kontroli wstępnych przed wykonaniem operacji przetwarzania. Dwie z tych pięciu spraw dotyczących kontroli wstępnej były związane z oceną, jedna z e-monitoringiem, a dwie z innymi tematami, takimi jak wspólne korzystanie on-line z bazy danych przez delegacje europejskie w Chinach lub niezależność podmiotów finansowych. Pozostałe 52 sprawy to sprawy dotyczące kontroli wstępnej *ex post.*

Poza wspomnianymi 57 sprawami dotyczącymi kontroli wstępnej, w związku z którymi wydana została opinia, EIOD zajmował się również 9 sprawami, które uznano za niepodlegające kontroli wstępnej. Pięć powiadomień pochodziło z Komisji, jedno z Komitetu Ekonomiczno-Społecznego (EKES) i Komitetu Regionów (KR) (które wspólnie korzystają z niektórych elementów infrastruktury), jedno z Europejskiego Centrum Monitorowania Rasizmu i Ksenofobii (EUMC), a dwa z Parlamentu – wszystkie dotyczyły rozmaitych spraw, takich jak na przykład służba audytu wewnętrznego (IAS), e-głosowanie lub Służba Audytu Wewnętrznego (w Komisji), zarządzanie kontami użytkowników, standardy korzystania z systemów i usług IT (EUMC) oraz uproszczenia (Parlament). Zob. również pkt 2.3.6.

**Analiza według instytucji/organu**

Większość instytucji i organów powiadamiała o operacjach przetwarzania mogących stwarzać szczególne zagrożenie. EIOD określił wiosnę 2007 roku jako termin nadsyłania wszystkich powiadomień dotyczących przeprowadzania kontroli wstępnych *ex post.*

Agencje zasługują na szczególny komentarz. W 2005 roku tylko jedna agencja (OHIM) przekazała powiadomienie o kilku przypadkach. EIOD założył, że wiele innych agencji powiadomi w bliskiej przyszłości o operacjach przetwarzania danych, tak się jednak nie stało. Tylko dwie inne agencje przesłały powiadomienia o operacjach przetwarzania, EUMC i centrum tłumaczeń, to ostatnie przesłało dwa powiadomienia dotyczące oceny i jedno dotyczące zwolnień lekarskich. EIOD faktycznie oczekuje większej liczby powiadomień ze strony agencji, jako że niektóre z nich, nowo ustanowione, już zapowiedziały przesłanie swoich własnych spisów i powiadomień; dotyczy to między innymi EMEA ([11]) i EMCDDA ([12]). Niektóre inne agencje zaczęły już powiadamiać o operacjach przetwarzania danych; związane z tym opinie zostaną wydane w 2007 roku (zob. poniżej podpunkt *Powiadomienia dotyczące przeprowadzenia kontroli wstępnych otrzymane przed 1 stycznia 2007 roku i będące w toku*).

**Analiza według kategorii**

Liczba rozpatrywanych spraw dotyczących kontroli wstępnej, według kategorii priorytetów, przedstawia się następująco:

| | |
|---|---|
| Kategoria pierwsza (akta medyczne) | 14 spraw |
| Kategoria druga (ocena personelu) | 23 sprawy |
| Kategoria trzecia (postępowania dyscyplinarne) | 4 sprawy |
| Kategoria czwarta (usługi socjalne) | 2 sprawy |
| Kategoria piąta (e-monitoring) | 5 spraw |
| Inne obszary | 9 spraw |

Kategoria pierwsza obejmuje akta medyczne jako takie oraz ich różnoraką zawartość (11 spraw dotyczących kontroli wstępnej), a także wszystkie procedury związane ze świadczeniami lub systemami ubezpieczeń zdrowotnych (3 sprawy dotyczące kontroli wstępnej). Odsetek spraw w tej kategorii pozostaje na niemal niezmienionym poziomie (26,5% spraw w 2005 roku, 24,6% spraw w 2006 roku), jednak liczba spraw znacznie wzrosła, co dowodzi, że instytucje i organy mają świadomość potrzeby kontroli wstępnej.

Kategoria druga, dotycząca oceny personelu (23 sprawy z 57), pozostaje najliczniejsza, chociaż odsetek spada (56% spraw w 2005 roku, 40,4% w 2006 roku). Ocena dotyczy wszystkich członków personelu Wspólnoty Europejskiej, w tym urzędników, personelu zatrudnionego na czas określony i personelu kontraktowego, łącznie z procedurami rekrutacji. Powiadomienia dotyczyły nie tylko procedur doboru kadr i oceny, ale także procedur certyfikacji i akredytacji. Należy dodać, że te 23 sprawy obejmują 3 istotne powiadomienia od EPSO (dotyczące, odpowiednio, rekrutacji

([11]) Europejska Agencja Leków.
([12]) Europejskie Centrum Monitorowania Narkotyków i Narkomanii.

urzędników, personelu zatrudnionego na czas określony i personelu kontraktowego), które są związane z systemem rekrutacji ustanowionym dla wszystkich instytucji UE.

Odnośnie do kategorii trzeciej (postępowania dyscyplinarne), przesłane zostały tylko 4 sprawy: przez EBC ([13]), ETS ([14]) i Radę. Wszystkie tzw. duże instytucje dopełniły obowiązku w odniesieniu do tej kategorii, z wyjątkiem EKES i KR. Niektóre agencje, takie jak OHIM i EMCDDA, zapowiedziały przesłanie tych powiadomień.

W odniesieniu do kategorii czwartej (usługi socjalne) przesłano zaledwie 2 sprawy dotyczące Rady i Komisji. Te dwa powiadomienia były bardzo dobrze opracowane i udokumentowane. Otrzymano już powiadomienia w tej kategorii od Parlamentu i Trybunału Sprawiedliwości, ale stosowne opinie EIOD zostaną wydane w 2007 roku. Spodziewane są oczywiście inne powiadomienia.

Kategoria piąta (e-monitoring) stanowiła jeden z głównych aspektów pracy EIOD w 2006 roku. Po wszechstronnym badaniu w instytucjach i organach wkrótce zostanie opublikowany dokument, zostanie również zorganizowane specjalne seminarium poświęcone tej kwestii. Tymczasem przeprowadzono wyłącznie właściwe kontrole wstępne. Instytucje przesłały już powiadomienia dotyczące pięciu dossier (Komisja [2], EBC, EBI i Rada). Wiele innych jest już zaplanowanych na 2007 rok.

Jeśli chodzi o powiadomienia dotyczące spraw *ex post,* które nie należą do powyższych kategorii priorytetów, można je podzielić na dwie grupy. Niektóre z nich są związane ze sprawami finansowymi, takimi jak zespół ds. nieprawidłowości finansowych (PIF – Komisja), system wczesnego ostrzegania (Komisja i Trybunał Sprawiedliwości), zaproszenie do składania ofert (Komitet Regionów), procedura udzielania zamówień (Trybunał Sprawiedliwości) oraz niezależność podmiotów finansowych (Parlament). Pozostałe są rozmaite, dotyczą umowy w sprawie turystyki pomiędzy UE a Chinami (Komisja), udziału w strajku (Komisja) czy dochodzeń wewnętrznych (OLAF). Te różne powiadomienia umożliwiły EIOD ustalenie kryteriów w bardzo sensytywnych obszarach, takich jak system wczesnego ostrzegania i wewnętrzne dochodzenia OLAF (zob. pkt 2.3.4).

([13]) Europejski Bank Centralny.
([14]) Europejski Trybunał Sprawiedliwości.

**Działalność EIOD oraz instytucji i organów**

Dwa wykresy znajdujące się w załączniku E obrazują działalność EIOD oraz instytucji i organów. Szczegółowo przedstawiają one liczbę dni roboczych EIOD, liczbę dni dodatkowych wymaganych przez EIOD oraz liczbę dni zawieszenia biegu terminu.

*Liczba dni roboczych EIOD przypadających na jedną kontrolę wstępną* wzrosła o zaledwie 4,4%, co stanowi 2,5 dnia więcej niż w 2005 roku (55,5 dnia w 2005 roku i 57,9 w 2006 roku). Jest to nadal liczba zadowalająca, biorąc pod uwagę coraz bardziej złożony charakter powiadomień przesyłanych EIOD.

*Liczba dni dodatkowych dla EIOD* wzrosła o 62,6 %, ale w ujęciu bezwzględnym stanowi to zaledwie 2 dni więcej niż w 2005 roku (3,3 dnia w 2005 roku i 5,4 dnia w 2006 roku). Wynika to głównie ze złożonego charakteru 3 konkretnych spraw: dossier na temat wewnętrznych dochodzeń OLAF, dossier na temat systemu wczesnego ostrzegania w Komisji (wraz z istotnymi zmianami w okresie, kiedy EIOD przygotowywał swoją opinię) oraz dossier dotyczące rekrutacji personelu kontraktowego przez EPSO (wraz z dużą nową bazą danych tworzoną również w trakcie działań EIOD). W dwóch pierwszych przypadkach niezbędne było specjalne spotkanie z administratorem danych i DPO.

*Liczba dni zawieszenia biegu terminu*: od połowy 2006 roku obejmuje ona zawieszenie na 7 lub 10 dni przeznaczone na uwagi i dalsze informacje od DPO na temat końcowego projektu. Wzrost między 2005 rokiem (średnio 29,8 dni na dossier) a 2006 rokiem (średnio 72,8 dni na dossier) wynosi 144,1%. Obejmuje to bardzo odmienne sytuacje. EIOD musi niestety podkreślić, że trzy powyższe dossier zostały zawieszone na bardzo długie okresy wynoszące, odpowiednio, 236, 258 i 276 dni.

Nawet jeśli pewne okoliczności mogą uzasadniać tego rodzaju opóźnienie, EIOD wyraża ubolewanie z powodu tych danych liczbowych. Instytucje i organy powinny dołożyć starań, aby skrócić okres niezbędny do przesłania informacji. W każdym razie EIOD ponownie przypomina instytucjom i organom, że mają one obowiązek współpracować z EIOD i przekazywać mu żądane informacje, zgodnie z art. 30 rozporządzenia.

*Średnia liczba według instytucji*: wykresy wskazują, że wiele instytucji i organów bardzo znacznie zwiększyło liczbę dni zawieszenia biegu terminu; niektóre z nich w mniejszym stopniu, czego przykładem może być Rada. EIOD chciałby nadmienić, że Komisja i Trybunał Obrachunkowy zmniejszyły liczbę dni zawieszenia biegu terminu w swoich instytucjach (odpowiednio o 39,3% i 45,2%). Należy mieć nadzieję, że pozostałe instytucje i organy podążą w tym samym kierunku.

**Powiadomienia dotyczące przeprowadzenia kontroli wstępnej otrzymane przed 1 stycznia 2007 roku i będące w toku**

W roku 2007 EIOD spodziewa się wielu powiadomień, jako że instytucje i organy będą dążyć do dotrzymania terminu określonego jako „wiosna 2007 roku". Do końca 2006 roku w toku znajdowało się już **26 spraw dotyczących kontroli wstępnej.** Spośród tych spraw jedno powiadomienie zostało przesłane w 2005 roku, a 25 w 2006 roku (z czego 9 w grudniu), w przypadku 11 spraw powiadomienia przesłano zaś w styczniu 2007 roku. Dwa z nich uznano za niepodlegające przeprowadzeniu kontroli wstępnej. Jedna z tych spraw to prawdziwa sprawa dotycząca kontroli wstępnej („Niekompetencja", powiadomienie przesłane przez Trybunał Obrachunkowy, opinia już została wydana 18 stycznia 2007 roku).

| | |
|---|---|
| OLAF | 5 spraw |
| Parlament | 4 sprawy |
| Komisja Europejska | 3 sprawy |
| Europejski Bank Centralny | 3 sprawy |
| EKES i KR | 2 sprawy |
| Europejski Bank Inwestycyjny | 2 sprawy |
| Trybunał Obrachunkowy | 1 sprawa |
| CPVO ([15]) | 1 sprawa |
| Europejski Trybunał Sprawiedliwości | 1 sprawa |
| EFSA ([16]) | 1 sprawa |
| EPSO | 1 sprawa |
| ETF ([17]) | 1 sprawa |
| Centrum Tłumaczeń (CdT) | 1 sprawa |

([15]) Wspólnotowy Urząd Odmian Roślin.
([16]) Europejski Urząd ds. Bezpieczeństwa Żywności.
([17]) Europejska Fundacja Kształcenia.

**Analiza według instytucji i organu**

EIOD z zadowoleniem przyjmuje fakt, że cztery agencje (CdT, ETF, EFSA i CPVO) zaczęły przesyłać swoje powiadomienia i zachęca do tego pozostałe agencje i organy. Szczególny przypadek OLAF opisano poniżej.

**Analiza według kategorii**

Liczba będących przedmiotem powiadomienia spraw dotyczących kontroli wstępnej, według kategorii priorytetów, przedstawia się następująco:

| | |
|---|---|
| Kategoria pierwsza (akta medyczne) | 4 sprawy |
| Kategoria druga (ocena personelu) | 8 spraw |
| Kategoria trzecia (postępowania dyscyplinarne) | 0 spraw |
| Kategoria czwarta (usługi socjalne) | 2 sprawy |
| Kategoria piąta (e-monitoring) | 6 spraw |
| Inne obszary | 6 spraw ([18]) |

W kategorii pierwszej przesyłanie powiadomień ma charakter ciągły. Spośród nich EIOD otrzymał (od trzech instytucji) powiadomienie dotyczące akt medycznych *sensu stricto,* tj. akt prowadzonych przez służby medyczne. Oczekuje się, że w 2007 roku będzie podobnie, ponieważ wiele procedur obejmuje akta medyczne. EIOD z zadowoleniem przyjmuje fakt, że od początku 2007 roku Komisja ([19]) przesyła powiadomienia w tej dziedzinie. Tak samo powinno postąpić biuro PMO ([20]), o czym już mu przypominano (zob. pkt 2.4.2).

([18]) Związane z zaproszeniami do składania ofert (Komisja) oraz 5 powiadomień od OLAF dotyczących następczych działań natury administracyjnej, finansowej, sądowej i dyscyplinarnej, a także spraw z zakresu monitorowania.
([19]) Odgrywa ona międzyinstytucjonalną rolę w szczególnych aspektach (np. archiwizacji akt medycznych).
([20]) Biuro Administrowania i Rozliczania Należności Indywidualnych.

Druga kategoria tematyczna (ocena personelu) nadal stanowi większość przypadków – 8 z 26 dossier (30,8%). W tym obszarze powiadomienia obejmowały poważne przypadki (sprawy EPSO – zob. powyżej), które dotyczą wszystkich instytucji i organów, jednak EIOD chciałby podkreślić, że niektóre instytucje nie przesłały powiadomień na temat stosowanych przez siebie procedur dotyczących wykorzystania list rezerwowych EPSO.

W odniesieniu do trzeciej kategorii (postępowania dyscyplinarne), EIOD oczekuje powiadomień od instytucji, w szczególności od agencji i obu komitetów.

Jeśli chodzi o kategorię czwartą (usługi socjalne), otrzymano już 2 powiadomienia (jedno od Parlamentu i jedno od Trybunału Sprawiedliwości).

Kategoria piąta (e-monitoring) nadal ma szczególne znaczenie. Jak wspomniano powyżej, dokument dotyczący e-monitoringu wykorzystuje się jako podstawę do przeprowadzania kontroli wstępnej systemów e-monitoringu, służy on także do celów przeprowadzania kontroli wstępnej w tej dziedzinie (zob. pkt 2.7). Ta dziedzina dotyczy wielu instytucji i organów; w tym kontekście wydano już sześć opinii: dla Komisji, EBC (dwie), EBI (dwie) i dla Rady. EKES i KR przesłały powiadomienia o tego rodzaju procedurach. EBC i EBI powiadomiły o innych operacjach przetwarzania w tej kategorii.

Kolejny obszar obejmuje w szczególności OLAF, który powiadamia o wielu sprawach dotyczących kontroli wstępnej z uwagi na szczególny i sensytywny charakter prowadzonych przez siebie działań. Powiadomienia te były pierwszą konsekwencją wspólnej analizy i planowania dokonanych przez DPO OLAF i zespół EIOD w celu umożliwienia pracy bez zakłóceń. Liczba przesyłanych powiadomień będzie nadal rosła. OLAF już w styczniu 2007 roku przekazał 7 powiadomień odnoszących się do spraw dotyczących kontroli wstępnej, a kolejnych 20 spodziewano się przed 1 marca 2007 roku.

### 2.3.4. Główne zagadnienia w sprawach dotyczących kontroli *ex post*

*Dane medyczne i inne dane dotyczące zdrowia* są przetwarzane przez instytucje i organy. Niniejszą kategorią są objęte wszelkie dane dotyczące bezpośredniej lub pośredniej wiedzy na temat stanu zdrowia danej osoby. W związku z tym zwolnienia lekarskie i roszczenia związane z systemem ubezpieczeń zdrowotnych podlegają przeprowadzeniu kontroli wstępnej.

Jak już wspomniano wcześniej, EIOD nadzorował 11 spraw dotyczących kontroli wstępnej bezpośrednio związanych z samymi aktami medycznymi oraz różnymi ich aspektami. Rada przesłała same akta medyczne do celów przeprowadzenia kontroli wstępnej. EIOD wydał liczne zalecenia, w szczególności dotyczące jakości danych, zatrzymywania danych i informacji przekazywanych podmiotowi danych.

Biorąc pod uwagę wszystkie sprawy dotyczące kontroli wstępnej (Rada, EBC i EBI), a także pozostające w toku sprawy na ten sam temat (Parlament, EKES i KR), EIOD ma dobry przegląd sytuacji.

*Ocena personelu* to – z oczywistych powodów – często wykonywana we wszystkich instytucjach i organach operacja przetwarzania. Jedną z głównych ról w tej dziedzinie odgrywa EPSO. EIOD otrzymał powiadomienia dotyczące rekrutacji urzędników, personelu zatrudnianego na czas określony i personelu kontraktowego. We wszystkich tych przypadkach EPSO w dużej mierze przestrzegało zasad rozporządzenia, choć EIOD wydał kilka zaleceń dotyczących okresu zatrzymywania danych, długotrwałego przechowywania danych oraz ograniczenia ich przekazywania wyłącznie do służb odpowiedzialnych za rekrutację. Szczególne zalecenie odnosiło się do potrzeby publikowania, jako ogólnej zasady, warunków konkursów, w szczególności dziedzin podlegających ocenie na egzaminach ustnych i ich szczegółowych ocen, a także stosownego prawa dostępu dla kandydatów. W odniesieniu do rekrutacji personelu kontraktowego, pośród innych zaleceń, EIOD wskazał na potrzebę niestosowania ograniczeń dotyczących prawa dostępu do wyników lub zniesienia podziału na grupy według wyników na listach laureatów konkursów, z których mają korzystać rekrutujące instytucje. EIOD skierował również zalecenia dotyczące okresu przechowywania danych w formacie elektronicznym.

Kolejną istotną sprawą dotyczącą kontroli wstępnej była sprawa życiorysu europejskiego (EU-CV) on-line (nie mylić z Sysper 2 e-CV; zob. główne zagadnienia właściwych kontroli wstępnych poniżej), który zastępuje obecną ręczną lub na wpół ręczną procedurę rozpatrywania tzw. spontanicznych aplikacji na wakaty Komisji zharmonizowanym systemem elektronicznym, względem którego EIOD wydał kilka zaleceń odnoszących się do okresów przechowywania danych, wykorzystywania zapasowych kopii danych oraz zgody osób wystawiających referencje podanych w CV.

Instytucje, takie jak CdT, EKES, ETS, EUMC, EBI i EBC, przesłały informacje dotyczące dokonywanych przez nie operacji przetwarzania danych związanych z rekrutacją lub oceną. Główne zalecenia dotyczą jakości danych, prawa dostępu, przekazywanych informacji oraz zatrzymywania danych. Zarówno Rada, jak i Trybunał Obrachunkowy przesłały także EIOD informacje związane z nowymi obszarami, jakimi są procedura certyfikacji i procedura akredytacji (jedna z nich została potraktowana jako prawdziwa sprawa dotycząca kontroli wstępnej – zob. poniżej); główne zalecenia dotyczą zatrzymywania danych oraz prawa do informacji. Procedura certyfikacji z EPSO jest w toku.

Wreszcie, dwie kontrole wstępne odnoszą się do zarządzania czasem (Rada i EBI). W innych obszarach zalecenia dotyczą okresu przechowywania danych, definicji dostępu kierowników do danych osobowych podlegających im członków personelu oraz informacji przekazywanych podmiotowi danych.

Administracyjne postępowania wyjaśniające i postępowania dyscyplinarne: w tym obszarze rozpatrzono 4 sprawy kontroli *ex post.* Dotyczyły one Rady, EBC (po jednej sprawie w każdym obszarze) oraz Trybunału Sprawiedliwości. Wydane zostały zalecenia odnoszące się do zatrzymywania danych, które pozostaje jednym z głównych zagadnień (zasada ograniczonego przechowywania a zasada nakładania sankcji), do prawa dostępu, sprostowania i informacji, a także do przetwarzania szczególnych kategorii danych.

*Usługi socjalne*: dossier dotyczące usług socjalnych może obejmować szczegółowe informacje związane ze zdrowiem urzędnika, co uzależnia przetwarzanie danych od wstępnej kontroli przez EIOD. Ponadto przetwarzanie danych przez służbę opieki społecznej może mieć na celu ocenę aspektów osobowych dotyczących podmiotów danych.

Przeanalizowano tylko 2 sprawy dotyczące kontroli wstępnej. Zalecenia dla Komisji koncentrowały się na najwyższej ostrożności niezbędnej we wszystkich kontaktach ze służbami zewnętrznymi obejmujących dane osobowe. Ponadto EIOD zaapelował, by przy opracowywaniu statystyk dotyczących pomocy finansowej zachować anonimowość danych; wezwał również do opieczętowywania wszystkich listów wyrazami „Staff matter" (sprawy pracownicze), mając na uwadze, że są to dane poufne i wrażliwe. Zalecenia dla Rady dotyczyły jakości danych, prawa dostępu i prawa do sprostowania oraz przekazywanych informacji.

*E-monitoring*: w 2006 roku, w oczekiwaniu na ogólne wnioski zawarte w dokumencie na temat e-monitoringu (zob. pkt 2.8), sprawy dotyczące kontroli *ex post* w tej dziedzinie odnosiły się do nagrywania rozmów telefonicznych. Zagadnienie to stwarza szczególne problemy, które są tak istotne, że w rozporządzeniu (WE) nr 45/2001 przewidziano odrębny przepis i szczególne zabezpieczenia, zwłaszcza w zakresie poufności komunikacji. Jako że nagrania są w głównej mierze wykorzystywane do identyfikowania przypadków naruszenia tajemnicy zawodowej lub niewłaściwego wykorzystania informacji poufnych, a także do identyfikowania oszustw, istnieją dalsze podstawy do przeprowadzenia kontroli wstępnej.

W przypadku alarmowych i awaryjnych linii telefonicznych Rady zalecenia dotyczą ograniczenia celu, ograniczenia prawa dostępu podmiotu danych i informacji przekazywanych osobom telefonującym z zewnątrz. Dla EBC i EBI zalecenia skupiły się zasadniczo wokół obowiązku przekazywania informacji stronom transakcji, których dane są również rejestrowane. EIOD podkreślił także znaczenie definiowania celów, do których dane są początkowo gromadzone, i dopilnowania, aby nie były one później przetwarzane do innych, niezgodnych z pierwotnymi celów. W przypadku alarmowych i awaryjnych linii telefonicznych Komisji zalecenia dotyczyły zasadniczo informacji przekazywanych podmiotom danych.

Obszar ten pozostanie istotny, jako że 6 spraw dotyczących kontroli wstępnej już oczekuje na rozpatrzenie w 2007 roku.

*Inne obszary*: należy podkreślić system wczesnego ostrzegania (EWS) i wewnętrzne dochodzenia OLAF.

System EWS był przedmiotem powiadomienia ze strony Komisji i Trybunału Sprawiedliwości. Zasadniczym celem EWS jest zapewnienie obiegu poufnych informacji dotyczących stron trzecich (osób fizycznych lub prawnych) we wszystkich departamentach Komisji na temat odbiorców wspólnotowych środków finansowych (beneficjentów), którzy dopuścili się oszustwa, popełnili błędy lub nieprawidłowości administracyjne, a także na temat innych okoliczności związanych z beneficjentami, którzy mogliby stwarzać zagrożenie dla interesów finansowych Wspólnot. Informacje mogą również obejmować osoby fizyczne posiadające uprawnienia do reprezentowania, podejmowania decyzji lub nadzorowania danych osób prawnych. Inne instytucje nie ustanawiają własnych centralnych baz danych, ale wykorzystują bazę danych Komisji do wymiany informacji z tą ostatnią (sprawa Trybunału Sprawiedliwości).

Na temat systemu EWS Komisji wydana została opinia. Wydano pewne zalecenia odnoszące się do możliwości opublikowania decyzji Komisji dotyczącej EWS w Dzienniku Urzędowym, do jakości danych, zdefiniowania i przyznania praw dostępu (ograniczenie tego prawa powinno pozostać wyjątkiem), które należy uzupełnić prawem do sprostowania w przypadku błędów lub niewłaściwej oceny, informacji przekazywanych podmiotom danych oraz zalecenie mówiące, że – co do zasady – zainteresowana osoba jest informowana o wydaniu wobec niej ostrzeżenia. Jeśli chodzi o sprawę Trybunału Sprawiedliwości, główne zalecenia dotyczyły polityki zatrzymywania danych, jakości danych, prawa dostępu i prawa do sprostowania oraz przekazywanych informacji.

Aby zwalczać nieprawidłowości finansowe, takie jak oszustwa i korupcja, OLAF ma prawo prowadzić w instytucjach i organach UE wewnętrzne dochodzenia administracyjne. Prawo do prowadzenia dochodzeń obejmuje również poważne sprawy związane z wykroczeniami popełnianymi przez personel UE. OLAF ma dostęp do wszelkich informacji na wszelkich nośnikach danych, może też zażądać ustnych informacji od członków personelu itp. W razie potrzeby wyniki dochodzeń są przedkładane władzom krajowym lub wspólnotowym celem kontynuowania stosownych działań (np. sądowych lub dyscyplinarnych). EIOD wydał liczne zalecenia służące poprawie przestrzegania przepisów rozporządzenia, w szczególności odnoszące się do praw podmiotów danych, takich jak prawo dostępu, prawo do sprostowania i informacji. EIOD zajął się również kwestią gwarancji dotyczących jakości danych wprowadzanych do akt dochodzeniowych oraz poufności poczty elektronicznej, jak również przekazywania sprawozdań i dokumentów pokrewnych itp.

### 2.3.5. Główne zagadnienia we właściwych kontrolach wstępnych

EIOD powinien zwykle wydawać swoją opinię przed rozpoczęciem operacji przetwarzania, tak aby od początku zagwarantować prawa i wolności podmiotów danych. Taki jest cel art. 27. Równolegle z rozpatrywaniem spraw dotyczących kontroli wstępnej *ex post* w 2006 roku, EIOD otrzymał powiadomienia o pięciu sprawach dotyczących właściwej (21) kontroli wstępnej. W przeciwieństwie do ogólnego wniosku dotyczącego wszystkich spraw dotyczących właściwej kontroli wstępnej w 2005 roku, w 2006 roku właściwe kontrole wstępne były bardzo dobrze udokumentowane. Zgodnie z oczekiwaniami zasady proceduralne pozostają jednym z głównych aspektów powiadomień.

Sprawa dotycząca procedury akredytacji zgłoszona przez Trybunał Obrachunkowy odnosiła się do nowej procedury umożliwiającej członkom personelu zmianę grupy zaszeregowania (z dawnych grup C i D na grupę AST). Jedyne zalecenia służące udoskonaleniu systemu z punktu widzenia ochrony danych dotyczyły zatrzymywania danych i przekazywanych informacji.

Kolejna sprawa mająca związek z oceną dotyczyła systemu Sysper 2 e-CV w Komisji (nie mylić z europejskim życiorysem [EU-CV] on-line – zob. powyżej) będącego narzędziem informatycznym umożliwiającym personelowi Komisji wprowadzanie swych danych zawodowych. Główne zalecenia dotyczyły informacji przekazywanych członkom personelu, jak również ustanowienia gwarancji związanych z dostępem do danych w systemie.

Sprawa związana z e-monitoringiem dotyczyła nagrywania rozmów z helpdeskiem w Komisji. EIOD wydał liczne zalecenia koncentrujące się wokół dwóch głównych kwestii i służące uniknięciu niezgodności z prawem: rozmowy nagrywane w celu rozwiązania problemów informatycznych powinny być przecho-

(21) Tj. spraw dotyczących jeszcze niewykonanej operacji przetwarzania.

wywane przez bardzo krótki okres; dalsze wykorzystanie nagrań do celów szkoleniowych może być dopuszczalne wyłącznie wtedy, gdy rozmowy i związane z nimi dane będą poddane edycji w celu zapewnienia anonimowości rozmówców lub po uzyskaniu zgody użytkowników i operatorów.

Parlament przesłał powiadomienie na temat niezależności podmiotów finansowych. Tego rodzaju przetwarzanie odbywa się za pomocą kwestionariuszy oceny umożliwiających wykrycie ryzyka związanego z konfliktem interesów w wykonywaniu obowiązków o charakterze poufnym przez podmioty finansowe w Parlamencie i mogącego stanowić zagrożenie dla odnośnych interesów finansowych. Główne zalecenia odnosiły się do gwarancji ograniczenia celu i do przekazywanych informacji.

Niecodzienne powiadomienie zostało przesłane przez Komisję na temat statusu zatwierdzonego celu wyjazdów turystycznych (ADS) w ramach umowy w sprawie turystyki pomiędzy UE a Chinami. Chroniona strona sieciowa Dyrekcji Generalnej ds. Stosunków Zewnętrznych Komisji Europejskiej ułatwia wymianę informacji w czasie rzeczywistym między Komisją a ambasadami i konsulatami krajów europejskich (UE plus kilka innych) uczestniczących w umowie w sprawie turystyki z Chinami dotyczącej statusu ADS. Strona internetowa zawiera wykaz akredytowanych biur podróży i ich przedstawicieli (osób działających w ich imieniu) upoważnionych do zajmowania się wnioskami wizowymi ADS do krajów Unii Europejskiej. Zawiera ona sankcje proponowane i nakładane za pogwałcenie zasad ADS, ale także inne informacje. EIOD dokonał wstępnej kontroli systemu, ponieważ dane dotyczące sankcji nakładanych na biura podróży mogą stanowić dane na temat „podejrzenia popełnienia przestępstwa" przez osoby fizyczne. Pozbawienie biur niektórych praw wiąże się również z pozbawieniem tych samych praw przedstawicieli tych biur. Zalecenia koncentrowały się na prawach podmiotów danych do dostępu i do sprostowania oraz na przekazywanych im informacjach. Dostęp do strony internetowej powinien być udzielany wyłącznie na podstawie analizy poszczególnych przypadków – gdy jest to niezbędne dla personelu Komisji do wykonania powierzonych mu zadań.

### 2.3.6. Konsultacje dotyczące potrzeby przeprowadzenia kontroli wstępnej i powiadomienia niepodlegające przeprowadzeniu kontroli wstępnej

W 2006 roku liczba konsultacji dotyczących potrzeby przeprowadzenia kontroli wstępnej przez EIOD była w dalszym ciągu znaczna. Niektóre przypadki, o których mowa powyżej, były wcześniej przedmiotem tego rodzaju konsultacji: strona intranetowa umowy w sprawie turystyki między UE a Chinami, nagrywanie rozmów telefonicznych w EBI, europejski życiorys (EU-CV) on-line itp.

Komisyjny wykaz osób prawnych (*legal entities file* – LEF) jako taki uznano za niepodlegający przeprowadzeniu kontroli wstępnej, jednak niektóre aspekty, w głównej mierze informacje przekazywane podmiotom danych i wprowadzane do tego wykazu, zostały przeanalizowane w opinii na temat systemu wczesnego ostrzegania (EWS), jako że LEF jest bazą danych zasilającą EWS i zasilaną przez ten system.

Uznano, że przetwarzanie do potrzeb „postępowania sprawdzającego" prowadzone w Radzie nie wymaga kontroli wstępnej, ponieważ rola Rady w ocenie przeprowadzanej przez zainteresowane państwo członkowskie nie jest znacząca.

Prowadzonej przez oba komitety „kontroli tradycyjnej papierowej poczty wychodzącej" również nie uznano za podlegającą kontroli wstępnej, ponieważ możliwe było uniknięcie ewentualnych przypadków naruszenia tajemnicy przez wprowadzenie zmiany do procedury. EIOD monitorował tę zmianę i zamknął sprawę.

System „Adonis" Trybunału Obrachunkowego, podobnie jak i system Komisji, nie podlega przeprowadzeniu kontroli wstępnej z uwagi na fakt, że treść korespondencji i poczty elektronicznej nie ma być przetwarzana, w związku z czym nie jest ona objęta zakresem art. 27 ust. 2 lit. a).

Sprawa dotycząca obowiązujących w EBC zasad odnoszących się do wykorzystywania poufnych informacji ma charakter szczególny w tym sensie, że choć początkowo stwierdzono, że podlega ona przeprowadzeniu kontroli wstępnej, to później uznano, że jednak tak nie jest, z tych samych przyczyn co w przypadku IAS,

o czym będzie mowa poniżej. Fakt, że audytorzy wewnętrzni również prowadzą, w danym przypadku, postępowanie wyjaśniające w zakresie ewentualnego naruszenia zasad przez daną osobę, nie zmienia charakteru przetwarzania. W tym przypadku zastosowanie ma postępowanie wyjaśniające, już poddane kontroli wstępnej.

Kolejna kategoria spraw była bardzo przydatna w określaniu zakresu kontroli wstępnej. Niekiedy, po uważnej analizie powiadomienia przesłanego przez DPO, EIOD stwierdza, że dana operacja przetwarzania nie podlega przeprowadzeniu kontroli wstępnej. W takich przypadkach podaje się uzasadnienie takiego wniosku, zazwyczaj w piśmie skierowanym do DPO, często wraz z pewnymi zaleceniami, które uznano za niezbędne w toku analizy. Ponieważ takie pismo zawierające powyższe elementy zastępuje formalną opinię, uznaje się jego publikację na stronie internetowej EIOD za przydatną.

Dwie interesujące decyzje w tej dziedzinie dotyczyły EKES i KR (wspólnie użytkują infrastrukturę informatyczną) i odnosiły się do systemu poczty elektronicznej i zarządzania kontami użytkowników. Stanowiły one okazję do sprecyzowania warunków niezbędnych, aby EIOD uznał sprawy związane z e-monitoringiem za podlegające przeprowadzeniu kontroli wstępnej. Krótko mówiąc, zagrożenie musi dotyczyć poufności lub oceny zachowania.

Kolejną ważną sprawą było powiadomienie przedłożone przez DPO Komisji na temat służby audytu wewnętrznego (IAS). Stwierdzono, że operacje przetwarzania na potrzeby audytu nie podlegają przeprowadzeniu kontroli wstępnej, ponieważ nie mają one na celu oceny osób, lecz systemów; każdorazowo, gdy pojawiają się wątpliwości co do zachowania osób, stosowne dane muszą zostać przesłane do właściwego organu dochodzeniowego. Kryterium to ma oczywiście zastosowanie również do zasadniczej działalności Trybunału Obrachunkowego.

Sprawa dotycząca „głosowania elektronicznego – wyborów do komitetu personelu" Komisji była okazją do wskazania, że nie wszystkie dane wrażliwe wymagają przeprowadzenia kontroli wstępnej (tylko te wymienione w art. 27 ust. 2 lit. a), oraz że ewentualne wadliwe funkcjonowanie systemu również nie jest wystarczającą podstawą do przeprowadzenia kontroli wstępnej.

### 2.3.7. Monitorowanie opinii i konsultacji dotyczących kontroli wstępnej

Wraz z opinią dotyczącą kontroli wstępnej EIOD wydaje zazwyczaj szereg zaleceń, które należy uwzględnić, aby dana operacja przetwarzania była zgodna z rozporządzeniem. Zalecenia są również wydawane, kiedy daną sprawę analizuje się w celu podjęcia decyzji dotyczącej potrzeby przeprowadzenia kontroli wstępnej i gdy wydaje się, że pewne zasadnicze aspekty wymagają przedsięwzięcia środków naprawczych. W przypadku gdy administrator danych nie stosuje się do tych zaleceń, EIOD może skorzystać z uprawnień przyznanych mu na mocy art. 47 rozporządzenia. EIOD może w szczególności przekazać sprawę do zainteresowanej instytucji lub organu wspólnotowego.

Ponadto EIOD może nakazać zastosowanie się do wniosków o skorzystanie z pewnych praw w odniesieniu do danych (gdy takie wnioski zostały odrzucone z naruszeniem art. 13–19), może też udzielić administratorowi danych ostrzeżenia lub upomnienia. Może również nakazać poprawę, zablokowanie, wykasowanie lub zniszczenie wszystkich danych albo też nałożyć czasowy lub całkowity zakaz przetwarzania. W przypadku niestosowania się do decyzji EIOD ma on prawo przekazać sprawę do Trybunału Sprawiedliwości Wspólnot Europejskich zgodnie z warunkami przewidzianymi w Traktacie WE.

Wszystkie sprawy dotyczące kontroli wstępnej skutkowały wydaniem zaleceń. Jak wyjaśniono powyżej (zob. pkt 2.3.4 i 2.3.5), większość zaleceń dotyczy informacji przekazywanych podmiotom danych, okresów przechowywania, ograniczenia celu oraz prawa dostępu i prawa do sprostowania. Instytucje i organy chętnie stosują się do tych zaleceń i do tej pory decyzje wykonawcze nie były potrzebne. Czas realizacji tych środków jest różny w poszczególnych przypadkach. Od czerwca 2006 roku w oficjalnym piśmie przesyłanym wraz z opinią EIOD zwraca się do danej instytucji o informowanie go o środkach przedsięwziętych w celu realizacji zaleceń w terminie 3 miesięcy. Powinno to doprowadzić do rozpoczęcia monitoringu z własnej inicjatywy danej instytucji lub organu, co faktycznie zaczyna mieć miejsce.

W 2006 roku, a także w odniesieniu do monitoringu, który mógł dotyczyć opinii wydanych w 2005 roku, 83 sprawy (spośród 137 powiadomień otrzymanych między 2004 a 2006 rokiem, co stanowi

60,6% spraw) zostały rozpatrzone zgodnie z poniższym podziałem:

| | |
|---|---|
| Sprawy zamknięte | 17 spraw |
| Sprawy, w odniesieniu do których rozpoczęto monitoring, jednak bez żadnej odpowiedzi ze strony instytucji | 17 spraw |
| Sprawy, w odniesieniu do których rozpoczęto monitoring, który jest w toku lub osiągnął zaawansowane stadium | 34 sprawy |
| Sprawy, w odniesieniu do których monitoring nie został jeszcze rozpoczęty, ponieważ opinie zostały wydane stosunkowo niedawno (od października 2006 roku) | 13 spraw |
| Szczególny monitoring spraw niepodlegających przeprowadzeniu kontroli wstępnej | 2 sprawy |

Monitoring rozpoczęty, jednak bez odpowiedzi ze strony instytucji lub organu (17 spraw), dotyczy 97 zaleceń EIOD. Monitoring będący w toku lub w zaawansowanym stadium (34 sprawy) dotyczy 256 zaleceń EIOD.

W dwóch sprawach analiza powiadomienia prowadziła do wniosku stwierdzającego, że dana sprawa nie podlega przeprowadzeniu kontroli wstępnej, ale pomimo to wydanych zostało 10 zaleceń, które następnie monitorowano. Jedna sprawa została zamknięta, a kolejna znajduje się w zaawansowanym stadium.

W przypadku trzech konsultacji na temat konieczności przeprowadzenia kontroli wstępnej wydano 7 zaleceń, które następnie monitorowano. Jedna sprawa została zamknięta, a dwie kolejne znajdują się w zaawansowanym stadium.

### 2.3.8. Wnioski i przyszłość

Rok 2006 był rokiem wytężonej pracy, czego dowodzi powyższa analiza ilościowa i jakościowa. Niemniej jednak liczba otrzymanych spraw dotyczących kontroli wstępnej pozostaje poniżej oczekiwań, zważywszy na określony na wiosnę 2007 roku termin, o którym była już mowa w sprawozdaniu rocznym za rok 2005. Oczekiwania odnośnie do liczby spraw, które miały wpłynąć w drugiej połowie 2006 roku, były wyższe. Wyjątkiem był OLAF, który przesłał liczne powiadomienia i kontynuuje tę praktykę. Pozostałe instytucje i organy zwiększyły liczbę przesyłanych powiadomień na początku 2007 roku. Nie we wszystkich instytucjach i organach priorytetowe obszary zostały już objęte powiadomieniami, należy zatem kontynuować starania w celu dotrzymania terminu.

Uwagi wymagają jednak nie tylko sprawy priorytetowe. Wszystkie sprawy *ex post* muszą być przedmiotem powiadomienia, jako że one także są objęte art. 27 rozporządzenia, stwarzają zatem szczególne zagrożenie dla praw i wolności podmiotów danych.

Szczególny obszar, który zasługiwał na uwagę w 2006 roku, pozostanie takim również w 2007 roku; chodzi o sprawy międzyinstytucjonalne podlegające kontroli wstępnej. W wielu przypadkach kilka instytucji lub organów wspólnie przeprowadza operacje przetwarzania w dziedzinach danych medycznych, oceny, promocji itp. Odnośne role są różne w poszczególnych przypadkach (jedna instytucja świadczy usługi na rzecz drugiej, kilka organów jest odpowiedzialnych za aspekty częściowe itp.), wszystkie one mają jednak jedną cechę wspólną – mają złożony charakter. Dużo uwagi zostanie poświęcone tej kwestii w 2007 roku.

Szczególna uwaga zostanie również poświęcona łączności elektronicznej. Sprawy dotyczące kontroli *ex post* w tym obszarze priorytetowym zostały nieco opóźnione z uwagi na potrzebę zakończenia analizy, której wynikiem jest dokument dotyczący e-monitoringu (zob. pkt 2.8). Wszystkie operacje przetwarzania przeprowadzane przez instytucje i organy mające na celu monitorowanie właściwego wykorzystania systemów telekomunikacyjnych powinny zostać sprawdzone przez EIOD w 2007 roku.

Opóźnienia w dostarczaniu informacji żądanych w celu uzupełnienia powiadomienia dotyczącego przeprowadzenia kontroli wstępnej również należy zniwelować. Zbyt wiele spraw wciąż oczekuje na rozpatrzenie, niektóre z nich od wielu miesięcy.

Rok 2007 musi również być rokiem, w którym wszystkie agencje i organy będą miały własnego DPO. W tym celu zostanie uruchomiona kampania raz jeszcze przypominająca o tym prawnym obowiązku.

Wraz z końcem wiosny nowe podejście zacznie funkcjonować równolegle z trwającymi pracami w zakresie kontroli wstępnych. Rozpoczną się kontrole, w tym, w razie potrzeby, kontrole na miejscu. Celem będzie upewnienie się, że procedura powiadomień objęła wszystkie sprawy w ramach art. 27, jak również zapewnienie zgodności z rozporządzeniem w pozostałych przypadkach przetwarzania danych osobowych.

## 2.4. Skargi

### 2.4.1. Wprowadzenie

Artykuł 41 ust. 2 rozporządzenia (WE) nr 45/2001 przewiduje, że EIOD „jest odpowiedzialny za monitorowanie i zapewnienie zastosowania przepisów niniejszego rozporządzenia i każdego innego aktu wspólnotowego, odnoszącego się do podstawowych praw i wolności osób fizycznych, w odniesieniu do przetwarzania danych osobowych przez instytucje i organy wspólnotowe". Elementem takiego monitoringu jest rozpatrywanie skarg zgodnie z art. 46 lit. a) ([22]).

Każda osoba fizyczna może wnieść skargę do EIOD niezależnie od narodowości czy miejsca zamieszkania ([23]). Skargi są dopuszczalne wyłącznie wtedy, gdy pochodzą od osoby fizycznej i dotyczą naruszenia zasad ochrony danych przez instytucję lub organ UE w trakcie przetwarzania danych osobowych w ramach wykonywania działań, których całość lub część wchodzi w zakres prawa wspólnotowego. Jak zobaczymy poniżej, wiele skarg złożonych do EIOD uznano za niedopuszczalne, ponieważ nie były one objęte obszarem kompetencji EIOD.

Każdorazowo gdy EIOD otrzymuje skargę, przesyła stronie skarżącej potwierdzenie odbioru bez uszczerbku dla dopuszczalności sprawy, chyba że bez potrzeby dalszej analizy widać, iż skarga jest wyraźnie niedopuszczalna. EIOD zwróci się również do strony skarżącej o dostarczenie informacji na temat innych ewentualnych działań przed sądem krajowym, Europejskim Trybunałem Sprawiedliwości lub Rzecznikiem Praw Obywatelskich (niezależnie od tego, czy są one w toku, czy nie).

Jeśli dana sprawa jest dopuszczalna, EIOD rozpocznie jej wyjaśnianie, w szczególności przez skontaktowanie się z zainteresowaną instytucją/organem lub przez zwrócenie się do strony skarżącej o dodatkowe informacje. EIOD ma prawo uzyskać od stosownego administratora danych lub instytucji/organu dostęp do wszystkich danych osobowych oraz wszystkich informacji niezbędnych do przeprowadzenia postępowania wyjaśniającego, a także uzyskać dostęp do wszelkich obiektów, w których administrator danych lub instytucja/organ wykonują swoje działania. Jak zobaczymy poniżej, EIOD korzystał z powyższych uprawnień w trakcie rozpatrywania skarg w 2006 roku.

W przypadku domniemanego naruszenia przepisów dotyczących ochrony danych EIOD może przekazać sprawę zainteresowanemu administratorowi danych i zaproponować środki mające na celu usunięcie tego naruszenia lub poprawę ochrony podmiotów danych; EIOD może nakazać administratorowi danych zastosowanie się do wniosków o wykonywanie pewnych praw podmiotu danych; może ostrzec lub upomnieć administratora danych; może nakazać sprostowanie, zablokowanie, usunięcie lub zniszczenie wszystkich danych; EIOD może nałożyć zakaz przetwarzania danych; może przekazać sprawę zainteresowanej instytucji wspólnotowej lub Parlamentowi Europejskiemu, Radzie i Komisji. EIOD może także przekazać sprawę Trybunałowi Sprawiedliwości ([24]). Gdyby decyzja miała obejmować przyjęcie środków przez instytucję/organ, EIOD monitoruje to odpowiednio z zainteresowaną instytucją/organem.

W 2006 roku EIOD otrzymał 52 skargi. Z tych 52 spraw tylko 10 zostało uznanych za dopuszczalne i przeanalizowanych przez EIOD. Poniżej przedstawiono ich krótką analizę.

### 2.4.2. Sprawy uznane za dopuszczalne

**Upublicznione informacje dotyczące lobbystów**

Wniesiono skargę przeciwko Parlamentowi Europejskiemu (2006-95) dotyczącą możliwej publikacji domowych adresów akredytowanych lobbystów. Formularz uprawniający do otrzymania identyfikatora lobbysty sugerował, że wpisanie adresu domowego było obowiązkowe. W dalszej części tego samego formularza wspomniano, że przedstawione dalej informacje nie zostaną podane do wiadomości publicznej, sugerując w ten sposób, że wcześniejsze informacje, w tym te dotyczące prywatnego adresu, zostaną upublicznione.

([22]) Zgodnie z art. 46 lit. a) EIOD „wysłuchuje i bada skargi oraz informuje podmiot danych o wyniku w odpowiednim czasie".

([23]) Zgodnie z art. 32 ust. 2 „każdy podmiot danych może wnieść skargę do europejskiego inspektora ochrony danych, jeżeli uważa, że jego prawa wynikające z art. 286 Traktatu zostały naruszone w wyniku przetwarzania jego danych osobowych przez instytucję lub organ Wspólnoty". Artykuł 33: „Każda osoba zatrudniona w instytucji lub organie Wspólnoty może złożyć skargę do europejskiego inspektora ochrony danych, dotyczącą domniemanego naruszenia przepisów niniejszego rozporządzenia regulującego przetwarzanie danych osobowych, bez użycia oficjalnych dróg".

([24]) Zob. art. 47 ust. 1 rozporządzenia (WE) nr 45/2001.

**Liczba kamer kontrolnych wzrosła w ostatnich latach.**

EIOD uznał, że poza nazwiskiem lobbysty i nazwą organizacji, którą reprezentuje, żadnych innych informacji nie podano do wiadomości publicznej. Wydano zatem zalecenie poprawienia formularza, tak aby odzwierciedlał on stosowaną praktykę, a Parlament Europejski odpowiednio zaktualizował swój formularz. EIOD stwierdził również, że publikowanie prywatnych adresów lobbystów naruszałoby ich prywatność. Niemniej jednak można do wiadomości publicznej podać więcej informacji, pod warunkiem że lobbyści byliby o tym informowani w chwili gromadzenia ich danych ([25]).

**Dostęp do raportu medycznego i przekazywanie danych medycznych**

Były urzędnik WE złożył skargę na PMO (Biuro Administrowania i Rozliczania Należności Indywidualnych) w odniesieniu do dwóch aspektów, które uważał za niezgodne z rozporządzeniem (2006-120 i 390). Pierwszy dotyczył prawa dostępu do raportu medycznego. Po zmianie wstępnej decyzji EIOD stwierdził, że tymczasowe ograniczenie, zastosowane wtedy gdy raport nie miał jeszcze charakteru ostatecznego, było zgodne z prawem, zalecił jednak, aby dostęp do raportu końcowego został przyznany w zwykłym trybie mającym zastosowanie do innych raportów tego rodzaju oraz aby ponownie rozważyć dostęp do raportu tymczasowego z myślą o raporcie końcowym. Drugi aspekt dotyczył przekazania danych medycznych firmie ubezpieczeniowej bez uzyskania zgody strony skarżącej. Stwierdzono, że przekazanie tych danych było konieczne i nie było działaniem zbyt daleko idącym w kontekście obowiązków administracji WE do celów ubezpieczenia finansowych skutków choroby zawodowej, wcześniejszej emerytury itp. W każdym razie informacja o przetwarzaniu danych medycznych przez PMO musi zostać przedłożona do przeprowadzenia kontroli wstępnej. Zwrócono się również o zmianę tej drugiej decyzji; sprawa jest obecnie w toku. Zgłoszono kilka innych zagadnień związanych z dostępem do dokumentów na mocy rozporządzenia (WE) nr 1049/2001.

**Skarga na dochodzenie**

Złożono skargę na Europejski Komitet Ekonomiczno-Społeczny (EKES) (2006-181 i 287) dotyczącą początkowej fazy dochodzenia, o które zwrócił się urzędnik, w sprawie nieupoważnionego dostępu do jego konta poczty elektronicznej (domniemane użycie jego loginu użytkownika i hasła) oraz późniejszego nieprzyznania przez dyrektora ds. zasobów ludzkich dostępu do plików dziennika strony skarżącej w celu udowodnienia takiego nieupoważnionego dostępu. Ze względu na zaistniałe na początku nieporozumienie co do elementów niezbędnych do celów zbadania nieupoważnionego dostępu (służby IT twierdziły, że dostęp dotyczył raczej plików dziennika strony trzeciej niż plików samego podmiotu danych), EKES stwierdził początkowo, że dochodzenie nie może mieć miejsca i poinformował o swym wniosku stronę skarżącą. Po złożeniu przez stronę skarżącą wniosku o interwencję do DPO w EKES dostęp do własnych plików dziennika strony skarżącej i ich analiza wskazuje na nieupoważniony dostęp do elektronicznych skrzynek pocztowych strony skarżącej. W decyzji dotyczącej tej sprawy EIOD wyraził ubolewanie z faktu, że do chwili złożenia formalnej skargi przez stronę skarżącą i interwencji ze strony DPO w EKES, administracja tego ostatniego – ze względu na nieporozumienie, o którym mowa powyżej, i brak właściwej analizy technicznej i prawnej – nie zdołała dojść do zadowalających konkluzji dotyczących wniosku strony skarżącej.

([25]) Zob. ustalenia dostępne pod adresem internetowym: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/06-08-31_transparency_lobbyists_EN.pdf.

**Nadzór wideo**

Jeden z obywateli UE złożył skargę na Parlament Europejski (PE) dotyczącą stosowanych przez PE praktyk w zakresie nadzoru wideo (2006-185). Strona skarżąca zakwestionowała proporcjonalność nadzoru poza budynkami PE w Brukseli. Twierdziła również, że informacje na ten temat dostarczane społeczeństwu są niewystarczające. W swej decyzji EIOD zażądał od PE poprawienia informacji przekazywanych społeczeństwu i dostosowania ustawienia kamer monitorujących. Głównym punktem, na którym skupił się EIOD, było dopilnowanie, aby demonstranci nie byli monitorowani przez PE, czy to celowo, czy przypadkowo, jako że mogłoby to mieć negatywne skutki dla wolności słowa. Monitorując działania wynikające z tej opinii, EIOD kontynuował wraz z PE prace na rzecz poprawy praktyk stosowanych przez PE w zakresie nadzoru wideo, z uwzględnieniem szczególnych potrzeb bezpieczeństwa PE, w tym zabezpieczenia wizyt głów państw lub innych ważnych osobistości wymagających zwiększonej ochrony, które nie zostały odzwierciedlone we wstępnej decyzji EIOD. W związku ze skargą EIOD zainicjował również badanie wśród instytucji i organów UE oraz rozpoczął prace nad zestawem wytycznych dotyczących nadzoru wideo, których opracowanie planuje się ukończyć w 2007 roku.

**Dostęp do raportu z dochodzenia**

Złożono skargę na Trybunał Obrachunkowy w zakresie prawa dostępu danej osoby, na mocy art. 13, do raportu z dochodzenia (2006-239). Raport ten dotyczył domniemanego przypadku nękania i złego zarządzania wynikającego ze skargi wniesionej na podstawie art. 90 regulaminu pracowniczego. Jedna z zainteresowanych stron zażądała dostępu do raportu, jednak Trybunał odmówił go jej, uzasadniając, że „raport nie dotyczył tej osoby". EIOD podjął w tym przypadku próbę przeanalizowania zakresu prawa dostępu danej osoby na mocy art. 13 i ewentualnych ograniczeń tego prawa na mocy art. 20. Rozpatrywanie sprawy obejmowało wizytę na miejscu złożoną przez zastępcę EIOD i członka jego zespołu, w szczególności w celu uzyskania dostępu do zawartości przedmiotowego raportu oraz raportów z rozmów przeprowadzonych przez osobę prowadzącą dochodzenie. EIOD wydał decyzję, w której uznał, że strona skarżąca ma prawo do uzyskania dostępu do wszelkich odnoszących się do niej wyników postępowania wyjaśniającego. Jedyne wyjątki powinny obejmować przypadki, gdy dane ujawniają informacje w żaden sposób nieodnoszące się do strony skarżącej oraz wyniki rozmów ze świadkami. EIOD zwrócił się zatem do Trybunału Obrachunkowego, aby ten przyznał stronie skarżącej szerszy, choć nie całkowity, dostęp do raportu z dochodzenia. Zalecenie to jeszcze nie zostało wykonane.

**Prawo dostępu i prawo do sprostowania**

Wniesiono skargę przeciwko Dyrekcji Generalnej ds. Personelu i Administracji Komisji Europejskiej, w której to skardze domagano się prawa dostępu na mocy art. 13 do niektórych dokumentów dotyczących strony skarżącej oraz prawa do sprostowania pewnych danych na mocy art. 14 (2006-266). W skardze tej przywoływano również art. 18 w celu wyrażenia sprzeciwu wobec przetwarzania danych strony skarżącej. Po dalszych wnioskach o wyjaśnienie sytuacji EIOD stwierdził, że administracja zapewniła dostęp do wszystkich wymaganych dokumentów, z wyjątkiem jednego e-maila, w odniesieniu do którego administracja nie posiadała wystarczających informacji, aby zidentyfikować dokument. Jeśli chodzi o korzystanie z prawa do sprostowania, EIOD ponownie wyraził swoje stanowisko mówiące, że nieścisłość nie może być przesłanką do stosowania prawa do sprostowania względem subiektywnych danych. i wreszcie, jeśli chodzi o możliwość sprzeciwienia się przetwarzaniu danych na podstawie art. 18 rozporządzenia, EIOD uznał, że strona skarżąca nie przywołała „istotnych uzasadnionych przyczyn".

**Prawo do sprostowania i zablokowania**

Jedna skarga (2006-436) dotyczyła prawa do niezwłocznego sprostowania niepełnych danych (art. 14) dotyczących przebiegu kariery zawodowej (*historique de carrière*) w Sysper2 (system informatyczny Komisji Europejskiej w obszarze zasobów ludzkich, który obejmuje kilka podmodułów). Chociaż Komisja zakwestionowała twierdzenie o niepełnych danych, zaproponowano wprowadzenie pola przeznaczonego na wpisanie uwag w przebiegu kariery zawodowej strony skarżącej. EIOD przyjął tę propozycję jako rozwiązanie tymczasowe, zwrócił się jednak dodatkowo o wyjaśnienie trudności technicznych dotyczących prawa do sprostowania danych odnoszących się do przebiegu kariery zawodowej w systemie Sysper2. Obie kwestie, i rozwiązania tymczasowego, i wyjaśnień, pozostają w toku.

**Skarga na dochodzenie prowadzone przez jednego z DPO**

Wpłynęła skarga na dochodzenie prowadzone przez jednego z urzędników ds. ochrony danych (2006-451). Dochodzenie DPO było wynikiem wniosku o dostęp do wycofanego e-maila. Strona skarżąca miała wątpliwości co do tego, czy to dochodzenie leży w zakresie kompetencji DPO, czy procedura zastosowana przez DPO jest zgodna z prawem oraz czy środki przyjęte przez DPO są zgodne z zasadami proporcjonalności, dobrej wiary i należytej staranności. Po przeprowadzeniu dochodzenia w tej sprawie i po zwróceniu się o dalsze wyjaśnienia do zainteresowanych stron EIOD stwierdził, że rozpoczęcie dochodzenia należy uznać za zgodne z prawem nie tylko dlatego, że DPO działał na podstawie uprawnień przyznanych w załączniku do rozporządzenia, ale także dlatego, że dochodzenie rozpoczęto w wyniku złożenia wniosku o dostęp na mocy art. 13 rozporządzenia. Niemniej jednak EIOD uznał skargę za uzasadnioną, ponieważ środki przyjęte przez DPO były zbyt daleko idące w świetle odnośnych interesów oraz możliwości wykorzystania innych mniej uciążliwych środków. DPO zwrócił się o zmianę, uwagi strony skarżącej jeszcze nie wpłynęły.

**Publikacja w sprawozdaniu rocznym za 2005 rok**

Kolejna skarga pojawiła się w kontekście monitorowania jednej ze spraw wspomnianych w sprawozdaniu rocznym za rok 2005 (2005-190), zgłoszonej później przez stronę skarżącą do Europejskiego Rzecznika Praw Obywatelskich. Strona skarżąca sprzeciwiła się również krótkiemu przedstawieniu tej sprawy w sprawozdaniu rocznym za rok 2005, twierdząc, że było ono nieprawidłowe i przedwczesne. EIOD odrzucił tę skargę. Również ta sprawa znajduje się obecnie przed Europejskim Rzecznikiem Praw Obywatelskich.

### 2.4.3. Sprawy niedopuszczalne: główne przyczyny niedopuszczalności

Z 52 skarg otrzymanych w 2006 roku 42 uznano za niedopuszczalne z uwagi na brak właściwości EIOD w tym zakresie. Stanowi to dwukrotny wzrost w porównaniu z 2005 rokiem. Znakomita większość tych skarg nie dotyczy przetwarzania danych osobowych przez instytucję lub organ WE; dotyczą one wyłącznie przetwarzania na poziomie krajowym. W niektórych z tych skarg zwracano się do EIOD o ponowne przeanalizowanie stanowiska przyjętego przez krajowy organ ds. ochrony danych; takie działanie nie jest objęte mandatem EIOD. Strony skarżące poinformowano, że Komisja Europejska jest kompetentna w przypadku, gdy dane państwo członkowskie nie wykonuje prawidłowo dyrektywy 95/46/WE.

Trzy sprawy dotyczyły przetwarzania danych osobowych członków personelu WE, chociaż istota tych skarg nie dotyczyła przetwarzania przez instytucję lub organ. Skargi obejmowały zatem podmioty administracji UE, które muszą przestrzegać rozporządzenia (WE) nr 45/2001, jednak domniemane naruszenia ochrony danych dotyczyły przetwarzania na poziomie krajowym. Jeden z takich przypadków dotyczył członka personelu skarżącego się na otrzymanie na adres biurowy materiałów politycznych od jednej z partii w związku z wyborami w państwie członkowskim jego pochodzenia. W tym przypadku nie można było wykluczyć, że adres biurowy został przekazany przez instytucję stałemu przedstawicielstwu tego państwa członkowskiego. Skarga dotyczyła jednak partii politycznej działającej na mocy prawa krajowego, która wykorzystała taką informację. W związku z tym przekazano dane kontaktowe krajowych organów ds. ochrony danych, wraz z wyjaśnieniem powodów, dla których EIOD był organem właściwym do zajęcia się tą sprawą.

Duża liczba skarg niedopuszczalnych, w szczególności dotyczących zagadnień na poziomie krajowym, skutkowała umieszczeniem bardziej precyzyjnych informacji na nowej stronie internetowej w odniesieniu do zakresu kompetencji EIOD. Temat ten okazał się również istotny dla kierowanych do Parlamentu Europejskiego petycji dotyczących kwestii ochrony danych, które czasem przekazuje się do EIOD celem uzyskania jego uwag lub porady. Jeśli dane zagadnienie dotyczy wyłącznie poziomu krajowego lub nie obejmuje przetwarzania danych osobowych przez instytucję lub organ wspólnotowy, EIOD nie jest właściwy w takiej sprawie i może jedynie udzielić ogólnych informacji, umożliwiając Komisji ds. Petycji podjęcie decyzji dotyczącej właściwego toku działania.

### 2.4.4. Współpraca z Europejskim Rzecznikiem Praw Obywatelskich

Zgodnie z art. 195 Traktatu WE Europejski Rzecznik Praw Obywatelskich jest uprawniony do przyjmowania skarg, które dotyczą przypadków niewłaściwego

**Od prawej: Peter Hustinx, P. Nikiforos Diamandouros i Joaquín Bayo Delgado po podpisaniu umowy.**

administrowania w działaniach instytucji lub organów wspólnotowych. Kompetencje Europejskiego Rzecznika Praw Obywatelskich i EIOD są zbieżne w obszarze rozpatrywania skarg w tym sensie, że przypadki niewłaściwego administrowania mogą dotyczyć przetwarzania danych osobowych. W związku z tym skargi wnoszone do Europejskiego Rzecznika Praw Obywatelskich mogą obejmować kwestie ochrony danych. Podobnie skargi wnoszone do EIOD mogą dotyczyć skarg, które były już, w części lub w całości, przedmiotem decyzji Rzecznika.

Aby uniknąć zbędnego powielania pracy i w jak największym stopniu zapewnić spójne podejście zarówno do ogólnych, jak i szczególnych kwestii ochrony danych zgłaszanych przez strony skarżące, w listopadzie 2006 roku podpisano protokół ustaleń między Europejskim Rzecznikiem Praw Obywatelskich a EIOD. Obie strony zobowiązują się w szczególności do informowania stron skarżących o drugiej instytucji w sytuacji, kiedy mogłoby to być dla nich istotne i ułatwić przekazywanie skarg; do informowania drugiej instytucji o skargach dla niej istotnych; do nieotwierania ponownie skargi, którą już wcześniej wniesiono, chyba że przedłożono istotne nowe dowody, a także do przyjęcia spójnego podejścia do prawnych i administracyjnych aspektów ochrony danych, w ten sposób propagując prawa i interesy obywateli oraz stron skarżących ([26]).

([26]) Protokół ustaleń jest dostępny pod adresem: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/News/06-11-30_EO_EDPS_MoU_EN.pdf.

### 2.4.5. Dalsze prace w dziedzinie skarg

EIOD kontynuował prace nad przygotowaniem wewnętrznego podręcznika rozpatrywania skarg przez personel EIOD. Główne elementy procedury i wzorcowy formularz do składania skarg, wraz z informacjami na temat dopuszczalności skarg, zostaną udostępnione na stronie internetowej we właściwym czasie.

Zastępca EIOD oraz jeden z członków personelu uczestniczyli w warsztatach dotyczących rozpatrywania spraw z udziałem krajowych organów ds. ochrony danych zorganizowanych w Madrycie w marcu 2006 roku. W trakcie tych warsztatów zastępca EIOD przedstawił prezentację na temat przeprowadzania kontroli wstępnej przez EIOD. Trzech członków personelu uczestniczyło również w podobnych warsztatach w Atenach w październiku 2006 roku i przedstawiło prezentację na temat badania przeprowadzonego przez EIOD w zakresie nadzoru wideo.

## 2.5. Postępowania wyjaśniające

W 2006 roku EIOD przeprowadził w różnych obszarach wiele postępowań wyjaśniających, z których kilka zasługuje na szczególną uwagę w niniejszym sprawozdaniu.

**Dyrekcja Generalna ds. Konkurencji Komisji Europejskiej**

W ślad za pismem otrzymanym od organu ds. ochrony danych w jednym z państw członkowskich przeprowadzono postępowanie wyjaśniające w związku z zakrojonym na szeroką skalę postępowaniem wyjaśniającym prowadzonym przez Komisję Europejską w sektorze energii elektrycznej (2005-207).

Komisja przesłała różne kwestionariusze do rozmaitych przedsiębiorstw w sektorze energii elektrycznej z siedzibą w 23 państwach członkowskich. Ponieważ w piśmie od organu ds. ochrony danych sugerowano, że w ramach sektorowego postępowania wyjaśniającego prowadzonego przez Komisję zgromadzono w sposób niezgodny z prawem dane osobowe, EIOD przeprowadził wstępne postępowanie wyjaśniające: zwracając się o przekazanie kwestionariuszy i analizując je, składając wizyty na miejscu i organizując spotkania z personelem w Dyrekcji Generalnej (DG)

ds. Konkurencji w celu wyjaśnienia pewnych aspektów przetwarzania informacji w postępowaniu wyjaśniającym Komisji.

Na podstawie wstępnych ustaleń EIOD zwrócił się do ww. DG o zapewnienie nieprzetwarzania danych osobowych w ramach postępowania wyjaśniającego Komisji, zalecił również szczególne środki w tym celu. W listopadzie 2006 roku DG ds. Konkurencji przedstawiła sprawozdanie z wykonania szeregu działań, zgodnie z sugestiami EIOD, wraz ze szczegółowymi kontrolami dotyczącymi zgromadzonych danych przy zapewnieniu szczegółowych informacji swemu personelowi. W wyniku tego sprawozdania, gwarantującego, że żadne dane osobowe dotyczące konsumentów energii elektrycznej nie były ani nie będą przetwarzane w trakcie postępowania wyjaśniającego prowadzonego przez Komisję w sektorze energii elektrycznej, EIOD podjął decyzję o zamknięciu swego wstępnego postępowania wyjaśniającego w tej sprawie.

**SWIFT**

W 2006 roku EIOD rozpoczął postępowanie wyjaśniające w sprawie przekazywania amerykańskim władzom danych bankowych europejskich obywateli za pośrednictwem Towarzystwa Światowej Finansowej Telekomunikacji Międzybankowej (SWIFT) (2006-357).

Po pojawieniu się informacji na ten temat w mediach w czerwcu 2006 roku EIOD wysłał do Europejskiego Banku Centralnego pismo, w którym zwrócił się o informacje dotyczące jego roli jako użytkownika, a także jako organu nadzorującego SWIFT. Ponadto EIOD wziął udział w przesłuchaniu zorganizowanym przez Parlament Europejski w październiku i aktywnie uczestniczył w przygotowaniu opinii przyjętej w listopadzie przez grupę roboczą art. 29.

W październiku EIOD spotkał się we Frankfurcie z prezesem Europejskiego Banku Centralnego z myślą o wymianie dalszych informacji na temat prowadzonego przez EIOD postępowania wyjaśniającego oraz uzyskaniu dodatkowych informacji na temat roli EBC. W grudniu, po otrzymaniu dalszych stosownych dokumentów i informacji faktycznych zarówno ze strony SWIFT, jak i EBC, EIOD przesłał projekt swojej opinii do EBC celem przedstawienia uwag.

Po uważnej analizie uwag EBC, EIOD przyjął końcową opinię na początku 2007 roku. Opinia dotyczy różnych ról, jakie w tej sprawie odgrywa EBC. Jako klient SWIFT, EBC – pełniąc wraz ze SWIFT funkcję administratora danych – powinien zapewnić pełne przestrzeganie rozporządzenia (WE) nr 45/2001 w odniesieniu do dokonywanych przez siebie operacji płatności. Jako organ nadzorujący, wraz z innymi bankami centralnymi, EBC powinien wspierać działania zmierzające do tego, aby nadzór nad systemem SWIFT obejmował ochronę danych oraz aby zasady dotyczące poufności nie uniemożliwiały terminowego informowania stosownych organów w razie potrzeby. Wreszcie, EIOD wezwał EBC do wykorzystania centralnej roli jako decydenta z myślą o dopilnowaniu, aby europejskie systemy płatności były zgodne z europejskim prawem dotyczącym ochrony danych.

W 2007 roku EIOD będzie uważnie monitorował rozwój wydarzeń w tej sprawie, mając na uwadze dopilnowanie, aby operacje płatności były dokonywane przez instytucje wspólnotowe w pełnej zgodności z rozporządzeniem w sprawie ochrony danych. W szerszej perspektywie EIOD, we współpracy z innymi krajowymi organami ds. ochrony danych, nadal będzie wykorzystywał swoją funkcję konsultacyjną w celu zadbania o to, aby struktura europejskich systemów płatności nie naruszała prywatności klientów banków w UE.

**Inne postępowania wyjaśniające**

Jak już wspomniano w pkt 2.4.2, zastępca EIOD oraz jeden z członków jego zespołu również przeprowadzili dochodzenie w ramach skargi na Trybunał Obrachunkowy (2006-239). Taka wizyta na miejscu umożliwiła zastępcy EIOD uzyskanie dostępu do pełnego sprawozdania, którego to dostępu częściowo odmówiono stronie skarżącej.

Miała miejsce również wizyta na miejscu w centrali nadzoru wideo w Parlamencie Europejskim w ramach skargi na Parlament Europejski dotyczącej nadzoru wideo (2006-185).

EIOD pracuje nad regulaminem wewnętrznym przewidzianym w art. 46 lit. k) rozporządzenia (WE) nr 45/2001. Będzie on obejmował pewne przepisy dotyczące postępowań wyjaśniających i zostanie wkrótce przyjęty.

EIOD pracuje również nad polityką w zakresie kontroli w celu ustanowienia ram i metodologii prowadzonych przez siebie kontroli. Od krajowych organów ds. ochrony danych oraz innych instytucji UE zebrano informacje na temat istniejących standardów kontroli służące jako wkład w te prace. Polityka EIOD w zakresie kontroli będzie się początkowo koncentrować na uzyskaniu – do wiosny 2007 roku – zgodności z przepisami dotyczącymi mianowania DPO w instytucjach i organach wspólnotowych oraz na powiadomieniach dotyczących przeprowadzenia kontroli wstępnej. Polityka ta zostanie później poszerzona do monitorowania pełnego przestrzegania rozporządzenia (WE) nr 45/2001.

## 2.6. Środki administracyjne

Rozporządzenie przewiduje prawo EIOD do uzyskiwania informacji o środkach administracyjnych, które dotyczą przetwarzania danych osobowych. EIOD może wydać opinię na wniosek instytucji lub organu albo z własnej inicjatywy. Artykuł 46 lit. d) wzmacnia ten mandat w odniesieniu do przepisów wykonawczych rozporządzenia, w szczególności przepisów dotyczących urzędników ds. ochrony danych (art. 24 ust. 8).

Z własnej inicjatywy, zgodnie z tym, co przewidziano w sprawozdaniu rocznym za rok 2005, EIOD rozpoczął badanie w zakresie aktualnych praktyk dotyczących akt osobowych personelu w instytucjach i organach. Na podstawie jego wyników i analizy kontroli wstępnych w dziedzinach pokrewnych w przygotowaniu znajduje się dokument na temat stosownych wytycznych. Jednocześnie w kontekście aktualnych przepisów regulaminu pracowniczego przeanalizowano szczególny problem przechowywania danych na temat środków dyscyplinarnych; w opracowaniu znajdują się pewne sugestie dotyczące praktyki ogólnej.

Jak przewidziano w ubiegłorocznym sprawozdaniu, omówiono również kwestię przekazywania danych państwom trzecim i organizacjom międzynarodowym, w szczególności przez OLAF, i opracowano wstępną wersję stosownego dokumentu. Uwzględniono zarówno potrzebę strukturalnego podejścia, przy zastosowaniu pragmatycznej interpretacji art. 9 ust. 8 rozporządzenia (WE) nr 45/2001 i wykorzystaniu protokołów ustaleń, jak i nieuniknione stosowanie wyjątków określonych w art. 9 ust. 6, wraz z ewentualnymi zabezpieczeniami.

Jak wspomniano powyżej w pkt 2.4.2, jedna ze skarg skutkowała rozpoczęciem kontroli dotyczącej nadzoru wideo w europejskich instytucjach i organach. Po otrzymaniu informacji od stosownych DPO obecnie gromadzone są informacje na temat najlepszych praktyk od krajowych instytucji nadzoru. Po zgromadzeniu całego materiału zostaną wydane wytyczne dotyczące stosowania nadzoru wideo.

Jeśli chodzi o porady udzielane na wniosek, w 2006 roku EBC przesłał do konsultacji swój projekt przepisów wykonawczych do rozporządzenia. EIOD zalecił dodanie wartości tekstowi samego rozporządzenia przez szczegółowe przedstawienie informacji na temat uprawnień i obowiązków DPO, korzystania z praw przysługujących podmiotom danych, powiadomień itp. Z zadowoleniem przyjął uprzednią konsultację EIOD przed dokonaniem oceny DPO i zasugerował mianowanie zastępcy DPO.

Przedmiotem konsultacji i uwag EIOD było wiele innych środków administracyjnych.

Jedną z istotniejszych konsultacji przewodniczącego kolegium szefów administracji była sprawa projektu noty na temat okresu przechowywania danych medycznych (2006-532). EIOD wydał opinię na początku 2007 roku, podkreślając potrzebę zmiany ogólnego terminu z minimalnego na maksymalny oraz ustalenia kilku krótszych okresów dla konkretnych przypadków, bez uszczerbku dla kilku wyjątków powyżej maksymalnego okresu 30 lat (pylica azbestowa itp.).

DPO Komisji zasięgnął rady w sprawie możliwości zastosowania art. 9 rozporządzenia (przekazywanie danych osobowych państwom i organizacjom spoza UE) (2006-403) w następstwie sprawy Lindqvista ([27]). Według opinii EIOD art. 9 nie ma zastosowania do publikowania danych osobowych za pośrednictwem Internetu przez europejskie instytucje i organy, zastosowanie mają jednak pozostałe przepisy rozporządzenia, zapobiegając wykorzystywaniu Internetu jako sposobu na obejście zasad ochrony danych w zakresie przekazywania danych osobowych.

([27]) Wyrok Europejskiego Trybunału Sprawiedliwości z 6 listopada 2003 r., (C-101/01).

Ten sam DPO zwrócił się o wydanie opinii w sprawie możliwości zastosowania rozporządzenia do działań podejmowanych na mocy Traktatu Euratom (2006-311). Odpowiedź była twierdząca.

DPO Parlamentu Europejskiego zasięgał konsultacji w sprawie wykorzystywania nadzoru wideo do celów innych niż bezpieczeństwo i bez rejestrowania (2006-490 i 2006-510). Stwierdzono, że rozporządzenie ma zastosowanie pod warunkiem, że przetwarzane są dane osobowe (tj. wizerunki zidentyfikowanych lub możliwych do zidentyfikowania osób). Wydano pewne zalecenia odnośnie do najlepszych praktyk.

DPO Trybunału Obrachunkowego zasięgał opinii w sprawie najlepszego sposobu przestrzegania art. 13 rozporządzenia (prawo dostępu) w odniesieniu do podmiotów danych, których dane zostały zgromadzone przez Trybunał, ale nie są przedmiotem faktycznej sprawy w zakresie kontroli, jako że nie zostały one losowo wybrane do takiej czynności (2006-341). Zalecono rozwiązanie praktyczne z poszanowaniem przepisów rozporządzenia.

DPO Europejskiego Trybunału Sprawiedliwości zwrócił się o opinię EIOD w sprawie jego analizy na temat publikacji w Intranecie list rezerwowych personelu kontraktowego (2006-122). Jego wnioski dotyczące, między innymi, potrzeby udzielenia praktycznych informacji i prawa do wyrażenia sprzeciwu zostały potwierdzone.

DPO Rady zasięgnął opinii EIOD w sprawie przetwarzania danych osobowych osób uczestniczących w posiedzeniach grup roboczych Rady (2006-125). Wydano pewne zalecenia dotyczące informacji i przechowywania danych.

Przedmiotem konsultacji prowadzonych przez tego samego i pozostałych DPO było wiele innych kwestii, na przykład dostęp do danych informatycznych, cofnięcie zgody, podmioty danych w dochodzeniach w sprawie nękania, archiwizowanie poczty elektronicznej itp.

## 2.7. Publiczny dostęp do dokumentów i ochrona danych

Dokument bazowy na temat publicznego dostępu do dokumentów i ochrony danych, który opublikowano w lipcu 2005 roku, otrzymał szerokie poparcie w instytucjach i organach, które zwykle podlegają zarówno rozporządzeniu (WE) nr 1049/2001, jak i rozporządzeniu (WE) nr 45/2001. Komisja Europejska odmiennie interpretuje kluczowy przepis – art. 4 ust. 1 lit. b) rozporządzenia (WE) nr 1049/2001 – i w związku z tym nie stosuje ustaleń zawartych w tym dokumencie w codziennej pracy.

Kwestią zasadniczą w tym dokumencie jest założenie, że nie jest możliwa automatyczna odmowa dostępu do dokumentów będących w dyspozycji administracji UE tylko dlatego, że zawierają one dane osobowe. Wyjątek, jaki ustanawia art. 4 ust. 1 lit. b) ([28]) rozporządzenia na temat publicznego dostępu, stanowi, że warunkiem uzasadniającym wstrzymanie ujawnienia dokumentu jest naruszona prywatność danej osoby. Wzywając do rzeczowej i indywidualnej analizy w każdym przypadku, powyższy dokument umieszcza starannie sformułowany wyjątek w kontekście, argumentując, że aby odmówić ujawnienia publicznego dokumentu, niezbędne jest spełnienie poniższych kryteriów:

1) zagrożona musi być prywatność podmiotu danych;
2) publiczny dostęp musi w istotny sposób wpływać na podmiot danych;
3) publiczny dostęp jest niedozwolony zgodnie z prawodawstwem dotyczącym ochrony danych.

Po wystąpieniu w stosownej sprawie przed Sądem Pierwszej Instancji (T-194/04; Bavarian Lager przeciwko Komisji) ([29]) EIOD uczestniczył w przesłuchaniu przed tym sądem we wrześniu. Sprawa pochodzi z 1996 roku, kiedy Komisja Europejska zorganizowała spotkanie, na którym odniesiono się do kwestii warunków importu piwa do Zjednoczonego Królestwa. Jedno z przedsiębiorstw pragnące sprzedawać w Zjednoczonym Królestwie niemieckie piwo zwróciło się o dostęp do wykazu uczestników spotkania. Komisja odmówiła, opierając się głównie na prawodawstwie dotyczącym ochrony danych w odniesieniu do nieujawniania dokumentów.

([28]) Instytucje odmówią dostępu do dokumentu, jeśli ujawnienie go „naruszyłoby ochronę […] prywatności i integralności osoby fizycznej, w szczególności w odniesieniu do ustawodawstwa Wspólnoty związanego z ochroną danych osobowych".

([29]) EIOD występował również w dwóch innych sprawach przed Sądem Pierwszej Instancji, w których podniesiono te same zagadnienia (sprawy T-170/03 i T-161/04). Sprawy te nie weszły jeszcze w etap przesłuchania.

Przesłuchanie w Sądzie stanowiło dla EIOD dobrą okazję, aby wyjaśnić i przedstawić wnioski zamieszczone w wyżej wspomnianym dokumencie bazowym, mówiące, że dokumenty zawierające dane osobowe można podawać do wiadomości publicznej, chyba że w istotny sposób szkodzi to prywatności danej osoby fizycznej. Ponieważ zasady ochrony danych nie zakładają istnienia ogólnego prawa do anonimowego udziału w czynnościach Komisji, EIOD udzielił poparcia wnioskodawcy. Podkreślając, że przejrzystość i ochrona danych stanowią dwa równie istotne podstawowe prawa, EIOD zwrócił się do Sądu o unieważnienie odmowy Komisji dotyczącej ujawnienia pełnego wykazu uczestników. Sąd nie wydał jeszcze orzeczenia.

Inne działania EIOD w tym obszarze obejmowały:
- doradzanie Europejskiemu Rzecznikowi Praw Obywatelskich w skargach na ten temat;
- dostarczenie sekretariatowi grupy roboczej art. 29 analizy na temat możliwości ujawnienia informacji o beneficjentach funduszu rybackiego;
- rozpatrzenie skargi na temat dopuszczalności ujawnienia adresu domowego lobbystów akredytowanych przy Parlamencie Europejskim (zob. również pkt 2.4.2).

## 2.8. E-monitoring

Korzystanie z narzędzi łączności elektronicznej w instytucjach i organach UE generuje dane osobowe, których przetwarzanie skutkuje stosowaniem rozporządzenia (WE) nr 45/2001. Pod koniec 2004 roku EIOD rozpoczął prace nad przetwarzaniem danych generowanych w wyniku korzystania ze środków łączności elektronicznej (telefonu, poczty elektronicznej, telefonu komórkowego, Internetu itp.) w instytucjach i organach UE. W marcu 2006 roku urzędnikom ds. ochrony danych (DPO) udostępniono projekt dokumentu na temat e-monitoringu dotyczącego korzystania i monitorowania sieci komunikacji, co miało na celu zebranie ich uwag i reakcji.

Aby przetestować główne zasady tego dokumentu, w czerwcu 2006 roku EIOD zorganizował stosowne warsztaty. Uczestniczyło w nich ponad 50 przedstawicieli administracji UE, począwszy od DPO, koordynatorów ds. ochrony danych i personelu IT aż po komitety personelu. Po ogólnej prezentacji głównych wniosków zawartych w dokumencie EIOD przetestował te wnioski oraz zestaw wytycznych w konkretnych scenariuszach. Uczestnicy pracowali nad takimi tematami, jak przechowywanie danych o połączeniach do celów budżetowych, czytanie poczty elektronicznej personelu w trakcie jego nieobecności oraz monitorowanie stosowania przez pracodawcę polityki sprawiedliwego dostępu (*fair use policy*).

Na podstawie wyników warsztatów i uwag zgłoszonych w ich następstwie końcowy dokument był gotowy do publikacji na początku 2007 roku.

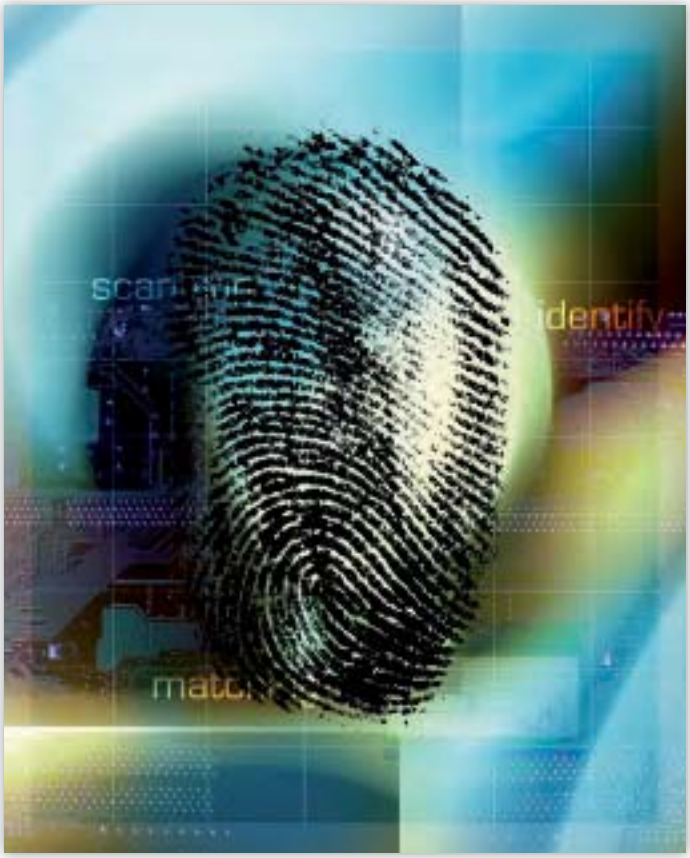
## 2.9. Eurodac

Eurodac to obszerna baza danych zawierająca odciski palców osób ubiegających się o azyl i nielegalnych imigrantów znajdujących się na terytorium UE. Baza danych pomaga w skutecznym stosowaniu konwencji dublińskiej w sprawie rozpatrywania wniosków o azyl. EIOD jest właściwym organem monitorującym działania centralnej jednostki Eurodac, dbającym o to, aby prawa podmiotów danych nie były naruszane. Kolejnym zasadniczym aspektem nadzorczej funkcji EIOD jest współpraca z krajowymi instytucjami nadzoru mająca na celu:
- analizowanie problemów wykonawczych w związku z funkcjonowaniem bazy Eurodac;
- analizowanie ewentualnych trudności napotykanych przez krajowe instytucje nadzoru w trakcie kontroli;
- formułowanie zaleceń dotyczących wspólnych rozwiązań istniejących problemów.

Z uwagi na te obowiązki EIOD i służby Komisji organizowały regularne spotkania i nawiązywały nieformalne kontakty w celu omawiania poszczególnych aspektów zadań nadzorczych EIOD. Kontakty te dotyczyły w szczególności kontroli Eurodac przeprowadzonej przez EIOD oraz obaw związanych z dużą liczbą „wyszukiwań specjalnych" wykonywanych w systemie ([30]). Komisja i Parlament Europejski również chciały, by ta kwestia została wyjaśniona. Zbadanie i, w razie potrzeby, poprawa tej sytuacji stanowi jeden z głównych celów współpracy z krajowymi organami ds. ochrony danych.

([30]) Odzwierciedlając zasady ochrony danych służące zabezpieczeniu praw podmiotu danych do dostępu do jego własnych danych, art. 18 ust. 2 rozporządzenia dotyczącego Eurodac przewiduje możliwość przeprowadzania „wyszukiwań specjalnych" na wniosek zainteresowanej osoby, której dane są przechowywane w centralnej bazie danych. Ta kategoria transakcji jest szeroko wykorzystywana przez niektóre państwa; dane liczbowe nie odpowiadają faktycznej liczbie wniosków o dostęp złożonych przez osoby fizyczne. Pojawiło się zatem pytanie o ich faktyczne wykorzystanie.

EIOD wziął również pod uwagę roczne sprawozdanie opublikowane przez Komisję dotyczące funkcjonowania Eurodac ([31]), a także statystyki opublikowane przez Komisję dotyczące wykorzystania systemu.



**W systemie Eurodac znajduje się ponad 250 tys. odcisków palców.**

## Nadzór nad jednostką centralną

W 2005 roku EIOD przeprowadził kontrolę sytuacji w zakresie bezpieczeństwa i ochrony danych w jednostce centralnej Eurodac. EIOD skontrolował pomieszczenia Eurodac (jednostkę centralną i system ciągłości działania) i przedłożył zestaw pytań. W sprawozdaniu wydanym w lutym 2006 roku ([32]) EIOD wydał szereg zaleceń w celu udoskonalenia systemu.

Drugi etap nadzoru Eurodac obejmujący szczegółowy audyt bezpieczeństwa rozpoczął się pod koniec września 2006 roku. Ma on na celu ocenę skuteczności wdrożonych środków bezpieczeństwa i środków z zakresu ochrony danych. W ramach zastosowania rozporządzenia 2004/46 EIOD zwrócił się do ENISA (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji) o zapewnienie kontaktów z ekspertami narodowymi w państwach członkowskich oraz doradztwa w dziedzinie metodologii audytu bezpieczeństwa. Utworzono zespół audytowy składający się z EIOD oraz z ekspertów z Niemiec i Francji. Na podstawie szczegółowej i interaktywnej prezentacji systemu i sytuacji przedstawionej przez helpdesk systemu Eurodac zespół audytowy przyjął metodologię IT-Grundschutz opracowaną przez BSI ([33]) (Bundesamt für Sicherheit in der Informationstechnik) w celu przeprowadzenia przedmiotowego audytu w ramach mandatu EIOD. Końcowego sprawozdania z audytu spodziewano się na wiosnę 2007 roku.

## Współpraca z krajowymi instytucjami nadzoru

EIOD i przedstawiciele krajowych organów ds. ochrony danych spotkali się już w 2005 roku, aby ustanowić pierwsze skoordynowane podejście do kwestii nadzoru: niektóre szczególne zagadnienia miałyby być badane na poziomie krajowym (wśród nich „wyszukiwania specjalne"), a wyniki takich badań byłyby przedstawiane we wspólnym sprawozdaniu. Takie krajowe badania prowadzono w 2006 roku w większości krajów uczestniczących w systemie Eurodac.

W dniu 28 czerwca 2006 roku EIOD zorganizował drugie spotkanie koordynujące dla krajowych organów ds. ochrony danych, którego tematem był wspólny nadzór Eurodac. Obecni byli przedstawiciele organów ds. ochrony danych z wszystkich państw członkowskich (a także Islandii i Norwegii) uczestniczących w systemie, jak również obserwatorzy ze Szwajcarii. EIOD przedstawił zarys sytuacji w dziedzinie nadzorowania systemu Eurodac z punktu widzenia poszcze-

([31]) Dokument roboczy służb Komisji: Trzecie sprawozdanie roczne dla Rady i Parlamentu Europejskiego na temat działalności jednostki centralnej Eurodac, SEC(2006) 1170.

([32]) Sprawozdanie z kontroli przeprowadzonej przez Europejskiego Inspektora Ochrony Danych w jednostce centralnej Eurodac, Bruksela, 27.2.2006.

([33]) http://www.bsi.de

gólnych zainteresowanych stron. Podkreślając, że „wyszukiwania specjalne" są przedmiotem kontroli poszczególnych instytucji, EIOD wspomniał, że w najbliższej przyszłości przewidywany jest przegląd rozporządzenia dotyczącego Eurodac. W razie potrzeby grupa mogłaby przedstawić zmiany do przedmiotowego rozporządzenia. EIOD przedstawił ustalenia pierwszej kontroli jednostki centralnej systemu Eurodac i zapowiedział szerszy audyt tej jednostki.

Omówiono również krajowe badania wszczęte po pierwszym spotkaniu koordynującym i wymieniono kilka bardzo interesujących ustaleń. Personel EIOD również nawiązywał dwustronne kontakty z krajowymi organami ds. ochrony danych w celu zapewnienia wytycznych dotyczących badań na poziomie krajowym lub odniesienia się do konkretnej sytuacji poszczególnych uczestników (nowych członków, członków lub obserwatorów o statusie specjalnym, takich jak Norwegia czy Szwajcaria).

**Czego można oczekiwać w 2007 roku?**

W 2007 roku powinny zakończyć się różne czynności prowadzone w obu obszarach nadzoru. Zaplanowane jest ukończenie audytu bezpieczeństwa i sprawozdanie końcowe na temat skoordynowanego nadzoru krajowego. Powinno się to zbiec z oceną całościową systemu dublińskiego, w tym Eurodac, którą Komisja ma sporządzić w kontekście pierwszej fazy europejskiej polityki azylowej. Aspekty dotyczące ochrony danych objęte nadzorem EIOD powinny stanowić przyczynek do oceny wartości dodanej wnoszonej przez system Eurodac, a jednocześnie zapewnić dalsze priorytetowe traktowanie kwestii ochrony danych przez poszczególne zainteresowane strony.

# 3. Konsultacje

## 3.1. Wprowadzenie

Rok 2006 był drugim pełnym rokiem funkcjonowania EIOD, również w odniesieniu do jego obowiązków doradczych wobec wspólnotowych instytucji w zakresie wniosków prawodawczych (i dokumentów pokrewnych). Był to ważny rok, w którym EIOD stanął w obliczu intensyfikacji prowadzonych przez siebie czynności i w którym w dalszym stopniu rozwijał i udoskonalał swoje działania. Można było to dostrzec w trzech kluczowych obszarach.

W dalszym ciągu rozwijano politykę konsultacji. W grudniu na stronie internetowej opublikowano spis zamierzeń na rok 2007. Obejmuje on część wprowadzającą, która zawiera krótką analizę najważniejszych tendencji i zagrożeń, jak również priorytetów na rok 2007. Zawiera on także załącznik z najistotniejszymi wnioskami Komisji Europejskiej, które już przyjęto lub które zostały zaplanowane i wymagają, lub też mogą wymagać, reakcji ze strony EIOD.

Liczba wydawanych opinii zwiększyła się; dotyczą one obecnie bardziej zróżnicowanych tematów. EIOD wydał w 2006 roku jedenaście opinii. Stanowi to blisko dwukrotny wzrost w porównaniu z liczbą opinii wydanych w roku poprzednim. Opinie te również odzwierciedlają istotne tematy zawarte w programach Komisji, Parlamentu Europejskiego i Rady dotyczących kierunków polityki. EIOD przedstawił opinie na temat wymiany informacji w ramach zasady dostępności, w dziedzinie wiz (w tym dostępu do obszernego Wizowego Systemu Informacyjnego (VIS)), paszportów i instrukcji konsularnych, a także na tematy finansowe.

EIOD stosował wielokrotnie inne instrumenty interwencyjne w zewnętrznych sytuacjach mających związek z prowadzoną przez niego działalnością. Dotyczyło to między innymi pojęcia interoperacyjności, rozwoju wydarzeń w dziedzinie przekazywania danych dotyczących przelotu pasażera (PNR) w wyniku wyroku Trybunału Sprawiedliwości w sprawie dotyczącej PNR ([34]), zatrzymywania danych o połączeniach, finalizacji ram prawnych dla systemu informacyjnego Schengen drugiej generacji oraz negocjacji w Radzie na temat wniosku dotyczącego decyzji ramowej w sprawie ochrony danych osobowych w trzecim filarze.

Wreszcie, niniejszy rozdział będzie nie tylko analizował działania z 2006 roku, ale również wybiegał w przyszłość. Przedstawiony zostanie w nim opis skutków, jakie dla EIOD ma rozwój nowych technologii oraz nowe wydarzenia w dziedzinie polityki i prawodawstwa.

## 3.2. Polityka konsultacyjna

### 3.2.1. Realizacja polityki konsultacyjnej

W dokumencie strategicznym zatytułowanym „EIOD jako doradca instytucji wspólnotowych w zakresie wniosków prawodawczych i dokumentów pokrewnych" ([35]) określono główne elementy metody, jaką EIOD zamierza zastosować w celu realizacji zadań powierzonych mu na mocy art. 28 ust. 2 i art. 41 rozporządzenia (WE) nr 45/2001.

([34]) Wyrok Trybunału z 30 maja 2006 r., Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04), sprawy połączone C-317/04 i C-318/04, Zb. Orz. 2006, str. I-4721.

([35]) Opublikowany w marcu 2005 roku; dostępny na stronie internetowej: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/21.

Realizacja przedmiotowego dokumentu strategicznego w 2006 roku wyraża się głównie w wynikach: opiniach wspomnianych w pkt 3.3 i innych czynnościach określonych w pkt 3.4. Ważnym krokiem naprzód był spis, o którym mowa w pkt 3.2.2.

Poza tym:

- służby Komisji Europejskiej zwykle zapraszają EIOD do udziału przed formalnym przyjęciem wniosku przez Komisję, co dość często przebiega równolegle z wewnętrznymi konsultacjami prowadzonymi między jej różnymi służbami. Na tym etapie EIOD zgłasza uwagi nieformalne;
- EIOD nawiązał również nieformalne kontakty z Radą, za pośrednictwem prezydencji i Sekretariatu Generalnego Rady. Kilkakrotnie EIOD wyjaśniał i omawiał swoje opinie z grupami roboczymi Rady zajmującymi się danym wnioskiem prawodawczym;
- takie same działania podjęto wobec Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych i innych komisji w Parlamencie Europejskim zajmujących się danym wnioskiem prawodawczym. EIOD nawiązał nieformalne kontakty z Parlamentem Europejskim – zarówno z posłami, jak i sekretariatami – chętnie uczestniczył również w ogólniejszych dyskusjach, na przykład podczas posiedzeń jawnych;
- funkcja doradcza EIOD staje się coraz bardziej oczywista dla instytucji. EIOD ze szczególnym zadowoleniem przyjmuje fakt, że Komisja wypracowała praktykę, zgodnie z którą wspomina o zasięganiu konsultacji EIOD w preambule przedstawianych przez siebie wniosków. Sprawia to, że zasięganie konsultacji EIOD jest lepiej widoczne dla opinii publicznej;
- szczególną uwagę poświęcono sposobowi doradzania Komisji w przypadkach niedotyczących przyjęcia wniosku (skierowanego do Rady lub Parlamentu Europejskiego), tylko podejmowanych przez nią samodzielnie decyzji. Taka sytuacja ma zastosowanie w przypadku wykonywania prawodawstwa przez Komisję (w ramach procedury komitologii lub nie), decyzji Komisji stwierdzających prawidłowy stopień ochrony w państwach trzecich zgodnie z art. 25 ust. 6 dyrektywy 95/46 lub gdy Komisja przedstawia komunikat. W tych przypadkach formalna opinia wydana po przyjęciu aktu przez Komisję nie może wpłynąć na tekst takiego aktu.

### 3.2.2. Spis

Ważnym elementem metody pracy opisanej we wspomnianym dokumencie strategicznym jest wybór i planowanie (w tym regularny przegląd tychże) niezbędny w celu skutecznego wypełniania funkcji doradcy. W sprawozdaniu rocznym EIOD za rok 2005 zapowiadano ustalenie priorytetów na nadchodzące lata w związku z priorytetami ustalonymi przez Komisję na 2006 rok. Stało się tak wraz z przygotowaniem i opublikowaniem na stronie internetowej w grudniu 2006 roku pierwszego spisu.

Spis taki będzie publikowany corocznie w grudniu i stanie się elementem rocznego cyklu pracy. Raz w roku EIOD składa retrospektywne sprawozdanie w formie sprawozdania rocznego; raz w roku w spisie przedstawiane są perspektywy na przyszłość. Głównym źródłem tego spisu jest program pracy Komisji, który jest zwykle publikowany co roku w październiku, oraz kilka związanych z nim dokumentów dotyczących planowania, opracowywanych przez Komisję. Spis na rok 2007 został przygotowany w ścisłej współpracy z zainteresowanymi stronami w Komisji.

Powyższy spis stanowił też przekonujące uzasadnienie potrzeby poszerzenia zakresu konsultacyjnej działalności EIOD, która do lata 2006 roku koncentrowała się głównie na dokumentach prawodawczych dotyczących przestrzeni wolności, bezpieczeństwa i sprawiedliwości, przy-

**Peter Hustinx podczas zebrania z personelem.**

gotowywanych w Komisji przez Dyrekcję Generalną ds. Sprawiedliwości, Wolności i Bezpieczeństwa. Przygotowywanie spisu wykorzystano jako okazję do wzmocnienia stosunków z Sekretariatem Generalnym Komisji, Dyrekcją Generalną ds. Społeczeństwa Informacyjnego i Mediów (INFSO) oraz Europejskim Urzędem ds. Zwalczania Nadużyć Finansowych (OLAF), a także do nawiązania stosunków z Dyrekcją Generalną ds. Zatrudnienia, Spraw Społecznych i Równości Szans (EMPL) oraz Dyrekcją Generalną ds. Zdrowia i Ochrony Konsumentów (SANCO). Wszystkie te podmioty uczestniczyły w opracowywaniu spisu.

Załącznik do spisu, w którym wymienia się najistotniejsze wnioski Komisji wymagające lub mogące wymagać reakcji EIOD, obejmuje:

- 16 tematów priorytetowych, odnośnie do których EIOD wyda opinię. Wspomniano o 20 innych tematach o mniejszym priorytecie, a EIOD może wydać opinię lub zareagować w inny sposób;
- 17 wniosków prawodawczych sensu stricto, 19 dokumentów pokrewnych (takich jak komunikaty wydane przez Komisję Europejską) ([36]);
- 11 (kompletów) dokumentów już przyjętych przez Komisję, przy czym pozostałe wymieniono w poszczególnych wykazach programowych.

## 3.3. Opinie na temat wniosków prawodawczych

### 3.3.1. Uwagi ogólne

Podobnie jak w 2005 roku, wnioski dotyczące przestrzeni wolności, bezpieczeństwa i sprawiedliwości – zarówno w ramach pierwszego filaru odnoszącego się do swobodnego przepływu osób i imigracji, jak i w ramach trzeciego filaru odnoszącego się do współpracy policyjnej i sądowej w sprawach karnych – stanowiły istotne źródło interwencji EIOD. EIOD opublikował również drugą opinię na temat wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach trzeciego filaru, która ma ustanowić nowy i konieczny element podstawowy ochrony danych na poziomie UE. Inne ważne wnioski o bardziej zasadniczym charakterze, które spotkały się z reakcją EIOD, obejmują wniosek w sprawie organizacji wymiany informacji pochodzących z rejestrów karnych pomiędzy państwami członkowskimi oraz treści tych informacji, a także wniosek dotyczący decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności.

Ponadto EIOD przeanalizował wnioski dotyczące dokumentów tożsamości i podróży. Wnioski odnoszące się do wspólnotowego dokumentu *laissez-passer* (paszport dyplomatyczny w państwach trzecich dla personelu i członków instytucji, którzy potrzebują takiego paszportu do pracy), jednolitego formatu zezwoleń na pobyt dla obywateli państw trzecich oraz zmiany wspólnych instrukcji konsularnych dla misji dyplomatycznych dotyczących wiz dały EIOD sposobność podkreślenia potrzeby posiadania szczególnych zabezpieczeń przy przetwarzaniu danych biometrycznych.

Ponadto EIOD doradzał w obszarach finansów, nadużyć i innych niezgodnych z prawem działań wywierających wpływ na wspólnotowy budżet. Wydał dwie opinie dotyczące nadużyć i innych niezgodnych z prawem działań: opinię na temat dochodzeń prowadzonych przez OLAF oraz opinię na temat wzajemnej pomocy administracyjnej do celów ochrony finansowych interesów Wspólnoty Europejskiej przed nadużyciami i innymi niezgodnymi z prawem działaniami. EIOD zareagował również na wnioski zmieniające rozporządzenie finansowe mające zastosowanie do budżetu ogólnego Wspólnot Europejskich i przepisów wykonawczych do tego rozporządzenia.

Wreszcie, wydano opinię na temat wniosku w sprawie wykonywania orzeczeń sądowych oraz współpracy w zakresie zobowiązań alimentacyjnych.

### 3.3.2. Zagadnienia horyzontalne

Przegląd jedenastu opinii prowadzi do następujących wniosków. Cztery opinie dotyczą wniosków w ramach trzeciego filaru, trzy opinie mają źródło w tytule IV Traktatu WE (dwie we wspólnej polityce wizowej i jedna we współpracy w dziedzinie prawa cywilnego), trzy opinie dotyczą zaś spraw leżących poza zakresem przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W większości przypadków EIOD poparł przedmiotowe wnioski, postulował jednak wprowadzenie szczególnych dodatkowych zabezpieczeń w zakresie ochrony danych.

([36]) Tematy mieszczą się w zakresie obowiązków 10 różnych dyrekcji generalnych lub podobnych podmiotów w Komisji.

Jednym z głównych powodów do niepokoju w trzecim filarze jest kolejność wniosków. EIOD sprzeciwia się przyjmowaniu prawodawstwa ułatwiającego wymianę danych przed zagwarantowaniem prawidłowego stopnia ochrony danych. Należy odwrócić tę kolejność. Ramy prawne ochrony danych stanowią niezbędny warunek wymiany danych osobowych przez organy ścigania, zgodnie z wymogiem art. 30 ust. 1 lit. b) Traktatu UE i założeniami szeregu dokumentów dotyczących kierunków polityki UE. Wspólne działania w zakresie gromadzenia, przechowywania, przetwarzania, analizowania i wymiany istotnych informacji podlegają właściwym przepisom o ochronie danych osobowych. Praktyka prawodawcza nie jest jednak zgodna z tym wymogiem.

EIOD kilkakrotnie poruszał kwestię danych biometrycznych wprowadzanych w konkretnych wnioskach Komisji. We wszystkich tych interwencjach EIOD podkreślił, że wprowadzaniu oraz przetwarzaniu danych biometrycznych muszą towarzyszyć szczególnie spójne i silne zabezpieczenia. Dane biometryczne są wysoce wrażliwe, a ich wprowadzanie stwarza szczególne zagrożenia, które należy minimalizować. Z uwagi na ich szczególny charakter EIOD raz jeszcze podkreślił znaczenie zastosowania podczas przetwarzania danych biometrycznych wszystkich koniecznych zabezpieczeń. Obowiązek wykorzystywania danych biometrycznych należy wprowadzić dopiero po dokładnej ocenie zagrożeń, powinien być on wynikiem procedury umożliwiającej pełną demokratyczną kontrolę. Takie podejście, rozwinięte w opinii na temat wniosków dotyczących systemu informacyjnego Schengen drugiej generacji (SIS II), powinno mieć zastosowanie do każdego systemu wykorzystującego biometrię, niezależnie od tego, czy dotyczy on wniosków w sprawie zezwoleń na pobyt, wspólnotowego dokumentu *laissez-passer,* czy też wiz dla misji dyplomatycznych.

Kolejny ważny temat przeanalizowany w opiniach EIOD w 2006 roku dotyczy baz danych, w szczególności ich ustanawiania oraz dostępu różnych organów do tych baz do konkretnych celów. Centralne bazy danych i obszerne systemy są obecnie w coraz powszechniejszym użyciu. W 2005 roku EIOD przeanalizował skutki prawne związane z rozwojem różnych obszernych systemów IT, kontynuował też działania w tym zakresie w 2006 roku. Stwierdzono, że każdorazowo należy właściwie i uważnie ocenić potrzebę posiadania tego typu baz danych. Ponadto, w chwili tworzenia takich baz danych należy wdrożyć konkretne zabezpieczenia w zakresie ochrony danych. Obowiązki prawne, które prowadzą do tworzenia istotnych baz danych, stwarzają szczególne zagrożenia dla podmiotów danych, między innymi z uwagi na zagrożenie nieuprawnionego użycia. Stopień ochrony danych musi być jednakowy, bez względu na rodzaj organu, który przegląda zawartość baz danych.

EIOD niejednokrotnie wyrażał zaniepokojenie brakiem zabezpieczeń w zakresie wymiany danych osobowych z państwami trzecimi. Kilka wniosków zawierało przepisy dotyczące takiej wymiany, a EIOD podkreślał, że należy wdrożyć mechanizmy zapewniające wspólne standardy i skoordynowane decyzje w sprawie zasadności wymiany danych. Wymiana danych z państwami trzecimi powinna być dozwolona wyłącznie w przypadku zapewnienia przez państwa trzecie prawidłowego stopnia ochrony danych osobowych lub w przypadku gdy dane przekazanie informacji jest objęte jednym z odstępstw określonych w dyrektywie 95/46/WE.

Wreszcie, jakość danych również stanowiła jeden z ważnych tematów horyzontalnych. Niezbędny jest wysoki poziom dokładności danych w celu uniknięcia niejasności treści przetwarzanych informacji. W związku z tym istotne jest regularne i właściwe sprawdzanie dokładności danych. Ponadto wysoki stopień jakości danych stanowi nie tylko jedną z podstawowych gwarancji dla podmiotu danych, ale ułatwia także osobom przetwarzającym dane skuteczne ich wykorzystywanie.

### 3.3.3. Poszczególne opinie ([37])

**Dostęp do VIS dla organów odpowiedzialnych za bezpieczeństwo wewnętrzne**

Opinia z 20 stycznia 2006 roku była reakcją na wniosek dotyczący decyzji Rady w sprawie wglądu do danych Wizowego systemu informacyjnego (VIS) dla organów państw członkowskich odpowiedzialnych za bezpieczeństwo wewnętrzne oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw.

System VIS jest opracowywany z myślą o stosowaniu europejskiej polityki wizowej. Powyższy wniosek wynika bezpośrednio z ustanowienia VIS, na temat którego EIOD wydał opinię 23 marca 2005

([37]) Zob. wykaz opinii na temat wniosków prawodawczych w załączniku G.

**Członkowie zespołu „Doradztwo" kończą prace nad wnioskiem legislacyjnym.**

roku. W tej opinii przewidywane już było założenie dotyczące dostępu organów ścigania do kilku obszernych systemów informacyjnych i identyfikacyjnych. W kolejnej opinii EIOD popiera zamysł, by organom ścigania można było udzielić dostępu do VIS wyłącznie w szczególnych okolicznościach, każdorazowo analizując potrzebę i proporcjonalność działania. Muszą temu towarzyszyć rygorystyczne zabezpieczenia. Innymi słowy, możliwość wglądu przez organy ścigania musi zostać ograniczona – za pomocą właściwych środków technicznych i prawnych – do określonych przypadków.

W opinii podkreślono, że w postulowanym akcie prawnym ochronie danych poświęca się znaczną uwagę, przede wszystkim przez ograniczenie dostępu do określonych przypadków i tylko w ramach walki z poważnymi przestępstwami. Niemniej jednak EIOD podkreślił również, że – w celu przyznania dostępu organom działającym w ramach trzeciego filaru – rozporządzenie podstawowe o VIS, będące aktem prawnym w obrębie pierwszego filaru, powinno przewidywać klauzulę pomostową. EIOD podkreślił także, że skoordynowane podejście do nadzoru należy zapewnić również w odniesieniu do dostępu do systemu VIS.

**Wymiana informacji w ramach zasady dostępności**

Zasada dostępności została wprowadzona w programie haskim w 2004 roku i stanowi, że informacje dostępne organom ochrony ścigania w jednym państwie członkowskim powinny zostać również udostępnione podobnym organom w pozostałych państwach członkowskich. Zasada ta stanowi ważne narzędzie rozwoju jednej przestrzeni wolności, bezpieczeństwa i sprawiedliwości, bez granic wewnętrznych. Wiąże się z nią wiele kwestii dotyczących ochrony danych, w szczególności z uwagi na wrażliwość danych oraz mniejszą kontrolę wykorzystywania informacji.

Wniosek dotyczący decyzji ramowej Rady czyni z tej zasady instrument prawodawczy. W swej opinii z 28 lutego 2006 roku EIOD analizuje wniosek również w kontekście innych instrumentów, które dotyczą wymiany informacji w procesie zwalczania poważnej przestępczości (takich jak konwencja z Prüm podpisana w maju 2005 roku przez siedem państw członkowskich). EIOD wykorzystał tę okazję do przedstawienia kilku ogólnych punktów widzenia w aktualnej debacie.

Wniosek odnosi się do takich tematów, jak dostępność dla policji w pozostałych państwach członkowskich informacji, którymi nie zawsze dysponuje policja w państwie członkowskim pochodzenia (takich jak dane telefoniczne czy dane dotyczące rejestracji pojazdów), warunki wprowadzenia systemu odnośników, a także wykorzystywanie profili DNA do celów wymiany informacji. W swej opinii EIOD opowiada się za stopniowym wprowadzaniem, zaczynając od jednego rodzaju danych (a nie sześciu, jak postuluje Komisja), dostępem pośrednim (odnośniki informacji, które nie są dostępne on-line) oraz systemem „trafienie / brak trafienia" co umożliwiłoby lepszą kontrolę wymiany informacji niż system oparty na dostępie bezpośrednim. Zasadnicze znaczenie ma, aby zasadę dostępności uzupełniały odpowiednie przepisy o ochronie danych w dziedzinie sprawiedliwości i współpracy policyjnej ([38]).

**Zobowiązania alimentacyjne**

W dniu 15 maja 2006 roku EIOD wydał opinię na temat wniosku dotyczącego rozporządzenia Rady w sprawie właściwości, prawa właściwego, uznawania i wykonywania orzeczeń sądowych oraz współpracy w zakresie zobowiązań alimentacyjnych. Wniosek ten odnosi się do złożonych realiów – alimenty mogą zostać przyznane dzieciom, rozwiedzionym małżonkom, rodzicom itp. Osoby, których to dotyczy, mogą mieszkać lub posiadać majątek w różnych państwach członkowskich.

([38]) W chwili pisania wydaje się oczywiste, że przedmiotowa decyzja ramowa jako taka nie zostanie przyjęta. Niemniej jednak nie ma to wpływu na wagę zasady dostępności dla wymiany informacji z zakresu ochrony porządku publicznego.

EIOD z zadowoleniem przyjmuje ten wniosek i uznaje znaczenie ułatwienia egzekucji transgranicznych należności z tytułu świadczeń alimentacyjnych w UE. Jednocześnie jednak należy przestrzegać zasad ochrony danych, takich jak ograniczenie celu, konieczność i proporcjonalność przetwarzanych danych, ograniczenia w wykorzystywaniu szczególnych kategorii danych, okresy przechowywania danych oraz informacje dla wierzyciela i dłużnika. Dla EIOD najistotniejsza jest kluczowa zasada, zgodnie z którą dane gromadzone do konkretnego celu nie powinny być wykorzystywane do innych celów, co byłoby skutkiem wniosku. Wyjątek od tej zasady jest dopuszczalny wyłącznie wtedy, gdy jest on proporcjonalny, niezbędny, określony przepisami prawa i możliwy do przewidzenia. W tym kontekście powyższy wniosek powinien przewidywać wyraźne i jednoznaczne obowiązki prawne.

**Rejestry karne**

W swej opinii z 29 maja 2006 roku EIOD z zadowoleniem przyjął kierunek polityki określony w postulowanej decyzji ramowej Rady w sprawie organizacji wymiany informacji pochodzących z rejestrów karnych pomiędzy państwami członkowskimi oraz treści tych informacji. Ponieważ jednak decyzja ramowa w sprawie ochrony danych w trzecim filarze nie została jeszcze przyjęta, nie istnieją żadne ogólne zabezpieczenia, co prowadzi do braku pewności prawnej dla europejskich obywateli. Zaledwie kilka artykułów we wniosku odnosi się do konkretnych sytuacji, nie zapewnia to jednak niezbędnej ochrony. W związku z tym EIOD zdecydowanie zalecił, by przedmiotowy wniosek nie wszedł w życie przed decyzją ramową w sprawie ochrony danych w trzecim filarze.

Szczególne uwagi EIOD dotyczą między innymi:

- właściwego rozwiązania przewidującego organ centralny, co zapewni jednoznaczne obowiązki w zakresie zarządzania informacjami oraz w zakresie nadzoru sprawowanego przez krajowe organy ds. ochrony danych;
- zalecenia jeszcze wyraźniejszego sprecyzowania, że skazujące państwo członkowskie uznaje się za „właściciela" danych osobowych oraz że państwo członkowskie osoby skazanej przechowuje dane w imieniu tego pierwszego;
- potrzeby opracowania bardziej precyzyjnych kryteriów przekazywania informacji osobowych do trzeciego państwa członkowskiego, do celów innych niż postępowanie karne;
- potrzeby skutecznego systemu językowego oraz opracowania znormalizowanego formatu wymiany informacji, który należy wprowadzić w terminie nieprzekraczającym roku.

***Laissez-passer***

W swej opinii z 13 października 2006 roku EIOD analizuje projekt rozporządzenia Rady w sprawie wspólnotowego *laissez-passer* (CLP) wydawanego członkom i personelowi instytucji, a wykorzystywanego jako paszport dyplomatyczny w państwach trzecich. Wprowadzony w Protokole w sprawie przywilejów i immunitetów Wspólnot Europejskich w 1965 roku i stosowany od 1967 roku dokument *laissez-passer* wymagał zmian w celu spełnienia aktualnych standardów bezpieczeństwa stawianych dokumentom podróży UE. Proponowana nowa wersja będzie zawierać elementy bezpieczeństwa, obejmuje również pewne nowe kategorie danych, takie jak dane biometryczne.

EIOD popiera wniosek, choć z pewnymi zastrzeżeniami, szczególnie w zakresie wykorzystywania danych biometrycznych. EIOD ponownie wyraża na przykład preferencję dla wykorzystywania procedur awaryjnych w trakcie procedury pobierania danych. Kolejnym przedmiotem niepokoju jest ewentualne utworzenie centralnych baz danych zawierających wszystkie dane biometryczne w CLP, co – zdaniem EIOD – nie byłoby środkiem proporcjonalnym. Ponadto z uwagi na fakt, że CLP ma być używany w państwach trzecich, należy zapewnić interoperacyjność systemów europejskich z systemami stosowanymi w państwach trzecich. W tym kontekście w opinii podkreśla się, że interoperacyjność systemów nie może naruszać zasady ograniczenia celu przetwarzania danych. Opinia odnosi się również do kwestii dostępu państw trzecich do danych.

Jako że wykorzystywanie danych biometrycznych może stwarzać zagrożenie dla zainteresowanych członków personelu, EIOD poinformował instytucje, że operacja przetwarzania będzie musiała podlegać procedurze kontroli wstępnej, zgodnie z art. 27 rozporządzenia (WE) nr 45/2001 ([39]).

**Zezwolenia na pobyt**

Po wprowadzeniu cech biometrycznych do paszportów europejskich i wiz strefy Schengen zmieniony wniosek

([39]) Więcej informacji – zob. pkt 2.3 dotyczący kontroli wstępnych.

dotyczący rozporządzenia Rady zmieniającego rozporządzenie (WE) nr 1030/2002 ustanawiające jednolity wzór dokumentów pobytowych dla obywateli państw trzecich jest trzecim wnioskiem zakładającym użycie danych biometrycznych. Wykorzystanie biometrii uzasadnia się zwiększeniem poziomu bezpieczeństwa i ułatwieniem zwalczania nielegalnej imigracji i nielegalnego pobytu.

W swej opinii z 16 października 2006 roku EIOD popiera wspomniany wniosek, podkreślając jednak, że zezwolenia na pobyt nie można postrzegać jako dokumentu podróży. Ponadto należy przyjąć najostrzejsze standardy bezpieczeństwa zgodnie z wymogami bezpieczeństwa przyjętymi przez państwa członkowskie pracujące nad dokumentem tożsamości w formie karty elektronicznej. EIOD nie sprzeciwia się wykorzystywaniu danych biometrycznych, o ile wdrażane są właściwe zabezpieczenia zalecane w opinii.

EIOD z zadowoleniem przyjmuje postępy osiągnięte na rzecz poszanowania zasady ograniczenia celu. Wyraża jednak zaniepokojenie faktem, że we wspomnianym wniosku nie określa i nie precyzuje się jednoznacznie organów mających dostęp do danych. EIOD z zadowoleniem przyjmuje założenie równego traktowania obywateli europejskich i rezydentów z państw trzecich przez umożliwienie im dostępu do usług elektronicznych, takich jak usługi e-administracji. Niemniej jednak włączenie dodatkowego mikroprocesora umożliwiającego korzystanie z takich usług należy odroczyć do czasu przeprowadzenia kompletnej oceny skutków.

**Dochodzenia prowadzone przez OLAF**

Opinia w sprawie wniosku dotyczącego rozporządzenia zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) została wydana 27 października 2006 roku. Powyższy wniosek zawiera zmiany do większości artykułów określających zasady operacyjne dla podmiotów uczestniczących w dochodzeniach prowadzonych przez OLAF i, jako taki, stanowi podstawę prawną czynności operacyjnych OLAF. Zasadnicze znaczenie ma zapewnienie przy tej okazji właściwego zabezpieczenia praw z zakresu ochrony danych i prywatności osób uczestniczących w takich dochodzeniach, osób podejrzewanych o naruszenie przepisów, a także członków personelu i innych osób fizycznych dostarczających OLAF informacji.

Postulowane zmiany mają na celu poprawę skuteczności i wydajności dochodzeń prowadzonych przez OLAF, ułatwienie wymiany informacji na temat podejrzewanych wykroczeń między OLAF a innymi organami, a także zagwarantowanie praw osób uczestniczących w dochodzeniu, w tym ich prawa do ochrony danych i prywatności. EIOD zgadza się co do znaczenia celów, jakie zamierza się osiągnąć w drodze postulowanych zmian, i z zadowoleniem przyjmuje wniosek, w szczególności zawarte w nim proceduralne gwarancje dla osób fizycznych. Wniosek można jednak jeszcze bardziej udoskonalić pod względem ochrony danych osobowych bez narażania celów, do których osiągnięcia dąży.

Opinia zwraca szczególną uwagę na zasadę jakości danych, prawo do informacji, prawo dostępu, prawo do sprostowania oraz na wymianę informacji osobowych. Postulowane są także środki dotyczące ochrony i poufności informatorów.

**Wspólne instrukcje konsularne (CCI)**

Opinia z 27 października 2006 roku odnosiła się do wniosku dotyczącego rozporządzenia zmieniającego wspólne instrukcje konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczące wiz w związku z wprowadzeniem technologii biometrycznych, łącznie z przepisami dotyczącymi organizacji przyjmowania i rozpatrywania wniosków wizowych. Główne punkty opinii dotyczą identyfikatorów biometrycznych i współpracy między urzędami konsularnymi w procedurze wizowej.

W odniesieniu do identyfikatorów biometrycznych EIOD podkreśla, że decyzja w sprawie określenia wieku, od którego pobierane są odciski palców, ma raczej charakter polityczny niż czysto techniczny. Nie powinna się ona opierać całkowicie na argumentach dotyczących wykonalności. Zwłaszcza obowiązkowe zdejmowanie odcisków palców wszystkich dzieci powyżej 6. roku życia budzi wątpliwości etyczne. EIOD przypomina ponadto, że wszystkie systemy identyfikacji biometrycznej są z natury niedoskonałe i że w związku z tym stosowny system musi przewidywać odpowiednie rozwiązania awaryjne.

W odniesieniu do współpracy między urzędami konsularnymi i ambasadami państw członkowskich EIOD podkreśla potrzebę zagwarantowania bezpieczeństwa danych, co w niektórych państwach trzecich może

okazać się trudne. W przypadku gdy rozpatrywanie wniosków wizowych, łącznie z gromadzeniem identyfikatorów biometrycznych, jest zlecane na zewnątrz prywatnemu przedsiębiorstwu, EIOD podkreśla potrzebę umieszczenia takiego podmiotu w miejscu objętym ochroną dyplomatyczną. W przeciwnym razie władze danego państwa trzeciego mogłyby uzyskać łatwy dostęp do danych dotyczących osób ubiegających się o wizę oraz ich kontaktów w UE. Mogłoby to się okazać niebezpieczne dla osób ubiegających się o wizę, na przykład w przypadku działaczy opozycji politycznej usiłujących wyjechać ze swojego kraju.

**Wzajemna pomoc administracyjna**

Zmieniony wniosek dotyczący rozporządzenia w sprawie wzajemnej pomocy administracyjnej w celu ochrony interesów finansowych Wspólnoty Europejskiej przed nadużyciami finansowymi i wszelkimi innymi działaniami niezgodnymi z prawem przedstawia procedury przekazywania informacji i procedury pomocy między Komisją a państwami członkowskimi. Obejmuje wzajemną pomoc administracyjną i wymianę informacji.

Wcześniejsza wersja wniosku z 2004 roku skutkowała przyjęciem pierwszej opinii EIOD na temat prawodawstwa wspólnotowego. W swej opinii z 13 listopada 2006 roku EIOD uznał, że ogólnie rzecz biorąc, zmieniony wniosek utrzymuje stopień ochrony danych osobowych zawarty w ogólnych ramach ochrony danych obowiązujących w UE. Wniosek nie zawiera nowych zasad dotyczących ochrony danych ani wyjątków w istniejących ramach ochrony danych, potwierdza jednak stosowanie tego prawodawstwa, a w pewnych obszarach wzywa do wprowadzenia regulacji wykonawczych, które będą się odnosić do kwestii ochrony danych. W związku z tym prawdziwą debatę na temat kwestii ochrony danych odkłada się na późniejszy etap. Ponieważ przepisy wykonawcze będą miały zasadnicze znaczenie dla ochrony danych osobowych w tym kontekście, EIOD ze szczególnym zadowoleniem przyjął włączenie obowiązku zasięgnięcia jego opinii przy opracowywaniu takiego prawodawstwa wykonawczego.

**Ochrona danych w trzecim filarze (druga opinia)**

W dniu 29 listopada 2006 roku EIOD po raz pierwszy wydał drugą opinię na temat wniosku dotyczącego prawodawstwa UE, odnoszącego się do decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Powód był dwojaki. Po pierwsze, decyzja ramowa w sprawie ochrony danych osobowych w trzecim filarze ma dla EIOD ogromne znaczenie. Po drugie, pojawiły się poważne obawy co do tego, że negocjacje w Radzie mogą doprowadzić do skreślenia lub znacznego osłabienia najistotniejszych zabezpieczeń dla obywateli. W związku z tym EIOD zalecił przedłużenie negocjacji w celu osiągnięcia rezultatu zapewniającego wystarczającą ochronę.

Najwięcej obaw wzbudzał fakt, że wniosek w formie, w jakiej był omawiany w Radzie, może doprowadzić do sztucznego podziału w plikach danych – na dane krajowe i dane pochodzące z innego państwa członkowskiego. Prowadziłoby to nie tylko do uciążliwego, skomplikowanego i kosztownego zarządzania, ale także do trudności w wykonywaniu przez obywateli należnych im praw. Ponadto EIOD był zaniepokojony możliwościami wymiany danych również z organami niebędącymi organami porządku publicznego i z podmiotami prywatnymi, ryzykiem braku wymogu „prawidłowego stopnia ochrony" przy wymianie danych z państwami trzecimi, jak również ryzykiem, że niektóre podstawowe prawa podmiotów danych, takie jak prawo do bycia informowanym, nie będą już zagwarantowane. Wyjątki od tego prawa mogą stać się regułą. W grudniu 2006 roku, po wydaniu opinii przez EIOD, stało się jasne, że wspomniany wniosek nie zostanie przyjęty i że poszukiwane są rozwiązania alternatywne.

**Rozporządzenie finansowe**

Wnioski dotyczące zmiany rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich oraz przepisów wykonawczych do tego rozporządzenia są istotne, ponieważ mają wpływ na sposób zarządzania danymi osobowymi osób fizycznych odnoszącymi się do czynności finansowych. Jednym z głównych punktów, jakie przewidują oba wnioski, jest 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 możliwość wymiany informacji zawartych w bazie danych z władzami na różnych szczeblach.

W swej opinii z 12 grudnia 2006 roku EIOD zgadza się z zasadą centralnej bazy danych w świetle przewidywanych celów przetwarzania danych. Niemniej

jednak podkreślił, że należy przestrzegać proaktywnego podejścia do praw podmiotów danych. To proaktywne podejście mogłoby polegać na wcześniejszym informowaniu podmiotów danych, w momencie gromadzenia ich 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. Ponadto EIOD podkreślił potrzebę wdrożenia określonych zabezpieczeń w świetle zasad ochrony danych do celów zdefiniowania kategorii podmiotów ujętych w bazie danych, określenia dokładnych ram czasowych dotyczących aktualizacji informacji, jak również zapewnienia odpowiedniej ochrony bazy danych. Ponadto, w odniesieniu do zasadności przekazywania danych osobowych innym państwom, EIOD nalegał na zapewnienie szczególnych zabezpieczeń w kontekście przekazywania danych osobowych z centralnej bazy danych oraz potwierdzanie otrzymywania danych osobowych z państw trzecich i organizacji międzynarodowych.

Wreszcie, przedmiotowe wnioski stanowiły także dla EIOD okazję do podkreślenia kwestii terminów przechowywania danych i kontroli budżetowej, w odniesieniu do których zasugerował zmianę zgodnie z rozporządzeniem (WE) nr 45/2001.

## 3.4. Inne rodzaje działalności

**Nadzór nad SIS II**

W dniu 19 października 2005 roku EIOD wydał opinię na temat wniosków dotyczących ustanowienia systemu informacyjnego Schengen drugiej generacji (SIS II). Jednym z tematów, którymi EIOD się zajmował, była kwestia obowiązkowego zapewnienia spójnego i kompleksowego nadzoru nad systemem zarówno na poziomie europejskim, jak i krajowym.

W styczniu 2006 roku EIOD odpowiedział na przedstawiony przez Parlament Europejski wniosek o poradę w sprawie sposobu jak najlepszej organizacji nadzoru nad systemem SIS II. W wyniku spotkania z udziałem przedstawicieli wspólnego organu nadzorczego systemu SIS opracowano model „skoordynowanego" nadzoru. Model taki został później ustanowiony w art. 44–46 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 roku w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) ([40]). Model ten jest również obecnie analizowany pod kątem zastosowania go w Wizowym systemie informacyjnym (VIS).

W marcu 2006 roku EIOD przesłał do prezydencji Rady pismo, w którym zwracał jej uwagę na problemy, jakie mogą się pojawić w świetle europejskiego prawa, gdyby zarządzanie systemem SIS II w okresie przejściowym zostało przez Komisję powierzone jednemu lub większej liczbie państw członkowskich, w szczególności w odniesieniu do skutecznego nadzoru nad obiektami centralnymi. Skutkowało to szczególnym przepisem w art. 47 rozporządzenia w sprawie ochrony danych w okresie przejściowym, zapewniając skuteczny nadzór ze strony EIOD.

**Uwagi na temat interoperacyjności**

W dniu 10 marca 2006 roku EIOD sformułował uwagi na temat komunikatu Komisji w sprawie interoperacyjności europejskich baz danych. W tym przypadku wybrano instrument o nieco mniejszym ciężarze gatunkowym niż opinia. Powyższe uwagi nie zostały, w przeciwieństwie do opinii, opublikowane w Dzienniku Urzędowym ani przetłumaczone na wszystkie języki Wspólnoty. Są one jednak dostępne do wiadomości publicznej na stronie internetowej.

EIOD kwestionuje jedno z istotniejszych założeń wspomnianego komunikatu, jakim jest stwierdzenie, że *interoperacyjność to pojęcie bardziej techniczne niż prawne czy polityczne.* Dla EIOD jest oczywiste, że jeśli dostęp do baz danych i wymiana danych między bazami danych staje się możliwa z technicznego punktu widzenia, to te środki techniczne zostaną wcześniej czy później zastosowane. Decydowanie o interoperacyjności wyłącznie w oparciu o uzasadnienie techniczne nie jest zatem neutralne. Ponadto EIOD sprzeciwia się jednej z bardziej szczegółowych propozycji w komunikacie – zastosowaniu biometrii jako podstawowego klucza – ponieważ dokładność biometrii jest przeceniana, a takie wykorzystanie ułatwiłoby nieuzasadnione łączenie baz danych.

**Wizowy system informacyjny (VIS)**

W dniu 23 marca 2005 roku EIOD wydał opinię na temat wniosku dotyczącego rozporządzenia w sprawie Wizowego systemu informacyjnego (VIS) oraz

([40]) Dz.U. L 381 z 28.12.2006, str. 4–23. Zob. również pkt 4.3 w niniejszym sprawozdaniu rocznym.

wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych. W 2006 roku EIOD uważnie śledził prace nad tym wnioskiem prowadzone w Parlamencie i Radzie.

W maju 2006 roku przewodniczący grupy roboczej Rady zajmującej się tym wnioskiem zwrócił się do EIOD o konsultację w sprawie wielu analizowanych zmian, w szczególności w zakresie niewłaściwego używania wiz. W czerwcu 2006 roku EIOD wyraził uznanie w związku ze zwróceniem się z wnioskiem o konsultację w tej kwestii na tym etapie. Niemniej jednak wyraził również poważne wątpliwości odnośnie do tego, czy wspomniane zmiany są odpowiednie zarówno z punktu widzenia ochrony danych, jak i w kontekście wspólnej polityki wizowej.

**Kwestie związane z danymi dotyczącymi przelotu pasażera (PNR)**

Wyrok Trybunału Sprawiedliwości z 30 maja 2006 roku, w którym unieważniona została umowa w sprawie PNR ze Stanami Zjednoczonymi, miała duży wpływ na działania EIOD.

Były to pierwsze sprawy, w których EIOD wykorzystał przysługujące mu uprawnienia do interwencji. EIOD udzielił poparcia wnioskom Parlamentu, zgodnie z którymi należało unieważnić zarówno umowę z USA, jak i decyzję Komisji. Trybunał zadecydował o unieważnieniu decyzji Rady i Komisji, na których opierał się dostęp władz USA do danych dotyczących przelotu pasażera (danych PNR) będących w dyspozycji europejskich linii lotniczych. Trybunał orzekł, że wybrana została błędna podstawa prawna, ponieważ operacje przetwarzania dotyczą bezpieczeństwa publicznego i działań objętych prawem karnym, w związku z czym nie są one objęte dyrektywą 95/46/WE. Dla Trybunału nie jest istotne, że dane zostały pierwotnie zgromadzone do celów handlowych (transportu lotniczego pasażerów). Trybunał nie oceniał przedstawionych przez EIOD i inne strony argumentów odnoszących się do ochrony praw podstawowych.

Niemniej jednak EIOD uważa ten wyrok za istotny z punktu widzenia ochrony danych, ponieważ ma on wpływ na zakres zastosowania dyrektywy 95/46/WE. Wspomniana dyrektywa nie ma zastosowania w sytuacjach, gdy dostęp do danych jest przyznawany prywatnym przedsiębiorstwom do celów egzekwowania prawa. Ta konsekwencja powyższego wyroku może spowodować stworzenie luki w ochronie Europejczyków.

Wyrok zawierał wymóg zawarcia nowej (tymczasowej) umowy ze Stanami Zjednoczonymi, którą podpisano w październiku 2006 roku i która wygaśnie do lipca 2007 roku. EIOD nie uczestniczył w negocjacjach prowadzących do tej tymczasowej umowy ani formalnie nie doradzał w tym zakresie, również dlatego, że celem negocjacji ze strony europejskiej było osiągnięcie porozumienia w sprawie tymczasowej umowy, której istota była identyczna z istotą unieważnionej umowy. Nowa umowa na okres po wygaśnięciu umowy tymczasowej będzie miała całkowicie inny charakter. Przygotowania do takiej nowej umowy, uważnie obserwowane przez EIOD, rozpoczęły się już w 2006 roku, przejawiając się między innymi wnioskiem Komisji w sprawie mandatu negocjacyjnego ([41]).

Ponadto w 2006 roku EIOD w inny sposób wyraził swoje poglądy na temat wymiany ze Stanami Zjednoczonymi danych dotyczących pasażerów. Wydał komunikat prasowy krótko po ogłoszeniu wyroku. Omawiał również tę kwestię z instytucjami europejskimi odpowiedzialnymi za negocjacje i uczestniczył w dyskusjach Komisji LIBE Parlamentu Europejskiego. Ponadto EIOD brał aktywny udział w działaniach podejmowanych w tych kwestiach w ramach grupy roboczej art. 29.

**Zatrzymywanie danych o połączeniach**

W lipcu 2006 roku przed Trybunał Sprawiedliwości trafiła nowa sprawa, która mogła rzucić nowe światło na konsekwencje wyroku w sprawie PNR, w szczególności na kwestię luki prawnej. W sprawie C-301/06, Irlandia przeciwko Parlamentowi Europejskiemu i Radzie, zagrożona jest ważność dyrektywy 2006/24/WE ([42]) w sprawie zatrzymywania danych z tego powodu, że w ramach trzeciego filaru nie istniałaby żadna podstawa prawna, która zobowiązywałaby prywatne przedsiębiorstwa do gromadzenia i przechowywania danych z zakresu łączności do celów egzekwowania prawa.

W październiku 2006 roku EIOD zwrócił się do Trybunału z prośbą o umożliwienie mu interweniowania, w ramach poparcia wniosków pozwanych, głównie z uwagi na to, że ta sprawa daje możliwość sprecyzowania wyroku Trybunału w sprawach dotyczących

([41]) Nie jest to dokument publiczny.

([42]) Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE.

PNR. Stanowisko to nie oznacza, że EIOD zmienia swą krytyczną ocenę na temat istoty wspomnianej dyrektywy ([43]).

**SWIFT**

Kwestia dostępu organów egzekwowania prawa do baz danych utworzonych przez podmioty prywatne została również podniesiona w sprawie przypadków poufnego przekazywania amerykańskim władzom danych bankowych europejskich obywateli za pośrednictwem Towarzystwa Światowej Finansowej Telekomunikacji Międzybankowej (SWIFT). EIOD przeprowadził postępowanie wyjaśniające i wydał opinię na temat roli Europejskiego Banku Centralnego w tej sprawie (zob. pkt 2.5); aktywnie uczestniczył też w opracowaniu opinii przyjętej przez grupę roboczą art. 29 w listopadzie 2006 roku.

**Publiczny dostęp do dokumentów**

W marcu 2006 roku, opowiadając się za wnioskami odwołujących się stron, EIOD zdecydował o interweniowaniu w trzech sprawach przed Sądem Pierwszej Instancji na temat stosunku, jaki istnieje między publicznym dostępem do dokumentów a ochroną danych ([44]). Stanowiło to sposobność do rozwinięcia tego tematu w świetle dokumentu bazowego zatytułowanego „Publiczny dostęp do dokumentów a ochrona danych", opublikowanego w lipcu 2005 roku ([45]).

## 3.5. Nowe wydarzenia

### 3.5.1. Rozwój technologiczny

**Technologie wspomagające na potrzeby prywatności i ochrony danych**

Instytucje europejskie stale inwestują w badania, wdrażanie i stosowanie nowych technologii w celu stworzenia konkurencyjnego europejskiego społeczeństwa informacyjnego zgodnie z programem lizbońskim. Europejskie społeczeństwo informacyjne będzie jednak miało charakter trwały tylko wówczas, gdy te technologie będą właściwie opracowane i wdrażane w sposób efektywnie przyczyniający się do rozwoju europejskich ram z zakresu ochrony danych oraz do tworzenia bezpieczniejszego środowiska.

EIOD z zadowoleniem przyjął komunikat Komisji zatytułowany „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego" ([46]), opublikowany w 2006 roku, w szczególności następującą zawartą w nim wizję: „Życie codzienne umożliwiające swobodne wzajemne łączenie się i przekazywanie danych między sieciami oferuje szerokie możliwości. Z drugiej jednak strony będzie wiązać się również z dodatkowym ryzykiem w zakresie bezpieczeństwa i ochrony prywatności". Należy zatem w trybie pilnym określić najlepsze dostępne techniki (BAT), które mogą efektywnie przyczynić się do realizacji wymogów związanych z uregulowaniem i bezpieczeństwem ochrony danych. Wybór tych technik, o ile będą one często poddawane przeglądowi, wzmocni model symbiozy wymogów dotyczących prywatności i bezpieczeństwa opracowywany przez Unię Europejską.

W poprzednim sprawozdaniu rocznym EIOD określił nowe wydarzenia z zakresu rozwoju technologii, takie jak systemy identyfikacji radiowej (RFID), biometria i systemy zarządzania tożsamością, których oczekiwany wpływ na ochronę danych będzie znaczny. Właściwe określenie najlepszych dostępnych technik w zakresie prywatności i bezpieczeństwa w odniesieniu do tych wydarzeń będzie mieć decydujące znaczenie dla ich przyjęcia przez użytkownika, jak również dla konkurencyjności przemysłu europejskiego.

W ramach wspólnej inicjatywy, w której uczestniczył EIOD w listopadzie ubiegłego roku w trakcie Międzynarodowej Konferencji Komisarzy ds. Ochrony Danych i Prywatności w Londynie ([47]), zasugerowano przeprowadzenie paraleli między ochroną indywidualnych swobód a ochroną środowiska. „Ochrona prywatności i danych może być równie cenna jak powietrze, którym oddychamy: oba te elementy są niewidoczne, ale kiedy ich zabraknie, skutki mogą być równie katastrofalne". Na podstawie tej paraleli kontrolę można porównać z zanieczyszczeniem, a

([43]) Zob. opinia EIOD z 26 września 2005 r. na temat stosownego wniosku Komisji.

([44]) Sprawy T-170/03 (British American Tobacco przeciwko Komisji), T-161/04 (Valero Jordana przeciwko Komisji) i T-194/04 (Bavarian Lager przeciwko Komisji). Posiedzenie jawne w tej trzeciej sprawie odbyło się we wrześniu 2006 roku; zgłoszono wtedy ustne uwagi w imieniu EIOD. W lutym 2007 roku nie było jeszcze rozstrzygnięcia w tej sprawie. Zob. również pkt 2.7 w niniejszym sprawozdaniu rocznym.

([45]) Dostępny na stronie internetowej: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/21.

([46]) Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy", COM(2006) 251.

([47]) Zob. pkt 4.5 i 5.1 w niniejszym sprawozdaniu rocznym.

wiedza fachowa wypracowana przez UE w zakresie zapobiegania zanieczyszczeniom i ich kontroli ([48]) – z wykorzystaniem koncepcji BAT, mogłaby stanowić cenne doświadczenie w łagodzeniu zagrożeń związanych ze społeczeństwem kontrolowanym (ang. *surveillance society*).

**Śledzenie rozwoju technologicznego, który ma wpływ na ochronę prywatności i danych jest częścią misji EIOD.**

**Badania i rozwój na potrzeby prywatności i ochrony danych**

Wymogi związane z ochroną prywatności i danych muszą być stosowane na możliwie wczesnym etapie w cyklu życia nowych technologii. EIOD uważa, że zasada uwzględniania poszanowania prywatności od samego początku (ang. *privacy by design*) powinna stanowić nieodłączny element działań prowadzonych przez UE w zakresie badań i rozwoju. Pod koniec 2006 roku Komisja ogłosiła i uruchomiła 7. program ramowy w zakresie badań i rozwoju (7. PR) ([49]), którego najważniejszy element zostanie poświęcony technologiom społeczeństwa informacyjnego. Aby uważnie obserwować przebieg 7. PR, EIOD podjął w pierwszej kolejności decyzję o aktywnym udziale w imprezie inaugurującej, konferencji IST 2006 zorganizowanej w Helsinkach, wzywając do:

- określenia na początkowym etapie kształtujących się tendencji, które będą stymulować wspomniane ambitne działania w ramach badań i rozwoju;
- nawiązania owocnych kontaktów z podmiotami realizującymi przyszłe projekty badawcze;
- zwiększania świadomości głównych zainteresowanych stron w zakresie ewentualnych aspektów ochrony danych w ich przyszłych projektach badawczych;
- korzystania z jego doradztwa w sprawie sposobu uwzględnienia obaw związanych z ochroną danych w przyszłych wnioskach i działaniach w zakresie badań.

Na podstawie tych pierwszych doświadczeń EIOD opracuje kilka modeli udziału w ukierunkowanych projektach badawczych w ramach 7. PR. Można spodziewać się opinii na temat zastosowanych metodologii lub uzyskanych wyników. Projekty badawcze realizowane w ramach 7. PR zazwyczaj muszą obejmować partnerów pochodzących z kilku państw członkowskich. EIOD również i w tym przypadku mógłby mieć udział we współpracy między odpowiednimi zainteresowanymi organami ochrony danych.

### 3.5.2. Nowe wydarzenia w polityce i prawodawstwie

Spis na 2007 rok przedstawia ogólny przegląd najważniejszych tendencji i zagrożeń związanych z ochroną danych, które prawdopodobnie będą miały wpływ na działania EIOD w zakresie konsultacji, a także wymienia priorytety działań EIOD. Opiera się on na sprawozdaniu rocznym za 2005 rok.

**Przestrzeń wolności, bezpieczeństwa i sprawiedliwości**

Sytuacja w zakresie przestrzeni wolności, bezpieczeństwa i sprawiedliwości (w szerszym sensie, łącznie z tytułem VI Traktatu UE) szybko się zmieniała. Pod sam koniec 2006 roku ogłoszono cele niemieckiej prezydencji Rady, a w styczniu 2007 roku stały się one jeszcze bardziej precyzyjne. Większa potrzeba prze-

([48]) http://eippcb.jrc.es/
([49]) http://cordis.europa.eu/fp7/home_en.html

chowywania i wymiany danych osobowych do celów egzekwowania prawa, o której mowa w spisie na 2007 rok, odgrywa jeszcze istotniejszą rolę. Z tego powodu prezydencja przewiduje złożenie formalnego wniosku o transpozycję traktatu z Prüm do instrumentów prawodawstwa UE.

Taki ruch umożliwiłby organom państw członkowskich UE udzielanie sobie wzajemnego automatycznego dostępu do danych genetycznych, danych o odciskach palców i wykroczeniach drogowych. Zakłada on również obowiązki przechowywania (i wymiany) informacji osobowych, takich jak DNA, co mieści się w drugiej tendencji związanej z coraz powszechniejszym wykorzystaniem biometrii. Ponadto trzecią stałą tendencją jest tworzenie i doskonalenie baz danych na poziomie europejskim, wspierających wymianę między państwami członkowskimi, takich jak SIS II, VIS oraz system informacyjny Europolu. Czwartą tendencją, o której należy wspomnieć, jest większy nacisk na dostęp do danych osobowych i ich wykorzystanie do celów egzekwowania prawa, w przypadku gdy dane te zostały pierwotnie zgromadzone do innych celów. Zapowiedziano wniosek mający również na celu otwarcie do celów egzekwowania prawa baz danych Eurodac utworzonych w ramach pierwszego filaru. Wnioski o tego rodzaju dostęp także stwarzają szczególne trudności, co wynika z opartej na filarach struktury Traktatu UE i nadrzędnej roli ochrony przewidzianej w ramach pierwszego filaru ([50]).

Zdaniem EIOD tendencje te wymagają ustanowienia odpowiednich ram dla ochrony danych w trzecim filarze, w tym zasad dotyczących skutecznego podziału obowiązków i nadzoru nad stosownymi podmiotami. Niezadowalające postępy w negocjacjach w sprawie decyzji ramowej Rady nadal będą wymagać uwagi ze strony EIOD.

**Inne obszary wymagające szczególnej uwagi**

- Łączność elektroniczna i społeczeństwo informacyjne (Dyrekcja Generalna ds. Społeczeństwa Informacyjnego i Mediów – DG INFSO)

W krótkiej perspektywie zasadniczym punktem odniesienia będzie przegląd ram regulacyjnych UE (w tym dyrektywy 2002/58/WE). Długofalowo rysuje się perspektywa społeczeństwa informacyjnego, w którym każdego będzie można śledzić, na przykład ze względu na rosnące znaczenie identyfikacji radiowej (RFID).

- Zdrowie publiczne (Dyrekcja Generalna ds. Zdrowia i Ochrony Konsumentów – DG SANCO)

Istnieje ogólna tendencja do intensyfikacji gromadzenia i wymiany informacji związanych ze zdrowiem, co ze swej natury (dane dotyczące zdrowia są danymi wrażliwymi) stwarza zagrożenie dla podmiotów danych. Ta tendencja jest jeszcze bardziej istotna w świetle rosnącej digitalizacji danych dotyczących zdrowia oraz w świetle pojęcia wykrywalności.

- Kwestie związane z pracą (Dyrekcja Generalna ds. Zatrudnienia, Spraw Społecznych i Równości Szans – DG EMPL)

Należy w większym stopniu zbadać potrzebę dysponowania specjalnym systemem ochrony danych w miejscu pracy, oddzielnie zaś – kwestię wymiany informacji dotyczących opieki społecznej w ramach ściślejszej współpracy w UE.

- Zwalczanie nadużyć finansowych (OLAF)

OLAF ma dla EIOD szczególne znaczenie, ponieważ jest to organ wspólnotowy nadzorowany przez EIOD, z uprawnieniami wykonawczymi w państwach członkowskich. OLAF wymienia dane z organami ścigania państw członkowskich, organami na poziomie UE, takimi jak Europol, a także z państwami trzecimi i organizacjami międzynarodowymi. Wymiana taka wymaga zabezpieczeń, w tym w zakresie skutecznego nadzoru.

- Kwestie przejrzystości (Sekretariat Generalny Komisji)

Inicjatywy miały na celu zmianę rozporządzenia (WE) nr 1049/2001 w sprawie publicznego dostępu do dokumentów; musi ono precyzować związek między publicznym dostępem a ochroną danych. EIOD zamierza wydać opinię i doradzać instytucjom, w odpowiednich przypadkach, przed przyjęciem stosownych wniosków Komisji i po ich przyjęciu. Wyniki spraw będących w toku przed Sądem Pierwszej Instancji (zob. pkt 3.4) mogą mieć w tym kontekście znaczenie.

**Konsolidacja i udoskonalenie**

Metody pracy EIOD zostaną skonsolidowane i wprowadzone we wszystkich obszarach polityki UE. Dyrekcja Generalna ds. Energii i Transportu będzie kolejną służbą Komisji, z którą EIOD nawiąże współpracę, co wynika z działań prawodawczych w sprawie skomputeryzowanych systemów rezerwacji dla

([50]) Artykuł 47 Traktatu UE.

transportu lotniczego. Celem EIOD jest nawiązanie dobrych stosunków roboczych ze wszystkimi służbami Komisji do końca 2007 roku w zakresie istotnym z punktu widzenia powierzonych mu zadań. EIOD będzie bazował na wewnętrznych komunikatach Komisji wydawanych przez Sekretarza Generalnego Komisji i urzędnika ds. ochrony danych, podkreślających kompetencje EIOD. Będzie się zwracać uwagę na szczególne aspekty decyzji Komisji (zob. również pkt 3.2.1).

Wzmocnione zostaną też stosunki z Radą i Parlamentem Europejskim w celu zwiększenia skuteczności EIOD po przyjęciu opinii. EIOD zamierza bazować na istniejących dobrych relacjach i pozytywnych doświadczeniach.

# 4. Współpraca

## 4.1. Grupa robocza art. 29

Grupę roboczą art. 29 utworzono na mocy art. 29 dyrektywy 95/46/WE. Jest to niezależny organ doradczy ds. ochrony danych osobowych w zakresie wspomnianej dyrektywy ([51]). Zadania grupy zostały określone w art. 30 dyrektywy i w skrócie można je przedstawić następująco:

- dostarczanie Komisji fachowych opinii państw członkowskich na temat zagadnień związanych z ochroną danych;
- promowanie jednolitego stosowania ogólnych zasad przedmiotowej dyrektywy we wszystkich państwach członkowskich przez współpracę między organami nadzoru w zakresie ochrony danych;
- doradzanie Komisji w sprawie wszelkich wspólnotowych środków mających wpływ na prawa i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych;
- formułowanie zaleceń przeznaczonych dla ogółu społeczeństwa, w szczególności dla instytucji Wspólnoty, w kwestiach dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie Europejskiej.

EIOD jest członkiem grupy roboczej art. 29 od początków 2004 roku. Artykuł 46 lit. g) rozporządzenia (WE) nr 45/2001 przewiduje, że EIOD bierze udział w działalności grupy roboczej. EIOD uważa, że jest to bardzo ważna platforma współpracy z krajowymi instytucjami nadzoru. Jest również oczywiste, że grupa robocza powinna odgrywać jedną z głównych ról w jednolitym stosowaniu dyrektywy oraz w interpretacji jej ogólnych zasad.

W kwietniu 2006 roku, przyjmując swój program pracy na lata 2006–2007, grupa robocza podjęła istotną decyzję ([52]) przy zdecydowanym poparciu ze strony EIOD. Grupa postanowiła skoncentrować się na ograniczonej liczbie kwestii strategicznych, mając na celu wniesienie wkładu we wspólną interpretację kluczowych przepisów dyrektyw 95/46/WE i 2002/28/WE oraz zapewnienie ich lepszego wykonania.

Zgodnie z powyższym programem grupa robocza odnosi się do tematów, które wymagają odrębnej uwagi, takich jak oddziaływanie identyfikacji radiowej (RFID) i zarządzania tożsamością, szczególnie w zakresie e-administracji i akt pacjentów w ramach e-zdrowia. Jednocześnie grupa robocza opracowała lepszą wspólną interpretację kluczowych pojęć, takich jak „dane osobowe" i „wyrażenie zgody", oraz specjalne zasady przetwarzania danych medycznych w art. 2 i 8 dyrektywy 95/46/WE. EIOD z uwagą uczestniczył w tych czynnościach i oczekuje ich wyników w 2007 roku.

W 2006 roku EIOD brał również udział w działaniach grupy roboczej w dziedzinie przekazywania danych państwom trzecim. Dotyczyło to w szczególności kwestii danych pasażerów linii lotniczych, w świetle wyroku Europejskiego Trybunału Sprawiedliwości w sprawach dotyczących PNR, oraz wynikającej stąd potrzeby negocjacji ze Stanami Zjednoczonymi (zob. pkt 3.4). Na tej podstawie grupa robocza opracowała zarys długoterminowej strategii i przyjęła rozmaite opinie ([53]) na temat kwestii pokrewnych:

- opinia 5/2006 na temat orzeczenia Europejskiego Trybunału Sprawiedliwości z dnia 30 maja 2006 r. w sprawach połączonych C-317/04 i C-318/04

([51]) W skład grupy roboczej wchodzą przedstawiciele krajowych organów nadzoru z każdego państwa członkowskiego, przedstawiciel organu ustanowionego dla instytucji i organów wspólnotowych (tj. EIOD) oraz przedstawiciel Komisji. Komisja zapewnia również sekretariat na potrzeby grupy roboczej. Krajowe organy nadzoru z Islandii, Norwegii i Liechtensteinu (jako partnerzy w ramach EOG) uczestniczą w obradach w charakterze obserwatorów.

([52]) Program pracy na lata 2006–2007, przyjęty 5 kwietnia 2006 r. (WP 120). Dostępny na stronie internetowej: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm.

([53]) Te i inne opinie grupy roboczej wspomniane w niniejszym rozdziale są dostępne z tego samego odnośnika co program pracy.

w sprawie przekazywania Stanom Zjednoczonym danych dotyczących przelotu pasażera (PNR), przyjęta 14 czerwca 2006 r. (WP 122);
- opinia 7/2006 na temat orzeczenia Europejskiego Trybunału Sprawiedliwości z dnia 30 maja 2006 r. w sprawach połączonych C-317/04 i C-318/04 w sprawie przekazywania Stanom Zjednoczonym danych dotyczących przelotu pasażera (PNR) oraz pilnej potrzeby zawarcia nowej umowy, przyjęta 27 września 2006 r. (WP 124);
- opinia 9/2006 na temat wykonania dyrektywy Rady 2004/82/WE w sprawie zobowiązania przewoźników do przekazywania danych pasażerów, przyjęta 27 września 2006 r. (WP 127).

Grupa robocza wydała kilka opinii na temat wniosków prawodawczych. W kilku przypadkach wnioski te były przedmiotem opinii EIOD na podstawie art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. Opinia EIOD jest obowiązkowym elementem procesu prawodawczego UE, ale opinie grupy roboczej oczywiście również są niezwykle przydatne, w szczególności z uwagi na fakt, że mogą one zawierać dodatkowe punkty wymagające uwagi widziane z perspektywy krajowej.

W związku z tym EIOD z zadowoleniem przyjmuje opinie grupy roboczej art. 29, które jak dotąd były w dużym stopniu zbieżne z opiniami przyjmowanymi przez EIOD. W kolejnym przypadku EIOD preferował ściślejszą współpracę w zakresie jednej opinii, bez zgłaszania własnych uwag. Oto przykłady dobrej synergii między grupą roboczą a EIOD w tej dziedzinie:
- opinia 3/2006 na temat dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE, przyjęta 25 marca 2006 r. (WP 119) ([54]);
- opinia 6/2006 na temat wniosku dotyczącego rozporządzenia Rady w sprawie właściwości, prawa właściwego, uznawania i wykonywania orzeczeń sądowych oraz współpracy w zakresie zobowiązań alimentacyjnych, przyjęta 9 sierpnia 2006 r. (WP 123) ([55]);
- opinia 8/2006 na temat przeglądu ram regulacyjnych dla łączności i usług elektronicznych, z naciskiem na dyrektywę o prywatności i łączności elektronicznej (*e-privacy directive*), przyjęta 26 września 2006 r. (WP 126).

EIOD brał również czynny udział w przygotowaniu opinii podkreślających znaczenie stosownych przepisów w ramach europejskiego systemu ochrony danych w różnych obszarach, takich jak:
- opinia 1/2006 na temat zastosowania zasad UE dotyczących ochrony danych do wewnętrznych systemów powiadamiania o nieprawidłowościach (ang. *whistle blowing schemes*) w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania łapownictwa, przestępczości bankowej i finansowej, przyjęta 1 lutego 2006 r. (WP 117);
- opinia 2/2006 na temat zagadnień prywatności związanych ze świadczeniem usług monitorowania wiadomości elektronicznych, przyjęta 21 lutego 2006 r. (WP 118).

Zgodnie z art. 46 lit. f) ppkt (i) rozporządzenia (WE) nr 45/2001 EIOD musi również współpracować z krajowymi instytucjami nadzoru w stopniu koniecznym do wykonywania ich obowiązków, w szczególności przez wymianę wszystkich użytecznych informacji i żądanie lub świadczenie innej pomocy w zakresie wykonywania powierzonych im zadań. Współpraca taka odbywa się stosownie do poszczególnych przypadków. Przypadek dotyczący SWIFT był przykładem wielostronnej współpracy, w której grupa robocza art. 29 ([56]) odegrała bardzo przydatną rolę (zob. również pkt 2.5).

Bezpośrednia współpraca z organami krajowymi staje się coraz istotniejsza w kontekście międzynarodowych systemów, takich jak Eurodac czy proponowany Wizowy system informacyjny (VIS), które wymagają skutecznego wspólnego nadzoru (zob. pkt 2.9).

## 4.2. Grupa Robocza Rady ds. Ochrony Danych

Prezydencja austriacka postanowiła zwołać dwa posiedzenia Grupy Roboczej Rady ds. Ochrony Danych. Jednym z celów było wznowienie dyskusji na temat

([54]) W tej opinii ponownie sformułowano zasadnicze zabezpieczenia w zakresie zatrzymywania danych o połączeniach, po przyjęciu dyrektywy 2006/24/WE, do analizy na poziomie krajowym w celu wykonania dyrektywy. Zob. również opinia EIOD z 26 września 2005 r. na temat wniosku Komisji.

([55]) Zob. również opinia EIOD wydana 15 maja 2006 r.

([56]) Zob. opinia 10/2006 na temat przetwarzania danych osobowych przez Towarzystwo Światowej Finansowej Telekomunikacji Bankowej (SWIFT), przyjęta 22 listopada 2006 r. (WP 128).

roli tej grupy roboczej w przyszłości, nie zapominając przy tym, że w przeszłości zajmowała się ona fundamentami polityki WE w dziedzinie ochrony danych, takimi jak dyrektywa 95/46/WE, dyrektywa 97/66/WE i rozporządzenie (WE) nr 45/2001. Prezydencja fińska poparła tę inicjatywę i jesienią 2006 roku zwołała trzecie posiedzenie.

EIOD z zadowoleniem przyjął tę inicjatywę, postrzegając ją jako użyteczną sposobność zapewnienia bardziej horyzontalnego podejścia do spraw pierwszego filaru. W trakcie drugiego posiedzenia przedstawił sprawozdanie roczne za 2005 rok. Na trzecim posiedzeniu EIOD przedstawił w zarysie swoje działania związane z pełnioną funkcją doradczą w zakresie wniosków dotyczących nowego prawodawstwa.

Prezydencja niemiecka postanowiła na tej samej zasadzie kontynuować dyskusje na temat ewentualnych inicjatyw Komisji i innych stosownych tematów w kontekście pierwszego filaru. EIOD będzie z ogromnym zainteresowaniem śledził te działania, w stosownych przypadkach pozostaje również do dyspozycji w kwestii doradzania i współpracy.


**Peter Hustinx podczas konferencji prasowej.**

## 4.3. Trzeci filar

Artykuł 46 lit f) ppkt (ii) rozporządzenia (WE) nr 45/2001 przewiduje, że EIOD współpracuje z organami nadzoru w dziedzinie ochrony danych ustanowionymi na mocy tytułu VI Traktatu UE („trzeci filar"), mając na względzie „poprawę spójności i zastosowania reguł i procedur, za zapewnienie zgodności z którymi są odpowiednio odpowiedzialne". Te organy nadzoru to wspólne organy nadzoru (JSB) dla Schengen, Europolu, Eurojustu i Systemu informacji celnej (CIS). W skład większości tych organów wchodzą – częściowo ci sami – przedstawiciele krajowych instytucji nadzoru. W praktyce współpraca odbywa się z udziałem stosownych wspólnych organów nadzoru (JSB), wspieranych przez wspólny sekretariat ds. ochrony danych przy Radzie, a bardziej ogólnie z udziałem krajowych organów ds. ochrony danych.

Potrzeba ściślejszej współpracy między krajowymi organami ds. ochrony danych a EIOD stała się w ostatnich latach oczywista dzięki stałemu zwiększaniu liczby inicjatyw na poziomie europejskim w celu zwalczania przestępczości zorganizowanej i terroryzmu, w tym różnych wniosków dotyczących wymiany danych osobowych.

W 2006 roku najwięcej uwagi poświęcono dwóm stosownym wnioskom omawianym w Radzie. Pierwszy to wniosek Komisji dotyczący decyzji ramowej w sprawie ochrony danych w trzecim filarze, na temat którego EIOD wydał opinię 19 grudnia 2005 roku. W dniu 24 stycznia 2006 roku Konferencja europejskich organów ochrony danych również przyjęła opinię, która była zbieżna z opinią EIOD. Drugi to wniosek Komisji dotyczący decyzji ramowej w sprawie wymiany informacji zgodnie z zasadą dostępności, na temat którego EIOD wydał opinię 28 lutego 2006 roku (zob. pkt 3.3.3) ([57]). Oba wnioski były ze sobą powiązane, co oznaczało, że przyjęcie pierwszego wniosku było warunkiem koniecznym do przyjęcia drugiego.

Na Konferencji europejskich organów ochrony danych, która odbyła się w dniach 24–25 kwietnia 2006 roku w Budapeszcie (zob. pkt 4.4), przyjęto

([57]) Zob. A Framework in Development: Third Pillar and Data Protection, opublikowane w: „Ochrona danych osobowych wczoraj, dziś, jutro / Personal Data Protection Yesterday, Today, Tomorrow", Warszawa 2006, str. 132–137 (w języku angielskim) i str. 137–142 (w języku polskim). Dostępne również na stronie internetowej EIOD (12 maja): http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/23.

deklarację. Przypomina ona państwom członkowskim, że wymiana informacji osobowych między ich organami ścigania jest dozwolona wyłącznie na podstawie zasad ochrony danych zapewniających wysoki i zharmonizowany standard ochrony danych na poziomie europejskim i we wszystkich uczestniczących państwach. W przeciwnym razie różne poziomy ochrony i brak wspólnych zasad dotyczących kontroli dostępu do informacji mogłyby prowadzić do sytuacji, w których nie przestrzega się minimalnych standardów ochrony danych. Jak już wskazano na powyższej konferencji w 2005 roku, istniejące instrumenty prawne obowiązujące w UE w zakresie ochrony danych są zbyt ogólne, aby zapewnić skuteczną ochronę danych w dziedzinie egzekwowania prawa.

W związku z tym na konferencji z zadowoleniem przyjęto propozycję Komisji dotyczącą zharmonizowania i wzmocnienia ochrony danych w zakresie działań organów policyjnych i sądowych przez ustanowienie zabezpieczeń ochrony danych w trzecim filarze, które należy stosować przy wymianie informacji na podstawie zasady dostępności. Podkreślono również, że nie ma alternatywnego rozwiązania dla stworzenia wysokiego i zharmonizowanego standardu ochrony danych w trzecim filarze UE. Jest to konsekwencją programu haskiego, zgodnie z którym zabezpieczenie wolności, bezpieczeństwa i sprawiedliwości to element nierozerwalnie związany z całą Unią Europejską ([58]).

Niemniej jednak wydawało się, że nie wszystkie państwa członkowskie popierają to podejście ([59]). W związku z tym postępy Rady w zakresie niezbędnych ram ochrony danych dla trzeciego filaru są niezadowalające pomimo starań podejmowanych przez kolejne prezydencje. Jednocześnie nastąpił znaczny postęp w dziedzinie inicjatyw promujących i ułatwiających wymianę informacji ([60]). W dniu 29 listopada 2006 roku EIOD wydał drugą opinię na temat ram dotyczących ochrony danych, przestrzegając Radę przed ograniczaniem praw obywatelskich w ramach ochrony danych w trzecim filarze (zob. pkt 3.3).

W Budapeszcie postanowiono także powierzyć Grupie Roboczej ds. Współpracy Policyjnej, wspieranej przez sekretariat ochrony danych, zadanie przeanalizowania kilku kwestii i złożenia stosownego sprawozdania na następnej konferencji, która odbędzie się wiosną przyszłego roku. Obejmowało to różne zagadnienia związane z zakresem i konsekwencjami zasady dostępności, jak również potrzebę dodatkowych zabezpieczeń. Wymagało to także opracowania wniosków w celu dalszej harmonizacji metod postępowania w poszczególnych państwach członkowskich w zakresie prawa dostępu.

**Schengen i Europol**

Współpraca EIOD ze wspólnym organem nadzorczym (JSA) Schengen zaowocowała w styczniu 2006 roku modelem „skoordynowanego" nadzoru nad SIS II. Model ten został obecnie określony w 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) ([61]).

W dniu 26 czerwca 2006 roku wspólny organ nadzorczy (JSB) Europol wydał opinię na temat wniosku dotyczącego decyzji Rady w sprawie wglądu do danych Wizowego systemu informacyjnego dla organów państw członkowskich odpowiedzialnych za bezpieczeństwo wewnętrzne oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw. Opinia ta podkreśla kilka punktów, które zostały również podniesione w opinii EIOD z 20 stycznia 2006 roku (zob. pkt 3.3.3), skupia się jednak w większym stopniu na stanowisku Europolu.

EIOD korzystał również ze ścisłej współpracy z JSB Europol i sekretariatem ochrony danych w zakresie analizy projektu wniosku dotyczącego decyzji Rady ustanawiającej Europejski Urząd Policji (EUROPOL), przyjętego przez Komisję w grudniu 2006 roku. Wniosek ten ma na celu zapewnienie Europolowi nowej i bardziej elastycznej podstawy prawnej w ramach prawa UE oraz zastąpienie istniejącej konwencji

([58]) Przesłanie to zostało powtórzone w oświadczeniu europejskich organów ochrony danych przyjętym w Londynie 2 listopada 2006 r. Oba oświadczenia są dostępne na stronie internetowej EIOD: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51.

([59]) Zob. również: Izba Lordów, Komisja ds. Unii Europejskiej, „Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm", sprawozdanie wraz z uzasadnieniem, lipiec 2006, zawierające między innymi oświadczenia EIOD (ustne uzasadnienie w dniu 6 czerwca 2006 r.).

([60]) Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz.U. L 386, str. 89). Zob. również inicjatywy prezydencji niemieckiej w zakresie transpozycji traktatu z Prüm do ram prawnych UE, co będzie przedmiotem analizy EIOD w 2007 roku.

([61]) Zob. również pkt 3.4 w niniejszym sprawozdaniu rocznym.

o Europolu. W dniu 16 lutego 2007 roku EIOD wydał opinię na temat powyższego wniosku.

## 4.4. Konferencja europejska

Przedstawiciele instytucji ochrony danych z państw członkowskich UE i Rady Europy co roku spotykają się na wiosennej konferencji w celu omówienia spraw będących przedmiotem wspólnego zainteresowania oraz w celu wymiany informacji i doświadczeń dotyczących zróżnicowanej tematyki. W dniach 24–25 kwietnia 2006 roku EIOD i jego zastępca wzięli udział w konferencji w Budapeszcie, której gospodarzem był węgierski komisarz ds. ochrony danych i wolności informacji. Konferencja ta zbiegła się z 10. rocznicą funkcjonowania węgierskiej instytucji ochrony danych ([62]). András Baka, węgierski sędzia w Europejskim Trybunale Praw Człowieka, przedstawił uwagi wprowadzające na temat orzecznictwa Trybunału w sprawie ochrony danych i wolności informacji.

EIOD wniósł konkretny wkład w prace sesji, koncentrując się na ochronie danych w trzecim filarze. Zastępca EIOD przemawiał w czasie sesji na temat „Powiadamiania o nieprawidłowościach i granic uczciwości", czerpiąc z doświadczeń instytucji UE, w szczególności OLAF-u. Inne tematy, które omawiano w trakcie konferencji, obejmowały: „Identyfikację radiową i lokalizację położenia", „Badania historyczne i naukowe", „Krajowe bazy danych dotyczących zdrowia", „Dane genetyczne" oraz „Skuteczność komisarzy". Na konferencji przyjęto także kilka istotnych dokumentów (zob. pkt 4.4).

Kolejna konferencja europejska zostanie zorganizowana w Larnace (Cypr) w dniach 10–11 maja 2007 roku, zostaną na niej podsumowane stosowne zagadnienia wymagające uwagi.

## 4.5. Konferencja międzynarodowa

Przedstawiciele instytucji ochrony danych oraz komisarze ds. prywatności z Europy i innych części świata, w tym Kanady, Ameryki Łacińskiej, Australii, Nowej Zelandii, Hongkongu, Japonii i innych jurysdykcji w regionie Azji/Pacyfiku od wielu lat spotykają się corocznie jesienią na konferencji. W dniach 2–3 listopada 2006 roku w Londynie odbyła się 28. Międzynarodowa konferencja komisarzy ds. ochrony danych i prywatności, w której uczestniczyli delegaci z 58 krajów z całego świata.

Konferencja ta miała niezwykły charakter z tego powodu, że była w całości poświęcona jednemu, bardzo ważnemu zagadnieniu: „społeczeństwu kontrolowanemu". Komisarz ds. informacji ze Zjednoczonego Królestwa zlecił również opracowanie sprawozdania wprowadzającego na ten temat, które zostało przygotowane przez brytyjskich badaczy we współpracy z Surveillance Studies Network ([63]). Pierwszy dzień konferencji obejmował prezentacje z rozmaitych perspektyw, natomiast drugi dzień poświęcono analizie i dyskusji między uczestnikami; odbyła się również sesja zamknięta dla komisarzy w celu wyciągnięcia wniosków.

W komunikacie końcowym komisarze zaakcentowali kilka tematów:

- *Społeczeństwo kontrolowane już istnieje.* Nadzór obejmuje celowe, rutynowe i systematyczne rejestrowanie za pośrednictwem środków technologicznych ruchów i działań osób fizycznych w miejscach publicznych i prywatnych. W życiu codziennym już teraz jest na to wiele przykładów.

- *Działania związane z nadzorem mogą być podejmowane w dobrej wierze i mogą przynosić korzyści.* Jak dotąd rozwój tych działań w społeczeństwach demokratycznych postępuje w sposób stosunkowo łagodny i stopniowy – nie wynika też z dążenia rządów lub przedsiębiorstw, by za wszelką cenę ingerować w życie jednostek w nieuzasadniony sposób.

- *Jednak niewidoczny, niekontrolowany lub nadmierny nadzór stwarza również zagrożenia, które wykraczają daleko poza naruszenie prywatności.* Może on sprzyjać atmosferze podejrzliwości i osłabiać zaufanie. Gromadzenie i wykorzystywanie dużej ilości informacji osobowych przez organizacje publiczne i prywatne skutkuje decyzjami, które wywierają bezpośredni wpływ na ludzkie życie.

([62]) Zob. „Adequate Protection" – Opinion 6/99 of the Article 29 Working Party revisited, opublikowano w: „Tízéves az Adatvédelmi Biztos Irodája / Ten years of DP & FOI Commissioner's Office" (Dziesięć lat Biura Komisarza ds. Ochrony Danych i Wolności Informacji), Budapeszt 2006, str. 79–87 (w języku węgierskim) i str. 251–259 (w języku angielskim). Dostępne również na stronie internetowej EIOD (27 kwietnia 2006 r.): http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/26.

([63]) Zob. dokumenty dostępne na stronie internetowej EIOD: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51.

- *Uregulowania dotyczące ochrony prywatności i danych stanowią istotne zabezpieczenie, nie są jednak jedynym rozwiązaniem.* Konsekwencje nadzorowania osób fizycznych nie tylko prowadzą do ograniczenia ich prywatności. Mogą mieć one również wpływ na ich możliwości, życiowe szanse i styl życia. Nadmierny nadzór wywiera również wpływ na sam charakter społeczeństwa.

- *Należy przyjąć przepisy w zakresie systematycznego wykorzystywania ocen oddziaływania.* Takie oceny obejmowałyby oceny oddziaływania na aspekt prywatności, miałyby jednak szerszy niż te ostatnie zakres, określając także oddziaływanie społeczne i możliwości zminimalizowania niepożądanych skutków dla osób i społeczeństwa.

- *Odnośne zagadnienia obejmują szeroki wachlarz tematyczny, a dalsze prace w tej dziedzinie nie mogą być kontynuowane tylko przez organy regulacyjne zajmujące się ochroną danych lub prywatnością.* Zaangażowanie się w tę kwestię powinno stanowić wspólną sprawę wszystkich stron zainteresowanych rozwojem sytuacji w tej dziedzinie. Komisarze powinni współpracować z organizacjami społeczeństwa obywatelskiego i rządami, sektorem prywatnym, wybieranymi przedstawicielami i samymi osobami fizycznymi na rzecz ochrony przed nieuzasadnionymi skutkami.

- *Zaufanie publiczne ma znaczenie nadrzędne.* Pomimo faktu, że znaczna część infrastruktury związanej ze społeczeństwem kontrolowanym została zbudowana w dobrych zamiarach, nie można przyjmować stałego zaufania publicznego za pewnik. Ludzie muszą mieć pewność, że każda ingerencja w ich życie jest podyktowana koniecznością i jest proporcjonalna do realizowanych celów.

EIOD jest oddany kontynuacji tego procesu. Stanowiło to podstawę jego współpracy w ramach inicjatywy londyńskiej – „Przekazywanie informacji na temat ochrony danych i zwiększanie jego efektywności" – omówionej w pkt 5.1.

Kolejna konferencja międzynarodowa odbędzie się w Montrealu w dniach 26–28 września 2007 roku, jej tematem przewodnim będą „Perspektywy prywatności: terra incognita".

# 5. Komunikacja

## 5.1. Wprowadzenie

Ochrona prywatności i danych osobowych dotyczy ludzi. Sposób postrzegania tych praw może się różnić w zależności od osoby, ponieważ oba pojęcia są z natury rzeczy związane z rodzajem społeczeństwa, w którym żyjemy – każde z nich ma własną historię i kulturę – oraz z osobistymi doświadczeniami życiowymi każdego z nas. Pomimo to, każdy ma te same prawa podstawowe, a prawa te nakładają pewne warunki ([64]), które przedstawiciele polityczni i decydenci są zobowiązani szanować, kiedy przyjmują lub proponują nowe środki wywierające wpływ na życie osobiste lub na sposób gromadzenia i wykorzystywania danych osobowych. Dlatego zasadnicze znaczenie ma, aby decydenci byli świadomi skutków i pola manewru, jakim dysponują.

Przepisy prawne dotyczące prywatności i ochrony danych osobowych przewidują także szczególne prawa i obowiązki na bardziej praktycznym poziomie. Prawo podmiotów danych do dostępu do danych i ich sprostowania albo prawo do wyrażenia sprzeciwu lub wstrzymania zgody na przetwarzanie danych osobowych ma również istotne znaczenie dla instytucji i organów UE. Podobnie jest z obowiązkiem dopilnowania, aby dane osobowe były przetwarzane wyłącznie w uzasadnionych przypadkach i zgodnie z prawem, aby zapewniono podmiotom danych odpowiednią przejrzystość i aby stosowano wystarczające środki bezpieczeństwa. W tym kontekście jest również bardzo istotne, aby wszystkie zainteresowane strony były świadome swoich praw i obowiązków, a także praktycznego znaczenia tych praw i obowiązków w ważnych dla nich sytuacjach. Ochrona prywatności i danych osobowych może stać się rzeczywistością tylko wtedy, gdy w praktyce przestrzegane będą stosowne zasady.

Badania sugerują, że Europejczycy w dalszym ciągu interesują się kwestią prywatności i bezpieczeństwa swych informacji osobowych ([65]). Ma to bardzo duże znaczenie w społeczeństwie, które w coraz większym stopniu staje się zależne od wykorzystania technologii informacyjno-komunikacyjnych. W wielu dziedzinach życia, w domu, w pracy, na zakupach, korzystając z telefonu komórkowego lub surfując w Internecie, większość ludzi zbiera i wymienia informacje, pozostawiając za sobą wiele osobistych śladów. Pomimo to wiele osób nie dostrzega praktycznej zależności między tym zjawiskiem a potrzebą ciągłej ochrony swej prywatności i informacji osobowych, a przede wszystkim nie dostrzega znaczenia tego w codziennym życiu każdego z nich. To tu właśnie komunikacja odgrywa kluczową rolę jako potężny środek zwiększania świadomości i informowania społeczeństwa o metodach radzenia sobie z tym zjawiskiem w sposób odpowiedzialny i jak najlepszego wykorzystania swych praw. Często określa się to krótko jako „upodmiotowienie".

Na 28. Międzynarodowej konferencji ([66]) komisarzy ds. ochrony danych i prywatności w Londynie przedstawiono oświadczenie ([67]) zatytułowane „Przekazywanie informacji na temat ochrony danych i zwiększanie jej efektywności", które spotkało się z ogólnym poparciem ze strony organów ochrony danych na całym świecie. Była to wspólna inicjatywa przewodniczącego

([64]) Zob. np. art. 8 Europejskiej konwencji praw człowieka, art. 7–8 Karty Praw Podstawowych UE, dyrektywa 95/46/WE i rozporządzenie (WE) nr 45/2001. Zob. również decyzję ETS z dnia 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 (Österreichischer Rundfunk).

([65]) Zob. np. Specjalny Eurobarometr 2003 oraz badanie brytyjskiego komisarza ds. informacji na temat rocznych postępów w latach 2004–2006.

([66]) Zob. również pkt 4.5 w niniejszym sprawozdaniu rocznym.

([67]) Dostępny na stronie internetowej: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51.

francuskiej instytucji ds. ochrony danych, brytyjskiego komisarza ds. informacji oraz EIOD (zwana również obecnie „inicjatywą londyńską"). Jako jeden z architektów wspomnianej inicjatywy, EIOD będzie aktywnie uczestniczył w monitorowaniu stosownych działań wraz z krajowymi organami ds. ochrony danych oraz wymieniał zdobyte doświadczenia i najlepsze praktyki.

Oto niektóre z ważniejszych punktów inicjatywy londyńskiej:

- *Ochrona prywatności i danych osobowych obywateli ma zasadnicze znaczenie* w każdym demokratycznym społeczeństwie, na równi z wolnością prasy czy swobodą przemieszczania się. Ochrona prywatności i danych może być w rzeczywistości równie cenna jak powietrze, którym oddychamy: oba te elementy są niewidoczne, ale kiedy ich zabraknie, skutki mogą być równie katastrofalne.
- *Komisarze powinni opracować nową strategię komunikacji* w celu lepszego uświadomienia społeczeństwu i stosownym zainteresowanym stronom należnych im praw i ich znaczenia. Komisarze powinni zainicjować długoterminowe kampanie na wielką skalę na rzecz zwiększenia świadomości społecznej i ocenić skutki tych działań.
- *Komisarze powinni również skuteczniej przekazywać informacje* dotyczące swej działalności i skonkretyzować ochronę danych. Tylko wtedy gdy działania te będą zrozumiałe, dostępne i istotne dla ogółu społeczeństwa, możliwe będzie uzyskanie kontroli niezbędnej do tego, aby wywierać wpływ na opinię publiczną i aby głos komisarzy został usłyszany przez decydentów.
- *Komisarze powinni oceniać swoją skuteczność i efektywność* i, w razie potrzeby, odpowiednio dostosowywać swoje działania. Należy im przyznać wystarczające uprawnienia i zasoby, powinni oni jednak również korzystać z nich w sposób selektywny i pragmatyczny, koncentrując się na poważnych i prawdopodobnych szkodach lub głównych rodzajach ryzyka dla osób fizycznych.

>>>

<<<

- *Komisarze powinni wzmocnić swoje zdolności w obszarach technologicznych* z myślą o zaawansowanych badaniach, ekspertyzach i interwencjach, w ścisłym powiązaniu z badaniami i sektorem nowych technologii, a także we wzajemnej współpracy. Należy skorygować nadmiernie „prawny" wizerunek kwestii ochrony danych.
- *Komisarze powinni propagować udział innych zainteresowanych stron* w dziedzinie ochrony danych i prywatności na poziomie krajowym lub międzynarodowym, takich jak społeczeństwo obywatelskie i organizacje pozarządowe, w celu rozwijania, w stosownych przypadkach, strategicznych partnerstw z myślą o poprawie skuteczności swej pracy.

Komisarze podejmą się realizacji programu działań następczych zgodnie z powyższymi wytycznymi, a na kolejnej międzynarodowej konferencji przeanalizują i ocenią poczynione postępy.

## 5.2. Główne działania i adresaci

W 2006 roku działania w zakresie komunikacji na poziomie UE w dalszym ciągu koncentrowały się na trzech głównych działaniach – nadzorze, konsultacji i współpracy; każde z nich było skierowane do innego adresata. Jako że EIOD i jego zastępca pełnią swoje funkcje od ponad dwóch lat, mniej pracy niż w latach poprzednich poświęcono zwiększaniu świadomości na temat samej instytucji pośród innych instytucji. Zamiast tego skupiono się na konkretnych zagadnieniach, które były przedmiotem uwagi.

### Nadzór

W odniesieniu do zadania polegającego na dopilnowaniu, aby instytucje i organy WE przestrzegały swych obowiązków związanych z ochroną danych, określono dwóch następujących adresatów:

- Społeczeństwo: podmioty danych ogółem, w szczególności personel instytucji i organów WE. Odnosi się to do „aspektu praw" ([68]), a nacisk kładzie się na wzmocnienie pozycji podmiotów danych przez

([68]) Zob. art. 13–19 rozporządzenia (WE) nr 45/2001 (prawa podmiotów danych).

dbanie o to, aby byli oni właściwie informowani o operacjach przetwarzania, które ich dotyczą, jak również o przysługujących im prawach dostępu, do sprostowania, blokowania itp.

- System instytucjonalny: koncentruje się na obowiązkach ([69]) tych podmiotów, które są z administracyjnego punktu widzenia odpowiedzialne za operacje przetwarzania. W instytucjach i organach WE są to administratorzy danych oraz urzędnicy ds. ochrony danych (DPO). Z uwagi na wielkość instytucji Komisja Europejska wprowadziła również dodatkowy poziom – koordynatora ds. ochrony danych (DPC) – który wypełnia w drodze delegacji swoje obowiązki w dyrekcjach generalnych Komisji.

Z punktu widzenia „aspektu praw", w uzupełnieniu obowiązku administratora danych polegającego na informowaniu podmiotów danych o wszelkich operacjach przetwarzania, prowadzone były wielorakie działania natury bardziej ogólnej. Jako przykład może posłużyć wywiad oraz inne publikacje w cotygodniowej gazetce wewnętrznej Komisji, drukowanej w ponad 50 tys. egzemplarzy i rozprowadzanej także wśród personelu innych instytucji.

Z punktu widzenia „aspektu obowiązków" komunikacja koncentrowała się w głównej mierze na regularnych spotkaniach z siecią DPO. Niemniej jednak odbywały się również spotkania z udziałem innych kluczowych podmiotów, takie jak spotkanie EIOD z sekretarzem generalnym i dyrektorami generalnymi Komisji w celu omówienia postępów w realizacji środków dotyczących ochrony danych.

**Konsultacje**

W odniesieniu do zadania polegającego na propagowaniu właściwej ochrony danych w nowym prawodawstwie i nowych politykach – adresatów można określić jako „zainteresowane podmioty polityczne w UE". Doradztwo EIOD jest w związku z tym na pierwszym etapie skierowane do Komisji, a na drugim – do Parlamentu Europejskiego i Rady. Po wysłaniu danej opinii do poszczególnych zainteresowanych stron i opublikowaniu jej na stronie internetowej EIOD zwykle przedstawia swoje poglądy na forum stosownych komisji Parlamentu Europejskiego (np. LIBE) albo stosownej grupy roboczej lub komitetu sterującego Rady (np. Komitet art. 36).

([69]) Zob. art. 4–12 rozporządzenia (WE) nr 45/2001 (zasady legalności przetwarzania danych, przekazywanie informacji podmiotowi danych).

Opinie prawodawcze są generalnie podawane do wiadomości publicznej wraz z komunikatem prasowym przesyłanym do około 100 stałych przedstawicieli mediów. Często skutkuje to pojawianiem się relacji w mediach, podobnie jak udział w posiedzeniach wspomnianych komisji lub komitetów, które mają charakter jawny, w związku z czym często uczestniczą w nich dziennikarze. Większość próśb dotyczących udzielenia wywiadu (zob. pkt 5.6) dotyczy funkcji konsultacyjnej, a przychylanie się do takich próśb jest kolejnym sposobem propagowania opinii EIOD.

**Współpraca**

Współpraca z „kolegami zajmującymi się ochroną danych" w całej Europie, jak również na szerszym forum międzynarodowym ma na celu propagowanie spójnego stopnia ochrony danych. Dotyczy to systemów informacyjnych, odnośnie do których EIOD wykonuje część swej funkcji nadzorczej, jak ma to miejsce w przypadku Eurodac. Dotyczy to jednak także wymiany doświadczeń i najlepszych praktyk w zakresie rozpatrywania spraw zarówno dwustronnie, jak i zbiorowo, z innymi organami ochrony danych.

Komunikacja w takich sytuacjach jest często zintegrowana z innymi czynnościami lub też jest prowadzona wspólnie z innymi zainteresowanymi podmiotami. Jako przykład może posłużyć współpraca w ramach grupy roboczej art. 29 lub w ramach Międzynarodowej konferencji komisarzy ds. ochrony danych i prywatności w Londynie, gdzie organizatorzy podjęli udaną inicjatywę w zakresie kontaktów z mediami.

## 5.3. Strona internetowa

Strona internetowa jest najważniejszym narzędziem komunikacyjnym EIOD. Jej pierwsza wersja została opracowana w pierwszej połowie 2004 roku, a jej podstawowa struktura była raczej prosta. Dodano nowe części i nowe rodzaje dokumentów; znacznie zwiększyła się też liczba dokumentów w formacie umożliwiającym ich pobranie. Przed nadejściem jesieni 2005 roku w ogólnym odczuciu bliski był kres naturalnych możliwości tej strony. Rozpoczęto więc realizację projektu mającego na celu opracowanie strony internetowej drugiej generacji; prace nad tym projektem trwały przez cały 2006 rok. Stworzono nową strukturę zbudowaną wokół trzech głównych zadań oraz nową szatę graficzną. Zaangażowano podwykonawcę

do przeprowadzenia analizy przygotowawczej oraz wykonania strony w ścisłej współpracy z Parlamentem Europejskim. Strona internetowa drugiej generacji została udostępniona w lutym 2007 roku, z pewnym opóźnieniem w stosunku do planowanego terminu. Dalsze jej funkcje będą opracowywane w 2007 roku.

W 2006 roku liczba wizyt na stronie nadal zwiększała się – z 1000 do 1500 wizyt tygodniowo. Liczba odsłon zwiększyła się po dodaniu na stronie wielu nowych dokumentów. Dodanie komunikatów prasowych również przyczyniło się do zwiększenia liczby wizyt. Oczekuje się, że uruchomienie nowej strony w istotny sposób zmieni raczej małą „skłonność do surfowania" – użytkownicy Internetu odwiedzali około 3 stron podczas jednej wizyty. Spodziewany jest również wzrost liczby odwiedzin na stronie.

Strona powitalna we wszystkich aktualnych językach Wspólnoty wskaże odwiedzającym drogę do dokumentów dostępnych w ich językach. Większość informacji jest obecnie dostępna przynajmniej w języku angielskim i francuskim. W niedalekiej przyszłości planuje się wprowadzić język niemiecki jako trzeci język.

## 5.4. Przemówienia

W ciągu całego roku EIOD nadal poświęcał wiele czasu i wysiłku na objaśnianie swoich zadań i propagowanie wiedzy o ochronie danych w ogóle, jak również o szeregu konkretnych zagadnień przez wystąpienia publiczne i inne podobne formy aktywności w różnorodnych instytucjach i w różnych państwach członkowskich. EIOD udzielił także pewnej liczby wywiadów dla odnośnych mediów.

EIOD pojawiał się często na posiedzeniach Komisji ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego lub uczestniczył w podobnych wydarzeniach. W dniu 24 stycznia przedstawił swoją opinię na temat wniosku dotyczącego dostępu do Wizowego systemu informacyjnego (VIS) do celów bezpieczeństwa wewnętrznego i egzekwowania prawa. W dniu 21 lutego spotkał się z posłami do PE w sprawie innych aspektów VIS. Tego samego dnia przedstawił także swoją opinię na temat decyzji ramowej dotyczącej ochrony danych w trzecim filarze. W dniu 27 kwietnia przedstawił swoje sprawozdanie roczne za 2005 rok. W dniu 30 maja wystąpił na seminarium poświęconym interoperacyjności baz danych. W dniu 22 czerwca podczas wspólnego posiedzenia Komisji ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego oraz przedstawicieli parlamentów krajowych zaprezentował swoje stanowisko w sprawie przekazywania Stanom Zjednoczonym danych dotyczących przelotu pasażera (PNR). W dniu 4 października przemawiał podczas przesłuchania publicznego w sprawie SWIFT. W dniu 19 października wystąpił na otwartym seminarium poświęconym bezpieczeństwu i wolności zorganizowanym przez Grupę Porozumienia Liberałów i Demokratów na rzecz Europy. W dniu 18 grudnia wygłosił przemówienie na otwartym seminarium poświęconemu współpracy policyjnej w UE.

**Peter Hustinx i Joaquín Bayo Delgado prezentują sprawozdanie roczne za 2005 rok podczas konferencji prasowej.**

Rozwijają się również kontakty z innymi komisjami i służbami parlamentarnymi. W dniu 26 czerwca EIOD wygłosił przemówienie na seminarium służby prawnej Parlamentu Europejskiego. Ponadto w dniu 23 listopada przemawiał przed Komisją ds. Zatrudnienia i Spraw Socjalnych PE (EMPL) podczas przesłuchania publicznego w sprawie zabezpieczenia społecznego. W dniu 22 grudnia na forum Komisji Kontroli Budżetowej (COCOBU) Parlamentu Europejskiego przedstawił swoją opinię w sprawie zmiany rozporządzenia finansowego i jego zasad wykonawczych.

W dniu 12 stycznia na posiedzeniu stosownej grupy roboczej Rady EIOD przedstawił swoją opinię w sprawie ochrony danych w trzecim filarze. W dniach 19 maja i 27 października brał udział w dyskusjach na forum grupy roboczej ds. ochrony danych, która ma zajmować się różnymi kwestiami w ramach pierwszego filaru.

Inne instytucje i organy UE oczywiście również znalazły się na liście kontaktów. W dniu 3 kwietnia EIOD wygłosił przemówienie adresowane do dyrektora generalnego i zarządu OLAF-u dotyczące potrzeby wdrażania w działalności tego organu odpowiednich środków w zakresie ochrony danych. W dniu 17 maja przemawiał w Komisji Europejskiej na publicznym seminarium poświęconym systemom identyfikacji radiowej (RFID). W dniu 18 maja wygłosił przemówienie w Europejskim Banku Inwestycyjnym. W dniu 29 czerwca przedstawił prezentację na cotygodniowym spotkaniu sekretarza generalnego i dyrektorów generalnych Komisji. W dniu 5 grudnia przemawiał na posiedzeniu prezydium Komitetu Regionów.

W ciągu roku EIOD odwiedził także szereg państw członkowskich. W dniu 29 marca w Madrycie na pierwszej europejskiej konferencji poświęconej ochronie danych wygłosił przemówienie dla przedstawicieli sektora publicznego i prywatnego. W dniu 24 kwietnia w Budapeszcie przemawiał na wiosennej konferencji europejskich komisarzy ds. ochrony danych. W dni 11 maja w Warszawie przedstawił prezentację podczas konferencji poświęconej ochronie danych i bezpieczeństwu publicznemu. W dniu 23 maja w Manchesterze na 4. Międzynarodowej konferencji komisarzy ds. informacji wygłosił przemówienie na temat „Ochrona danych i przejrzystość w instytucjach UE". W dniu 1 czerwca EIOD w Amsterdamie brał udział w konferencji Międzynarodowej Federacji Stowarzyszeń Prawa Komputerowego (International Federation of Computer Law Associations), podczas której wygłosił przemówienie poświęcone aktualnej sytuacji w dziedzinie ochrony danych. W dniu 7 czerwca w Londynie zeznawał przed podkomisją Izby Lordów w sprawie różnych kwestii związanych z ochroną danych w ramach trzeciego filaru. W dniu 27 czerwca w Brukseli wygłosił przemówienie skierowane do uczestników Międzynarodowego forum bankowego ds. przestępczości finansowej (International Banking Forum on Financial Crime).

W dniu 27 września EIOD wygłosił przemówienie na 5. dorocznej konferencji poświęconej spełnianiu wymogów ochrony danych (Annual Data Protection Compliance Conference), która odbyła się w Londynie. W dniu 28 września przemawiał na zorganizowanym niedaleko Helsinek przez prezydencję fińską seminarium poświęconym europejskiemu społeczeństwu informacyjnemu. W dniu 4 października wygłosił przemówienie w Barcelonie na pierwszej międzynarodowej konferencji poświęconej ochronie danych w państwach wielonarodowych i federacyjnych. W dniu 8 listopada we Frankfurcie wygłosił przemówienie podczas warsztatów zorganizowanych przez Międzynarodowe Konsorcjum Prywatności w Farmaceutyce (International Pharmaceutical Privacy Consortium). W dniu 9 listopada przemawiał w Akademii Prawa Europejskiego w Trewirze na temat „Europejskich ram instytucjonalnych w zakresie ochrony danych". W dniu 14 listopada w Brukseli na posiedzeniu okrągłego stołu zorganizowanym przez organizację ARMA (Association of Records Managers and Administrators) wygłosił przemówienie dotyczące zatrzymywania danych. W dniu 15 grudnia w Brukseli podczas holenderskiego forum technologii biometrycznych (Dutch Biometrics Forum) wygłosił przemówienie dotyczące stanowiska EIOD w kwestii technologii biometrycznych.

Zastępca EIOD przedstawił w Budapeszcie, Warszawie, Madrycie i Barcelonie, między innymi dla Hiszpańskiej Szkoły Prawniczej, podobne prezentacje poświęcone ochronie danych w ramach trzeciego filaru.

## 5.5. Biuletyn

W 2006 roku opublikowano pięć wydań biuletynu. Liczba subskrybentów stale rosła od około 250 osób w styczniu do około 460 pod koniec roku. Z biuletynu korzystają między innymi posłowie do Parlamentu Europejskiego, pracownicy UE oraz personel krajo-

**Peter Hustinx w rozmowie z dziennikarką.**

wych organów ochrony danych, aby śledzić bieżącą działalność EIOD. Biuletyn zawiera opinie dotyczące wniosków prawodawczych oraz opinie na temat kontroli wstępnych wraz ze stosownymi informacjami i kontekstem oraz innymi bieżącymi wydarzeniami. Subskrypcję można zamówić automatycznie na stronie internetowej ([70]).

Biuletyn jest skutecznym instrumentem informującym o najnowszych zmianach na stronie internetowej i umożliwiającym ich rozpowszechnianie.Dzięki temu strona internetowa jest bardziej eksponowana i zachęca do kolejnych wizyt. Społeczeństwo sieciowe zainteresowane działalnością w zakresie ochrony danych na poziomie UE rośnie w ten sposób ilościowo; podwyższa się również poziom zainteresowania tą tematyką, uwidaczniający się przynajmniej rosnącą liczbą interakcji.

## 5.6. Służba prasowa

Służba prasowa jest odpowiedzialna za kontakty z dziennikarzami, pisanie komunikatów prasowych i organizację konferencji prasowych. Urzędnik ds. prasowych kieruje także elastycznym zespołem informacyjnym, który uczestniczy we wszelkich działaniach promocyjnych (dzień otwartych drzwi UE itp.), jak również w przygotowywaniu materiałów informacyjnych kierowanych do społeczeństwa i dziennikarzy.

W roku 2006 zorganizowano dwie konferencje prasowe. W połowie kwietnia przedstawiono sprawozdanie roczne za 2005 rok, którego głównym przesłaniem była „konsolidacja EIOD". Konferencja prasowa podkreśliła różnice między rokiem 2004, w którym powstał omawiany organ, a jego drugim rokiem działalności. Wraz z upływem czasu coraz wyraźniej dawało się odczuć, że istnieje powszechne błędne przekonanie o niepotrzebnym utrudnianiu przez ochronę prywatności i danych osobowych walki z terroryzmem i przestępczością zorganizowaną. Dlatego też w połowie swojego pięcioletniego mandatu EIOD i zastępca EIOD zorganizowali w połowie września drugą konferencję prasową, koncentrując się na prawie do prywatności w UE i jego prawnej i kluczowej roli w tworzeniu polityki.

Te cieszące się dużym zainteresowaniem konferencje prasowe obejmowały zarówno działania EIOD związane z zapewnianiem wywiązywania się przez instytucje i organy Wspólnoty ze swoich zobowiązań w zakresie ochrony danych, jak i jego działalność doradczą dotyczącą nowych aktów prawodawczych i nowych polityk. Ponadto w tym roku udzielono ponad 20 wywiadów dla mediów drukowanych oraz audiowizualnych. Większość próśb o udzielenie wywiadu złożyła „EU Press" – organizacja medialna specjalizująca się w sprawach UE dla osób zajmujących się zawodowo tą problematyką. Udzielano jednak również wywiadów mediom o bardziej krajowym zasięgu w celu dotarcia poza środowisko brukselskie oraz zaznaczenia swojej obecności w dyskusjach prowadzonych w państwach członkowskich. Trzy przykłady takich działań to wywiady dla niemieckiego i szwedzkiego radia oraz dla słoweńskiego dziennika.

([70]) http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/27

**Personel EIOD przy stoisku w Parlamencie Europejskim podczas dni otwartych drzwi, 6 maja 2006.**

Nie spełniano próśb o wywiady dotyczące spraw wykraczających poza instytucjonalną rolę EIOD. Prośby takie wpływają do służby prasowej przynajmniej raz w tygodniu i często prowadzą do przekazania podstawowych informacji oraz szczegółów dotyczących kontaktu z organem odpowiedzialnym.

## 5.7. Informacje oraz porady

Liczba próśb o informacje i próśb o poradę wzrosła w 2006 roku o około 70%. W sumie wpłynęło ponad 170 próśb – dotyczących szerokiego spektrum zagadnień – od studentów i innych zainteresowanych obywateli, jak też od kierowników projektów i prawników.

Ponad 80% tych próśb sklasyfikowano jako „prośby o informacje" – jest to szeroka kategoria obejmująca ogólne pytania dotyczące polityk UE, ale także pytania związane z ochroną danych w państwach członkowskich, jak również w administracji UE. Przykładowo są to pytania o spam e-mailowy i kradzież tożsamości, o prywatność i Internet oraz o sposób postępowania zgodny z dyrektywą 95/46/WE w przypadku projektów obejmujących działania w kilku państwach członkowskich.

Prośby o informacje o bardziej złożonym charakterze wymagające głębszej analizy klasyfikowane są jako „prośby o poradę". Stanowią one prawie 20% próśb. Oto dwa przykłady pytań związanych ze sposobami postępowania z publicznym dostępem do dokumentów zawierających dane osobowe: jakie informacje można udostępniać o lobbystach akredytowanych przy Parlamencie Europejskim ([71]) oraz czy zdjęcia pracowników umieszczane na identyfikatorach bezpieczeństwa można umieszczać w instytucyjnym informatorze „Kto jest kim".

Podobnie jak w 2005 roku, większość próśb napływała w języku angielskim lub francuskim, dzięki czemu możliwa była szybka odpowiedź – prawie zawsze w ciągu 15 dni roboczych. Znaczna liczba próśb napłynęła jednak także w innych językach urzędowych – niektóre z nich wymagały pomocy służby tłumaczeniowej, co przedłużyło czas przygotowania na nie odpowiedzi. Prośby te są również pomocne w opracowywaniu nowych treści zamieszczanych na stronie internetowej, które mają informować osoby wchodzące na tę stronę oraz, w możliwie największym stopniu, zapobiegać zbędnym pytaniom lub skargom.

## 5.8. Dzień otwartych drzwi UE

W 2006 roku dzień otwartych drzwi zorganizowano 6 maja. Wszystkie główne instytucje i organy UE uczestniczą w tym wydarzeniu, które nabiera charakteru ulicznego festiwalu ożywiającego obszar, na którym znajdują się siedziby kluczowych instytucji UE, między centralnym kompleksem budynków Parlamentu Europejskiego a budynkiem Komisji.

Przygotowano stoisko i drobne materiały promocyjne (długopisy, karteczki samoprzylepne oraz karty pamięci USB), które można wykorzystywać podczas dnia otwartych drzwi, jak również przy innych okazjach. Stoisko EIOD umiejscowiono w budynku Parlamentu Europejskiego; ponad 200 osób wzięło udział w quizie z zakresu problematyki ochrony danych, co dało asumpt do dyskusji na temat ochrony prywatności i danych w Europie.

([71]) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/06-08-31_transparency_lobbyists_EN.pdf

# 6. Administracja, budżet i personel

## 6.1. Wprowadzenie: rozwój nowej instytucji

Rozwój EIOD jako nowej instytucji ([72]) był kontynuowany na podstawach utworzonych w 2005 roku w celu utrwalenia osiągnięć pierwszego okresu jego działalności. W 2006 roku EIOD uzyskał *dodatkowe zasoby,* zarówno budżetowe (wzrost z 2 879 305 EUR do 4 138 378 EUR), jak i osobowe (wzrost z 19 do 24 osób).

*Otoczenie administracyjne* jest stopniowo rozszerzane na podstawie priorytetów ustalonych na dany rok z uwzględnieniem potrzeb i rozmiarów instytucji. EIOD przyjął różne przepisy wewnętrzne ([73]) niezbędne do prawidłowego funkcjonowania tej instytucji. Utworzono komitet personelu. Jego funkcjonowanie jest ściśle związane z ogólnymi przepisami wykonawczymi odnoszącymi się do regulaminu pracowniczego oraz innymi przepisami wewnętrznymi przejętymi przez instytucję EIOD. Służby EIOD opracowały sprawozdanie dotyczące wdrażania standardów kontroli wewnętrznej. Pierwszy audyt wewnętrzny został przeprowadzony przez audytora wewnętrznego, a wnioski z niego będą przedstawione w 2007 roku.

*Współpraca z innymi instytucjami* – Parlamentem Europejskim, Radą i Komisją Europejską uległa dalszej poprawie, co pozwoliło uzyskać znaczne korzyści z efektu skali. W grudniu podpisano przedłużenie o trzy lata porozumienia o współpracy administracyjnej z dnia 24 czerwca 2004 roku. Wciąż jeszcze dało się zauważyć wolniejsze wykonywanie niektórych zadań związane z zasadą wzajemnej pomocy (głównie w zakresie dostępu do oprogramowania administracyjnego i finansowego), problem ten powinien jednak zostać rozwiązany w 2007 roku. EIOD przejął pewne zadania, które pierwotnie wykonywane były przez inne instytucje.

Zwiększono liczbę pomieszczeń pierwotnie udostępnionych EIOD i obecnie instytucja ta zajmuje dwa piętra w budynku Parlamentu Europejskiego przy ulicy Montoyer 63.

## 6.2. Budżet

Szacunki budżetowe na rok 2006 opracowano w marcu 2005 roku. Były to pierwsze szacunki, jakie opracował EIOD bez korzystania ze wsparcia służb Parlamentu Europejskiego (jak to miało miejsce w przypadku budżetów na lata 2004 i 2005).

Budżet ten przyjęty przez władzę budżetową na rok 2006 wynosił 3 583 833 EUR. Stanowi to wzrost o 24,5% w porównaniu z budżetem na 2005 rok. W dniu 27 września 2006 roku przyjęto zmieniony budżet wynoszący 4 138 378 EUR w związku ze znacznym wzrostem liczby opinii wydawanych przez EIOD dotyczących wniosków prawodawczych, które to opinie muszą zostać opublikowane w Dzienniku Urzędowym, oraz wpływem tych publikacji na liczbę wymaganych tłumaczeń.

EIOD postanowił zastosować przepisy wewnętrzne Komisji w odniesieniu do wykonania swojego budżetu w zakresie, w jakim przepisy te mają zastosowanie do struktury i skali EIOD, oraz w przypadku braku przepisów szczegółowych.

Komisja nadal udzielała EIOD wsparcia, w szczególności w zakresie rachunkowości, jako że księgowy komisji został także mianowany księgowym EIOD.

([72]) Na podstawie art. 1b Regulaminu pracowniczego urzędników Wspólnot Europejskich oraz art. 1 rozporządzenia finansowego EIOD traktowany jest jako jedna z instytucji Wspólnot. Zobacz również art. 43 ust. 6 rozporządzenia (WE) nr 45/2001.

([73]) W załączniku I znajduje się wykaz umów i decyzji administracyjnych.

**Członkowie wydziału personalnego dyskutują nad dossier.**

W swoim sprawozdaniu za rok budżetowy 2005 Trybunał Obrachunkowy stwierdził, że nie ma żadnych uwag po przeprowadzeniu kontroli.

## 6.3. Zasoby ludzkie

W odniesieniu do zadań w zakresie zarządzania personelem EIOD (składającym się z dwóch mianowanych członków i 24 osób personelu) EIOD korzysta z bardzo efektywnej pomocy służb Komisji.

### 6.3.1. Rekrutacja

EIOD – instytucja która powstała niedawno – jest wciąż w fazie tworzenia i tak będzie jeszcze przez kilka najbliższych lat. Rosnące eksponowanie działalności EIOD oznacza dla niego wzrost obciążenia pracą, jak również poszerzenie zakresu zadań. Znaczny wzrost obciążenia pracą w 2006 roku opisano w poprzednich rozdziałach. Zasoby ludzkie mają oczywiście w tym kontekście do odegrania bardzo istotną rolę.

Początkowo EIOD zdecydował o ograniczeniu rozszerzania zakresu zadań i zwiększania liczebności personelu, stosując wzrost kontrolowany, aby dopilnować, by nowi pracownicy zostali w pełni wdrożeni do pracy i odpowiednio wyszkoleni oraz by mogli się odpowiednio zintegrować z zespołem. Dlatego też EIOD postulował utworzenie tylko pięciu stanowisk w 2006 roku (trzy stanowiska AD ([74]) i dwa stanowiska AST ([75])). Wniosek dotyczący wzrostu liczby personelu z 19 w 2005 roku do 24 w 2006 roku został zatwierdzony przez władzę budżetową. Na początku roku opublikowano ogłoszenia o naborze i w ciągu roku wszystkie stanowiska obsadzono.

Pomoc Komisji w tym względzie była wartościowa, w szczególności pomoc udzielona przez Biuro Administrowania i Rozliczania Należności Indywidualnych (PMO) oraz służbę medyczną. W 2006 roku EIOD rozwijał również działalność w sferze socjalnej. Dzięki świetnej współpracy z innymi instytucjami, w szczególności z Radą, Komitetem Regionów, Parlamentem Europejskim i Rzecznikiem Praw Obywatelskich, możliwa była wymiana informacji i najlepszych praktyk w tej dziedzinie.

EIOD ma dostęp do usług świadczonych przez Europejski Urząd Doboru Kadr (EPSO) i uczestniczy w pracach jego zarządu, obecnie w charakterze obserwatora.

([74]) Administratorzy.
([75]) Asystenci.

### 6.3.2. Program stażowy

Program stażowy został uruchomiony w 2005 roku. Jego głównym celem jest stworzenie osobom, które właśnie skończyły studia, okazji do wykorzystania swojej wiedzy teoretycznej w praktyce, a jednocześnie do zdobycia doświadczenia w zakresie bieżącej działalności EIOD. Dzięki temu EIOD staje się bardziej widoczny dla młodych obywateli UE, w szczególności dla tych studentów i młodych absolwentów, którzy specjalizują się w problematyce ochrony danych.

Główny program obejmuje dwie pięciomiesięczne sesje rocznie, a w jednej sesji uczestniczy dwoje lub troje stażystów. W 2006 roku w programie wzięło udział po dwoje stażystów w sesji; większość z nich specjalizowała się w dziedzinie ochrony danych. Pierwsza sesja rozpoczęła się w październiku 2005 roku i trwała do końca lutego 2006 roku. Jej wyniki były bardzo dobre. Stażyści uczestniczyli zarówno w teoretycznych, jak i praktycznych pracach, zdobywając doświadczenie z pierwszej ręki.

Oprócz głównego programu stażowego stworzono specjalne warunki umożliwiające studentom i doktorantom uczestnictwo w krótkoterminowych bezpłatnych stażach. Ta druga część programu daje ograniczonej liczbie młodych studentów dobranych na podstawie konkretnych kryteriów sposobność do prowadzenia badań związanych z tematyką ich prac naukowych. Program ten jest realizowany zgodnie z procesem bolońskim oraz w związku z obowiązkiem odbycia przez studentów stażu w ramach studiów. Na początku roku do odbycia dwumiesięcznego bezpłatnego stażu wybrano jednego doktoranta. Uczestnictwo we wspomnianym wyżej bezpłatnym stażu jest ograniczone do wyjątkowych przypadków i uzależnione od spełnienia konkretnych kryteriów doboru.

Oprócz stażystów specjalizujących się w ochronie danych do odbycia stażu od października 2006 roku do lutego 2007 roku w dziale zasobów ludzkich, administracji i budżetu wybrano jednego kandydata z wykształceniem w zakresie biznesu i finansów.

EIOD korzysta z pomocy administracyjnej Biura ds. Staży Dyrekcji Generalnej ds. Edukacji i Kultury (DG EAC) Komisji Europejskiej, które udziela stale wartościowego wsparcia, możliwego dzięki bogatemu doświadczeniu pracowników, na podstawie porozumienia o gwarantowanym poziomie usług podpisanego w 2005 roku. Równolegle kontynuowana była współpraca z biurami ds. staży innych instytucji europejskich, w szczególności Rady, Komitetu Regionów oraz Europejskiego Komitetu Ekonomiczno-Społecznego.

### 6.3.3. Programy dla oddelegowanych ekspertów krajowych

Realizacja programu dla oddelegowanych ekspertów krajowych rozpoczęła się w styczniu 2006 roku po ustanowieniu jesienią 2005 roku jego podstaw prawnych i organizacyjnych ([76]).

Oddelegowanie ekspertów krajowych umożliwia EIOD wykorzystanie wiedzy fachowej i doświadczenia pracowników organów ochrony danych z państw członkowskich. Program ten umożliwia także ekspertom krajowym zapoznanie się z ochroną danych w środowisku UE (pod względem nadzoru, konsultacji i współpracy). Jednocześnie działalność EIOD staje się bardziej widoczna na poziomie operacyjnym w terenie.

W celu wyłonienia ekspertów krajowych EIOD kontaktuje się bezpośrednio z krajowymi organami ochrony danych. Stałe przedstawicielstwa państw członkowskich są również informowane o tym programie i proszone o pomoc w znalezieniu właściwych kandydatów. Dyrekcja Generalna ds. Administracji Komisji Europejskiej służy cenną pomocą administracyjną w organizacji programu.

Oddelegowanie od połowy stycznia 2006 roku jednego eksperta z węgierskiego organu ochrony danych – komisarza ds. ochrony danych i wolności informacji – dało początek realizacji programu.

### 6.3.4. Struktura organizacyjna

Struktura organizacyjna EIOD nie zmienia się od 2004 roku: jedna sekcja licząca obecnie 7 osób jest odpowiedzialna za administrację, personel i budżet; pozostałych 17 pracowników zajmuje się wykonywaniem zadań operacyjnych z zakresu ochrony danych. Pracują oni pod bezpośrednim zwierzchnictwem inspektora lub zastępcy inspektora w dwóch dziedzinach i zajmują się głównie nadzorem i konsultacjami. Zachowana jest pewna elastyczność w przydzielaniu pracownikom zadań, ponieważ instytucja EIOD wciąż ewoluuje.

([76]) Decyzja EIOD z dnia 10 listopada 2005 r.

### 6.3.5. Działalność szkoleniowa

Pracownicy EIOD mogą uczestniczyć w szkoleniach ogólnych oraz w kursach językowych organizowanych przez inne instytucje, głównie Komisję, a także w kursach prowadzonych przez Europejską Szkołę Administracji (ESA).

Współpraca w zakresie szkoleń językowych jest w przeważającej części organizowana za pośrednictwem międzyinstytucjonalnego komitetu ds. szkoleń językowych, którego EIOD jest członkiem. W 2006 roku instytucje będące członkami tego komitetu podpisały porozumienie w sprawie harmonizacji kosztów międzyinstytucjonalnych kursów językowych.

Dostęp do kursów organizowanych przez ESA zapewnia podpisane z tą szkołą w 2005 roku porozumienie o gwarantowanym poziomie usług.

W 2006 roku EIOD wysunął propozycję opracowania polityki w zakresie szkoleń opartej na charakterystyce działalności danej instytucji, jak również na jej celach strategicznych. Celem EIOD jest stanie się centrum doskonałości w dziedzinie ochrony danych, podniesienie poziomu wiedzy i umiejętności pracowników, tak aby wartości, którym hołduje ta instytucja, były w pełni rozumiane i przestrzegane przez jej personel.

Dzięki współpracy z Europejską Szkołą Administracji EIOD zorganizował pierwsze zajęcia w zakresie integracji zespołu z myślą o osiągnięciu wspólnych celów i wypracowaniu wyraźnej i niepowtarzalnej tożsamości.

## 6.4. Pomoc administracyjna i współpraca międzyinstytucjonalna

### 6.4.1. Przedłużenie porozumienia o współpracy międzyinstytucjonalnej

Istotnym wydarzeniem w 2006 roku było przedłużenie o trzy lata porozumienia o współpracy międzyinstytucjonalnej zawartego w czerwcu 2004 roku z sekretarzami generalnymi Parlamentu Europejskiego, Rady i Komisji. Współpraca ta ma wielką wartość dla EIOD, ponieważ daje mu ona dostęp do wiedzy fachowej innych instytucji w obszarach, w których udzielana jest pomoc, a także pozwala skorzystać z efektu skali.

Na podstawie tego porozumienia prowadzona była współpraca z różnymi służbami Komisji ([77]), rozmaitymi służbami Parlamentu Europejskiego (usługi informatyczne, szczególnie związane z pracami na drugą generacją strony internetowej; wyposażanie lokali, ochrona budynku, druk, poczta elektroniczna, telefon, materiały itp.) oraz z Radą (tłumaczenia).

W celu usprawnienia współpracy między wydziałami Komisji a EIOD w 2005 roku wystąpiono o bezpośredni dostęp z zajmowanych przez EIOD pomieszczeń do głównych programów komputerowych Komisji obsługujących zasoby ludzkie i zarządzanie finansami. Taki bezpośredni dostęp, który poprawiłby wymianę informacji i umożliwiłby efektywniejsze i szybsze zarządzanie poszczególnymi dossier zarówno przez EIOD, jak i służby Komisji, jest niestety możliwy tylko do systemu SI2 i częściowo do systemu Syslog; do pozostałych programów nie ma jeszcze bezpośredniego dostępu (np. do systemu ABAC) ([78]). EIOD przewiduje intensyfikację współpracy w tej dziedzinie i ma nadzieję, że dostęp do pozostałych systemów będzie możliwy w 2007 roku.

Zapewniono realizację porozumień o gwarantowanym poziomie usług podpisanych w 2005 roku z różnymi instytucjami i ich wydziałami. Obejmują one:

- porozumienie z Radą dotyczące pomocy udzielanej EIOD w dziadzienie tłumaczeń; pomoc ta jest bardzo istotna, ponieważ liczba dokumentów wymagających przetłumaczenia znacznie wzrosła;
- porozumienie z Biurem Komisji ds. Staży (w ramach DG ds. Edukacji i Kultury), które umożliwiło kontynuację programu stażowego w 2006 roku);
- porozumienie z Dyrekcją Generalną ds. Zatrudnienia, Spraw Społecznych i Równości Szans (DG EMPL) Komisji Europejskiej, dotyczące niezbędnej pomocy technicznej udzielanej EIOD w zakresie konstrukcji przenośnego stoiska, opracowania logo i nowego układu strony internetowej.

([77]) Dyrekcja Generalna ds. Personelu i Administracji, Dyrekcja Generalna ds. Budżetu, Służba Audytu Wewnętrznego, Dyrekcja Generalna ds. Bezpieczeństwa, Dyrekcja Generalna ds. Edukacji i Kultury, Dyrekcja Generalna ds. Zatrudnienia, Spraw Społecznych i Równości Szans oraz Biuro Administrowania i Wypłacania Należności Indywidualnych.

([78]) Syslog jest systemem informatycznym służącym do zarządzania szkoleniami. SI2 i ABAC są systemami służącymi do zarządzania księgowością.

### 6.4.2. Dalsze działania w ramach współpracy międzyinstytucjonalnej

Współpraca międzyinstytucjonalna ma podstawowe znaczenie dla EIOD i dalszego rozwoju tej instytucji. W 2006 roku, oprócz porozumienia administracyjnego, współpraca międzyinstytucjonalna stała się codzienną praktyką, umożliwiając wzrost efektywności w wielu dziedzinach administracji.

Trwał międzyinstytucjonalny przetarg na dostawę umeblowania, co umożliwiło EIOD uzyskanie pewnej niezależności pod względem wyposażania przestrzeni biurowej.

Dzięki współpracy z różnymi służbami Parlamentu Europejskiego, który dał EIOD możliwość skorzystania ze swoich umów ramowych, udało się opracować nową stronę internetową EIOD. Idąc za poradą Parlamentu, EIOD podpisał z konsultantem wymienionym w umowie ramowej z tą instytucją umowę dotyczącą całkowitej przebudowy strony. Strona internetowa drugiej generacji została uruchomiona w styczniu 2007 roku.

W 2006 roku EIOD podpisał umowę o pomocy administracyjnej z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA), określającą zasady wykonawcze w zakresie kontroli bezpieczeństwa bazy danych EURODAC, a także warunków prowadzenia współpracy (zob. pkt 2.9).

EIOD nadal uczestniczył w pracach różnych międzyinstytucjonalnych komitetów, jednak ze względu na wielkość tej instytucji udział taki musiał się ograniczyć tylko do prac kilku komitetów. Uczestnictwo w działalności tych komitetów sprawiło, że EIOD stał się bardziej widoczny dla innych instytucji, a także pobudziło stałą wymianę informacji i dobrych praktyk.

### 6.4.3. Stosunki zewnętrzne

Zakończyły się działania prowadzące do uznania EIOD przez władze Belgii, co umożliwiło tej instytucji i jego personelowi korzystanie z przywilejów i immunitetów określonych w Protokole w sprawie przywilejów i immunitetów Wspólnot Europejskich.

## 6.5. Infrastruktura

EIOD dysponował zbyt małą przestrzenią biurową, aby pomieścić rosnącą liczbę pracowników. Problem ten rozwiązało przyznanie EIOD w 2006 roku dodatkowych pomieszczeń – siódmego piętra w budynku Parlamentu Europejskiego „Montoyer 63", w wyniku czego EIOD może obecnie korzystać z dwóch kolejnych pięter w tym gmachu. W związku z faktem, że EIOD przetwarza dane wrażliwe, nowe piętro zostało zabezpieczone za pomocą tego samego systemu ochronnego, który stosowany jest na szóstym piętrze, w celu zadbania o to, aby dostęp do tych pomieszczeń miały tylko osoby upoważnione.

Pomoc administracyjna, jaką Parlament Europejski udzielał EIOD w zakresie umeblowania, zakończyła się w 2005 roku. EIOD podjął więc niezależne działania w tym względzie i wziął udział w międzyinstytucjonalnym przetargu.

Zgodnie z porozumieniem o współpracy administracyjnej Parlament Europejski wspiera EIOD w zakresie infrastruktury informatycznej i telefonicznej.

## 6.6. Otoczenie administracyjne

### 6.6.1. Działania podejmowane w następstwie ustanowienia standardów kontroli wewnętrznej

Na podstawie porozumienia międzyinstytucjonalnego z 24 czerwca 2004 roku audytor wewnętrzny Komisji został mianowany audytorem EIOD.

Na mocy swojej decyzji z 7 listopada 2005 roku oraz zgodnie z art. 60 ust. 4 rozporządzenia finansowego EIOD ustalił szczególne procedury kontroli wewnętrznej uwzględniające strukturę, wielkość i charakter działalności tej instytucji.

Sprawozdanie oceniające system kontroli wewnętrznej zostało opracowane przez służby EIOD. Zawiera ono szczegółową analizę już przyjętych procedur oraz określa pewne ulepszenia, których wprowadzenie powinno być traktowana priorytetowo w 2007 roku. Sprawozdanie to potwierdziło również skuteczność przyjętych standardów kontroli.

W 2006 roku po raz pierwszy przeprowadzono w EIOD kontrolę wewnętrzną. Wnioski z tej kontroli zostaną podsumowane w sprawozdaniu, które ma być sporządzone przez służby audytu wewnętrznego.

### 6.6.2. Utworzenie komitetu pracowniczego

Zgodnie z art. 9 Regulaminu pracowniczego urzędników Wspólnot Europejskich 8 lutego 2006 roku inspektor przyjął decyzję o utworzeniu komitetu pracowniczego. Komitet ten został wybrany w marcu 2006 roku. Konsultowano się z nim w sprawie szeregu ogólnych przepisów wykonawczych dotyczących regulaminu pracowniczego oraz innych przepisów wewnętrznych przyjętych przez tę instytucję.

### 6.6.3. Elastyczny czas pracy (*flexitime*)

W 2005 roku EIOD przyjął decyzję dotyczącą elastycznego czasu pracy. Nie jest to formuła obowiązująca na podstawie regulaminu pracowniczego, jest to raczej środek służący organizacji dnia pracy w taki sposób, aby umożliwić pracownikom godzenie pracy zawodowej z życiem prywatnym, a EIOD ustalanie godzin pracy zgodnie z priorytetami. Każdy pracownik może wybrać między tradycyjnymi godzinami pracy a elastycznym czasem pracy z możliwością odebrania przepracowanych nadgodzin. Okazało się, że metoda ta jest bardzo korzystna zarówno dla instytucji, jak i jej personelu.

### 6.6.4. Przepisy wewnętrzne

Nadal przyjmowano nowe przepisy wewnętrzne niezbędne do prawidłowego funkcjonowania instytucji EIOD, jak również nowe ogólne przepisy wykonawcze dotyczące regulaminu pracowniczego (zob. załącznik I).

W przypadku gdy przepisy te odnoszą się do dziedzin, w których EIOD korzysta ze wsparcia Komisji, są one podobne do przepisów Komisji z zastosowaniem pewnych dostosowań w celu uwzględnienia specyficznego charakteru EIOD. Przepisy te udostępnia się nowym pracownikom EIOD w celach informacyjnych. Usprawniono niektóre stosowane procedury administracyjne, w rezultacie czego w listopadzie 2006 roku zaktualizowano przewodnik administracyjny.

W celu zapewnienia stosowania przepisów rozporządzenia (WE) nr 45/2001 mianowano wewnętrznego urzędnika ds. ochrony danych (DPO).

EIOD rozpoczął pewne działania w dziedzinie socjalnej (głównie dotyczące dzieci, np. żłobek). Zagwarantowano również dzieciom pracowników możliwość uczęszczania do Szkoły Europejskiej.

## 6.7. Cele na 2007 rok

Cele ustalone na 2006 rok zostały w pełni osiągnięte. W 2007 roku EIOD będzie kontynuował konsolidację rozpoczętą w 2006 roku i pogłębiał niektóre aspekty swojej działalności.

Struktura *budżetu* tej instytucji zostanie odnowiona przez przyjęcie nowej terminologii budżetowej mającej zastosowanie do ustalania budżetu na rok 2008. Będzie ona oparta na trzyletnim doświadczeniu EIOD i będzie uwzględniać szczególne potrzeby tej instytucji oraz zapewniać przejrzystość wymaganą przez władzę budżetową.

W 2007 roku EIOD zamierza także przyjąć nowe wewnętrzne zasady finansowe dostosowane do wielkości tej instytucji. Jeśli chodzi o oprogramowanie finansowe, EIOD podejmie wszelkie niezbędne działania w celu nabycia programów umożliwiających mu dostęp do danych finansowych ze swojej siedziby.

W roku 2007 planuje się podjęcie decyzji dotyczącej oceny *pracowników* oraz przewodnika dla osób przeprowadzających ocenę. Po przyjęciu tych dokumentów zostanie przeprowadzona pierwsza ocena. W 2007 roku zakończy się opracowywanie wewnętrznej polityki szkoleniowej.

Bardzo istotna dla EIOD będzie dalsza *współpraca administracyjna* oparta na przedłużonym porozumieniu administracyjnym. Jednocześnie EIOD będzie nadal pracował nad rozwojem otoczenia administracyjnego i przyjmował ogólne przepisy wykonawcze dotyczące regulaminu pracowniczego.

Dzięki pomocy PE i przyjęciu systemu zarządzania pocztą elektroniczną poprawi się zarządzanie pocztą.

Wprowadzanie ulepszeń określonych podczas pierwszej oceny *systemu kontroli wewnętrznej* będzie traktowane jako priorytet w 2007 roku.

W roku 2007 spis i analiza operacji przetwarzania danych zostaną ukończone, przy wsparciu DPO.

Mając na uwadze stopień poufności wymagany w niektórych dziedzinach działalności, EIOD zamierza opracować kompleksową politykę w zakresie *bezpieczeństwa* stosowną do funkcji wypełnianych przez tę instytucję.

Załącznik A

# Ramy prawne

Artykuł 286 Traktatu WE, przyjęty w 1997 roku jako część traktatu z Amsterdamu, stanowi, że akty wspólnotowe dotyczące ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych oraz swobodnego przepływu tych danych mają również zastosowanie do instytucji i organów wspólnotowych, z czym wiąże się ustanowienie niezależnego organu kontrolnego.

Aktami wspólnotowymi, o których mowa w tym postanowieniu, są: dyrektywa 95/46/WE ustanawiająca ogólne ramy dla przepisów dotyczących ochrony danych w państwach członkowskich oraz dyrektywa 97/66/WE, dyrektywa sektorowa zastąpiona dyrektywą 2002/58/WE o prywatności i łączności elektronicznej. Obie dyrektywy można uważać za efekt procesu prawnego, który rozpoczął się na początku lat 70. na forum Rady Europy.

## Informacje ogólne

Artykuł 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności przewiduje prawo do poszanowania życia prywatnego i rodzinnego z wyjątkiem ograniczeń dozwolonych wyłącznie pod pewnymi warunkami. W 1981 roku za konieczne uznano jednak przyjęcie oddzielnej konwencji o ochronie danych w celu zastosowania pozytywnego i strukturalnego podejścia do ochrony podstawowych praw i wolności, na które, w nowoczesnym społeczeństwie, może mieć wpływ przetwarzanie danych osobowych. Konwencja ta, znana również jako konwencja 108, została już ratyfikowana przez prawie 40 państw członkowskich Rady Europy, w tym przez wszystkie państwa członkowskie UE.

Dyrektywa 95/46/WE opierała się na zasadach określonych w konwencji 108, precyzowała i rozwijała je jednak pod różnymi względami. Jej celem było zapewnienie wysokiego poziomu ochrony i swobodnego przepływu danych osobowych w UE. We wniosku w sprawie tej dyrektywy złożonym przez Komisję na początku lat 90. stwierdzono, że instytucje i organy Wspólnoty powinny być objęte podobnymi prawnymi środkami bezpieczeństwa, dzięki czemu mogłyby uczestniczyć w swobodnym przepływie danych osobowych, z zastrzeżeniem przestrzegania przez nie równoważnych zasad ochrony. Do czasu przyjęcia art. 286 Traktatu WE brak było jednak podstaw prawnych dla takiego rozwiązania.

Stosowne zasady, o których mowa w art. 286 Traktatu WE, zostały określone w rozporządzeniu (WE) nr 45/2001 Parlamentu Europejskiego i Rady o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, które weszło w życie w 2001 roku ([79]). Rozporządzenie to przewidywało również ustanowienie niezależnego organu kontrolnego zwanego „europejskim inspektorem ochrony danych", któremu, zgodnie z Traktatem, postawiono by konkretne zadania i nadano konkretne uprawnienia.

Traktat konstytucyjny podpisany w październiku 2004 roku kładzie wielki nacisk na ochronę podstawowych praw. Poszanowanie życia prywatnego i rodzinnego oraz ochrona danych osobowych traktowane są jako oddzielne prawa podstawowe w art. II-67 i II-68 konstytucji. Ochrona danych jest także wspomniana w art. I-51 konstytucji, w tytule VI dotyczącym „demokratycznego życia" Unii. Wynika z tego jasno, że ochrona danych jest obecnie uważana za podstawowy składnik „dobrych rządów". Niezależny nadzór jest kluczowym elementem tej ochrony.

## Rozporządzenie (WE) nr 45/2001

Przyglądając się uważniej temu rozporządzeniu, należy przede wszystkim odnotować, że ma ono zastosowanie do „przetwarzania danych osobowych przez instytucje i organy wspólnotowe, o ile takie przetwarzanie jest dokonywane podczas wykonywania czynności, które w całości lub w części wchodzą w zakres prawa wspólnotowego". Oznacza to, że z zadań i uprawnień EIOD

([79]) Dz.U. L 8 z 12.1.2001, str. 1.

w zakresie nadzoru wyłączone są jedynie te czynności, które znajdują się całkowicie poza obszarami wchodzącymi w skład „pierwszego filaru".

Definicje i treść tego rozporządzenia są zgodne z podejściem stosowanym w dyrektywie 95/46/WE. Można stwierdzić, że rozporządzenie (WE) nr 45/2001 jest wdrożeniem tej dyrektywy na poziomie europejskim. Wynika stąd, że rozporządzenie to zajmuje się ogólnymi zasadami, takimi jak zgodne z prawem i rzetelne przetwarzanie, proporcjonalność i użycie zgodne z przyjętymi celami, szczególne kategorie danych wrażliwych, informacje przekazywane podmiotowi danych, prawa podmiotu danych, obowiązki administratorów danych – uwzględniając w stosownych przypadkach szczególne okoliczności na poziomie UE – a także nadzorem, stosowaniem prawa i środków odwoławczych. Oddzielny rozdział zajmuje się ochroną danych osobowych i prywatności w kontekście wewnętrznych sieci telekomunikacyjnych. Rozdział ten jest faktycznie wdrożeniem na poziomie europejskim dyrektywy 97/66/WE o prywatności i łączności.

Interesującym aspektem tego rozporządzenia jest zobowiązanie instytucji i organów Wspólnoty do wyznaczenia co najmniej jednej osoby jako urzędnika ds. ochrony danych (DPO). Zadaniem tych urzędników jest zapewnienie niezależnego wewnętrznego stosowania przepisów rozporządzenia, w tym właściwego powiadamiania o operacjach przetwarzania. Wszystkie instytucje Wspólnoty i szereg organów mają teraz takich urzędników; niektórzy z nich działają od kilku lat. Oznacza to, że w celu wdrożenia tego rozporządzenia wykonano istotną pracę pomimo braku organu nadzoru. Urzędnikom tym może także być łatwiej udzielać rad oraz interweniować na wczesnym etapie, jak również pomagać w wypracowaniu dobrej praktyki. Ponieważ formalnym obowiązkiem DPO jest współpraca z EIOD, współdziałanie z tą siecią i jej rozwój są bardzo istotne i wartościowe (zob. pkt 2.2).

## Zadania i uprawnienia EIOD

Zadania i uprawnienia EIOD zostały precyzyjnie określone w art. 41, 46 i 47 wyżej wspomnianego rozporządzenia (zob. załącznik B), zarówno w kategoriach ogólnych, jak i szczegółowych. Artykuł 41 określa ogólną misję EIOD – zapewnienie poszanowania przez instytucje i organy wspólnotowe podstawowych praw i wolności osób fizycznych, w szczególności ich prywatności, w odniesieniu do przetwarzania danych osobowych. Ponadto określa on szersze aspekty szczegółowych elementów misji EIOD. Artykuły 46 i 47 rozwijają i precyzują te ogólne zadania, podając szczegółowy wykaz obowiązków i uprawnień.

Przedstawione zadania, obowiązki i uprawnienia są zasadniczo zbieżne z analogicznymi elementami działalności krajowych organów nadzoru i obejmują: wysłuchiwanie skarg oraz prowadzenie dochodzeń w związku z nimi, prowadzenie innych dochodzeń, informowanie administratorów i podmiotów danych, przeprowadzanie kontroli wstępnych, jeżeli operacje przetwarzania obciążone są konkretnym ryzykiem, itp. Rozporządzenie to uprawnia EIOD do uzyskania dostępu do stosownych informacji i miejsc, w przypadku gdy jest to niezbędne dla prowadzonych dochodzeń. EIOD może również nakładać kary i przekazać daną sprawę do rozpoznania Trybunałowi Sprawiedliwości. Te czynności ***nadzorcze*** zostały omówione bardziej wyczerpująco w rozdziale 2 niniejszego sprawozdania.

Niektóre zadania mają charakter specjalny. Zadanie polegające na udzielaniu porad Komisji i innym instytucjom Wspólnoty dotyczących nowego prawodawstwa – uwydatnione w art. 28 ust. 2 przez nałożenie na Komisję formalnego zobowiązania do konsultowania się z EIOD w przypadku przyjmowania wniosku prawodawczego odnoszącego się do ochrony danych osobowych – dotyczy także projektów dyrektyw i innych środków, które mają mieć zastosowanie na poziomie krajowym lub mają być wdrażane w ramach prawa krajowego. Jest to zadanie o znaczeniu strategicznym, umożliwiające EIOD analizę na wczesnym etapie wpływu na prywatność oraz omówienie wszelkich możliwych alternatywnych rozwiązań, również w ramach „trzeciego filaru" (współpracy policyjnej i sądowej w sprawach karnych). Istotnym zadaniem jest również monitorowanie stosownych bieżących wydarzeń mogących mieć wpływ na ochronę danych osobowych. Te czynności ***konsultacyjne*** omówiono obszerniej w rozdziale 3 niniejszego sprawozdania.

Obowiązek współpracy z krajowymi organami nadzoru oraz organami nadzoru „trzeciego filaru" ma podobny charakter. EIOD jest członkiem grupy roboczej art. 29 utworzonej w celu doradzania Komisji oraz opracowywania zharmonizowanych polityk, dzięki czemu może wnosić na tym poziomie swój wkład. Współpraca z organami nadzoru „trzeciego filaru" umożliwia EIOD śledzenie rozwoju sytuacji w tym zakresie, a także wnoszenie wkładu w opracowywanie bardziej spójnych i konsekwentnych ram ochrony danych osobowych, niezależnie od „filaru" lub konkretnego kontekstu. ***Współpracy*** tej poświęcono więcej miejsca w rozdziale 4 niniejszego sprawozdania.

Załącznik B

# Wyciąg z rozporządzenia (WE) nr 45/2001

## Artykuł 41 – Europejski inspektor ochrony danych

1. Niniejszym ustanawia się niezależny organ nadzoru nazywany europejskim inspektorem ochrony danych.
2. Europejski inspektor ochrony danych jest odpowiedzialny za zapewnienie, że podstawowe prawa i wolności osób fizycznych, w szczególności prawo do prywatności, są respektowane przez instytucje i organy wspólnotowe w odniesieniu do przetwarzania danych osobowych.

   Europejski inspektor ochrony danych jest odpowiedzialny za monitorowanie i zapewnienie zastosowania przepisów niniejszego rozporządzenia i każdego innego aktu wspólnotowego, odnoszącego się do podstawowych praw i wolności osób fizycznych, w odniesieniu do przetwarzania danych osobowych przez instytucje i organy wspólnotowe oraz za doradzanie instytucjom i organom wspólnotowym i podmiotom danych we wszystkich kwestiach związanych z przetwarzaniem danych osobowych. W tym celu wypełnia on obowiązki przewidziane w art. 46 i korzysta z uprawnień nadanych w art. 47.

## Artykuł 46 – Obowiązki

Europejski inspektor ochrony danych:

a) wysłuchuje i bada skargi oraz informuje podmiot danych o wyniku w odpowiednim czasie;
b) przeprowadza dochodzenia zarówno z własnej inicjatywy, jak i na podstawie skarg oraz informuje podmioty danych o ich wyniku w rozsądnym czasie;
c) monitoruje i zapewnia zastosowanie przepisów niniejszego rozporządzenia i każdego innego aktu wspólnotowego odnoszącego się do ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucję lub organ Wspólnoty, z wyjątkiem Trybunału Sprawiedliwości Wspólnot Europejskich działającego z mocy prawa;
d) doradza wszystkim instytucjom i organom wspólnotowym, albo z własnej inicjatywy, albo w odpowiedzi na konsultacje, we wszystkich kwestiach dotyczących przetwarzania danych osobowych, w szczególności zanim przyjmą przepisy wewnętrzne związane z ochroną podstawowych praw i wolności w odniesieniu do przetwarzania danych osobowych;
e) monitoruje rozwój w odpowiednich dziedzinach, o ile ma on wpływ na ochronę danych osobowych, w szczególności rozwój technologii informatycznych i telekomunikacyjnych;
f) (i) współpracuje z krajowymi organami nadzoru, do których odnosi się art. 28 dyrektywy 95/46/WE w krajach, do których ta dyrektywa ma zastosowanie, w stopniu koniecznym dla wykonywania ich obowiązków, w szczególności poprzez wymianę wszystkich użytecznych informacji i wnioskowanie, aby taka władza lub organ skorzystała ze swoich uprawnień lub odpowiadając na wniosek takiej władzy lub organu;
   (ii) współpracuje także z organami nadzoru w dziedzinie ochrony danych ustanowionymi przez tytuł VI Traktatu o Unii Europejskiej, w szczególności mając na względzie poprawę spójności i zastosowania reguł i procedur, za zapewnienie zgodności z którymi są odpowiednio odpowiedzialne;
g) bierze udział w działalności grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, o którym mówi art. 29 dyrektywy 95/46/WE;
h) określa, podaje powody i ogłasza wyłączenia z zabezpieczenia, upoważnienia i warunki wspomniane w art. 10 ust. 2 lit. b), ust. 4, 5 i 6, art. 12 ust. 2, art. 19 i art. 37 ust. 2;
i) prowadzi rejestr operacji przetwarzania, o których został powiadomiony na mocy art. 27 ust. 2 i które zostały zarejestrowane zgodnie z art. 27 ust. 5, oraz zapewnia metody dostępu do rejestrów prowadzonych przez inspektorów ochrony danych na mocy art. 26;
j) przeprowadza wstępne kontrole przetwarzania, o których został powiadomiony;
k) uchwala swój regulamin wewnętrzny.

## Artykuł 47 – Uprawnienia

1. Europejski inspektor ochrony danych może:

a) doradzać podmiotom danych w kwestii korzystania z ich praw;
b) przekazać sprawę administratorowi w przypadku domniemanego naruszenia przepisów rządzących przetwarzaniem danych osobowych i w miarę potrzeb zaproponować środki prawne dla usunięcia tego naruszenia i dla poprawy ochrony podmiotów danych;
c) nakazać, aby przyjęte zostały wnioski o skorzystanie z pewnych praw w odniesieniu do danych, gdy takie wnioski zostały odrzucone z naruszeniem art. 13–19;
d) ostrzec lub upomnieć administratora danych;
e) nakazać poprawę, zablokowanie, wykasowanie lub zniszczenie wszystkich danych, jeżeli były one przetwarzane z naruszeniem przepisów rządzących przetwarzaniem danych osobowych oraz powiadomienie o takich działaniach osób trzecich, którym dane zostały ujawnione;
f) nałożyć czasowy lub całkowity zakaz przetwarzania;
g) przekazać sprawę odpowiedniej instytucji lub organowi Wspólnoty i, jeśli to konieczne, Parlamentowi Europejskiemu, Radzie i Komisji;
h) przekazać sprawę Trybunałowi Sprawiedliwości Wspólnot Europejskich zgodnie z warunkami przewidzianymi w Traktacie
i) interweniować w sprawach wniesionych przed Trybunał Sprawiedliwości Wspólnot Europejskich.

2. Europejski inspektor ochrony danych ma uprawnienia:

a) do uzyskania od administratora lub instytucji bądź organu Wspólnoty dostępu do wszystkich danych osobowych i do wszystkich informacji koniecznych dla prowadzonych przez niego dochodzeń;
b) do uzyskania dostępu do pomieszczeń, w których administrator lub instytucja bądź organ Wspólnoty prowadzi działalność, jeżeli są wystarczające powody, aby przypuszczać, że prowadzona jest tam działalność podlegająca niniejszemu rozporządzeniu.

Załącznik C

# Wykaz skrótów

| | |
|---|---|
| ADS | (*Approved Destination Status*) status zatwierdzonego celu wyjazdów turystycznych |
| ALDE | (*Alliance of Liberals and Democrats for Europe*) Grupa Porozumienia Liberałów i Demokratów na rzecz Europy (grupa polityczna w PE) |
| API | (*Advance Passenger Information*) dane pasażera przekazane przed podróżą |
| CdT | Centrum Tłumaczeń dla organów Unii Europejskiej |
| CLP | wspólnotowy *laissez-passer* |
| CPVO | (*Community Plant Variety Office*) Wspólnotowy Urząd Ochrony Odmian Roślin |
| DG ADMIN | Dyrekcja Generalna ds. Personelu i Administracji |
| DG EAC | Dyrekcja Generalna ds. Edukacji i Kultury |
| DG EMPL | Dyrekcja Generalna ds. Zatrudnienia, Spraw Społecznych i Równości |
| DG INFSO | Dyrekcja Generalna ds. Społeczeństwa Informacyjnego i Mediów |
| DG JLS | Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa |
| DPA | (*Data Protection Authority*) organ ochrony danych |
| DPC | (*Data Protection Coordinator*) koordynator ds. ochrony danych |
| DPC | (*Data Protection Coordinator*) koordynator ds. ochrony danych (wyłącznie w Komisji Europejskiej) |
| DPO | (*Data Protection Officer*) urzędnik ds. ochrony danych |
| EBC | Europejski Bank Centralny |
| EBI | Europejski Bank Inwestycyjny |
| EFSA | (*European Food Safety Authority*) Europejski Urząd ds. Bezpieczeństwa Żywności |
| EKES | Europejski Komitet Ekonomiczno-Społeczny |
| EKOPC | Europejska konwencja praw człowieka |
| EMCDDA | (*European Monitoring Centre for Drugs and Drug Addiction*) Europejskie Centrum Monitorowania Narkotyków i Narkomanii |
| EMEA | (*European Medicines Agency*) Europejska Agencja Leków |
| EMPL | Komisja Zatrudnienia i Spraw Socjalnych w PE |
| EPSO | (*European Personnel Selection Office*) Europejskie Biuro Doboru Kadr |
| ESA | Europejska Szkoła Administracji |
| ETF | (*European Training Foundation*) Europejska Fundacja Kształcenia |
| ETS | Europejski Trybunał Sprawiedliwości |
| EUMC | Europejskie Centrum Monitorowania Rasizmu i Ksenofobii |
| EWS | system wczesnego ostrzegania |
| IAS | służba audytu wewnętrznego |
| KR | Komitet Regionów |
| LIBE | Komisja ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w PE |
| OHIM | (*Office of Harmonisation of the Internal Market*) Urząd Harmonizacji w ramach Rynku Wewnętrznego |
| OLAF | Europejski Urząd ds. Zwalczania Nadużyć Finansowych |
| PE | Parlament Europejski |
| PMO | Biuro Administrowania i Rozliczania Należności Indywidualnych |
| PNR | (*Passenger Name Record*) dane dotyczące przelotu pasażera |
| R&D | (*Research and Development*) badania i rozwój |
| RFID | (*Radio Frequency Identification*) identyfikacja radiowa |
| 7PR | siódmy program ramowy |
| SIS | system informacyjny Schengen |
| SWIFT | Towarzystwo Światowej Finansowej Telekomunikacji Międzybankowej Szans |
| Trzeci filar | współpraca policyjna i sądowa w sprawach karnych |
| UE | Unia Europejska |
| VIS | (*Visa Information System*) wizowy system informacyjny |
| WE | Wspólnoty Europejskie |

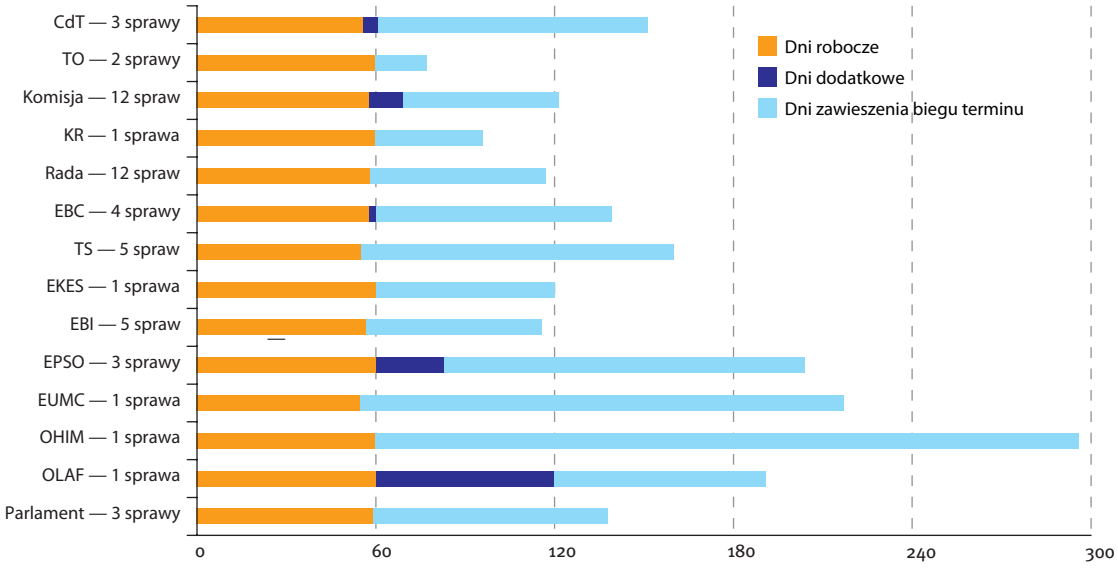
Załącznik D

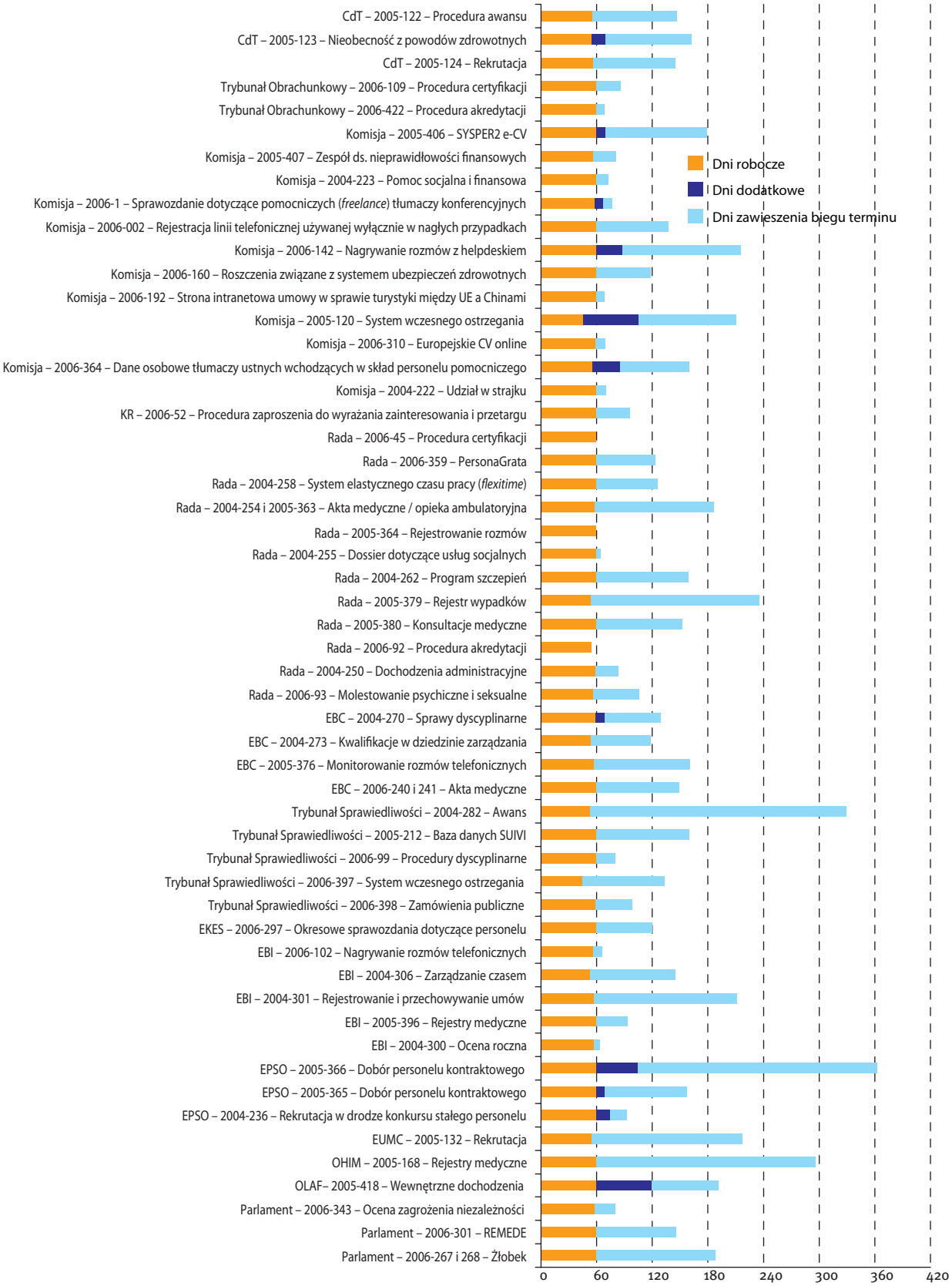
# Wykaz urzędników ds. ochrony danych (DPO)

| Organizacja | Nazwisko | E-mail |
|---|---|---|
| Parlament Europejski | Jonathan STEELE | dg5data-protection@europarl.europa.eu |
| Rada Unii Europejskiej | Pierre VERNHES | data.protection@consilium.europa.eu |
| Komisja Europejska | Philippe RENAUDIERE | data-protection-officer@ec.europa.eu |
| Trybunał Sprawiedliwości Wspólnot Europejskich | Marc SCHAUSS | dataprotectionofficer@curia.europa.eu |
| Trybunał Obrachunkowy Wspólnot Europejskich | Jan KILB | data-protection@eca.europa.eu |
| Europejski Komitet Ekonomiczno-Społeczny | *jeszcze niemianowany* | |
| Komitet Regionów | Maria ARSENE | data.protection@cor.europa.eu |
| Europejski Bank Inwestycyjny | Jean-Philippe MINNAERT | dataprotectionofficer@eib.org |
| Europejski Rzecznik Praw Obywatelskich | Loïc JULIEN | dpo-euro-ombudsman@europarl.europa.eu |
| Europejski Inspektor Ochrony Danych | Giuseppina LAURITANO | giuseppina.lauritano@edps.europa.eu |
| Europejski Bank Centralny | Martin BENISCH | dpo@ecb.int |
| Europejski Urząd ds. Zwalczania Nadużyć Finansowych | Laraine LAUDATI | Laraine.Laudati@ec.europa.eu |
| Centrum Tłumaczeń dla Organów Unii Europejskiej | Benoît VITALE | data-protection@cdt.europa.eu |
| Urząd Harmonizacji w ramach Rynku Wewnętrznego | Luc DEJAIFFE | dataprotectionofficer@oami.europa.eu |
| Europejskie Centrum Monitorowania Rasizmu i Ksenofobii | Jean-Marie ADJAHI | Jean-Marie.Adjahi@eumc.europa.eu |
| Europejska Agencja Leków | Vincenzo SALVATORE | data.protection@emea.europa.eu |
| Wspólnotowy Urząd Ochrony Odmian Roślin | Martin EKVAD | ekvad@cpvo.europa.eu |
| Europejska Fundacja Kształcenia | Romuald DELLI PAOLI | dataprotectionofficer@etf.europa.eu |
| Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji | Andreas MITRAKAS | dataprotection@enisa.europa.eu |
| Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy | Markus GRIMMEISEN | dataprotectionofficer@eurofound.europa.eu |
| Europejskie Centrum Monitorowania Narkotyków i Narkomanii | Arne TVEDT | arne.tvedt@emcdda.europa.eu |
| Europejski Urząd ds. Bezpieczeństwa Żywności | Claus REUNIS | DataProtectionOfficer@efsa.europa.eu |
| Europejska Agencja ds. Bezpieczeństwa na Morzu | Joachim MENZE | joachim.menze@emsa.europa.eu |
| Europejska Agencja Odbudowy | Olli KALHA | olli.kalha@ear.europa.eu |
| Europejskie Centrum Rozwoju Kształcenia Zawodowego (CEDEFOP) | Spyros ANTONIOU | spyros.antoniou@cedefop.europa.eu |
| Agencja Wykonawcza ds. Edukacji, Kultury i Sektora Audiowizualnego | Hubert MONET | hubert.monet@ec.europa.eu |

Załącznik E

# Czas trwania kontroli wstępnej w poszczególnych sprawach i instytucjach




CdT – 2005-122 – Procedura awansu
CdT – 2005-123 – Nieobecność z powodów zdrowotnych
CdT – 2005-124 – Rekrutacja
Trybunał Obrachunkowy – 2006-109 – Procedura certyfikacji
Trybunał Obrachunkowy – 2006-422 – Procedura akredytacji
Komisja – 2005-406 – SYSPER2 e-CV
Komisja – 2005-407 – Zespół ds. nieprawidłowości finansowych
Komisja – 2004-223 – Pomoc socjalna i finansowa
Komisja – 2006-1 – Sprawozdanie dotyczące pomocniczych (freelance) tłumaczy konferencyjnych
Komisja – 2006-002 – Rejestracja linii telefonicznej używanej wyłącznie w nagłych przypadkach
Komisja – 2006-142 – Nagrywanie rozmów z helpdeskiem
Komisja – 2006-160 – Roszczenia związane z systemem ubezpieczeń zdrowotnych
Komisja – 2006-192 – Strona intranetowa umowy w sprawie turystyki między UE a Chinami
Komisja – 2005-120 – System wczesnego ostrzegania
Komisja – 2006-310 – Europejskie CV online
Komisja – 2006-364 – Dane osobowe tłumaczy ustnych wchodzących w skład personelu pomocniczego
Komisja – 2004-222 – Udział w strajku
KR – 2006-52 – Procedura zaproszenia do wyrażania zainteresowania i przetargu
Rada – 2006-45 – Procedura certyfikacji
Rada – 2006-359 – PersonaGrata
Rada – 2004-258 – System elastycznego czasu pracy (flexitime)
Rada – 2004-254 i 2005-363 – Akta medyczne / opieka ambulatoryjna
Rada – 2005-364 – Rejestrowanie rozmów
Rada – 2004-255 – Dossier dotyczące usług socjalnych
Rada – 2004-262 – Program szczepień
Rada – 2005-379 – Rejestr wypadków
Rada – 2005-380 – Konsultacje medyczne
Rada – 2006-92 – Procedura akredytacji
Rada – 2004-250 – Dochodzenia administracyjne
Rada – 2006-93 – Molestowanie psychiczne i seksualne
EBC – 2004-270 – Sprawy dyscyplinarne
EBC – 2004-273 – Kwalifikacje w dziedzinie zarządzania
EBC – 2005-376 – Monitorowanie rozmów telefonicznych
EBC – 2006-240 i 241 – Akta medyczne
Trybunał Sprawiedliwości – 2004-282 – Awans
Trybunał Sprawiedliwości – 2005-212 – Baza danych SUIVI
Trybunał Sprawiedliwości – 2006-99 – Procedury dyscyplinarne
Trybunał Sprawiedliwości – 2006-397 – System wczesnego ostrzegania
Trybunał Sprawiedliwości – 2006-398 – Zamówienia publiczne
EKES – 2006-297 – Okresowe sprawozdania dotyczące personelu
EBI – 2006-102 – Nagrywanie rozmów telefonicznych
EBI – 2004-306 – Zarządzanie czasem
EBI – 2004-301 – Rejestrowanie i przechowywanie umów
EBI – 2005-396 – Rejestry medyczne
EBI – 2004-300 – Ocena roczna
EPSO – 2005-366 – Dobór personelu kontraktowego
EPSO – 2005-365 – Dobór personelu kontraktowego
EPSO – 2004-236 – Rekrutacja w drodze konkursu stałego personelu
EUMC – 2005-132 – Rekrutacja
OHIM – 2005-168 – Rejestry medyczne
OLAF– 2005-418 – Wewnętrzne dochodzenia
Parlament – 2006-343 – Ocena zagrożenia niezależności
Parlament – 2006-301 – REMEDE
Parlament – 2006-267 i 268 – Żłobek
Dni robocze
Dni dodatkowe
Dni zawieszenia biegu terminu
0
60
120
180
240
300
360
420

Załącznik F

# Wykaz opinii w sprawie kontroli wstępnych

**System wczesnego ostrzegania – Trybunał Sprawiedliwości**

Opinia z dnia 22 grudnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej systemu wczesnego ostrzegania (sprawa 2006-397)

**Dane osobowe tłumaczy ustnych wchodzących w skład personelu pomocniczego – Komisja**

Opinia z dnia 22 grudnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Zarządzanie danymi osobowymi tłumaczy ustnych wchodzących w skład personelu pomocniczego przechowywanymi w bazie Signalétique (aplikacja centralnej bazy danych CORALIN)" (sprawa 2006-364)

**Żłobek – Parlament**

Opinia z dnia 8 grudnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Akta medyczne – żłobek Parlamentu" oraz „Akta medyczne – żłobki prywatne" (sprawa 2006-267 i 2006-268)

**System wczesnego ostrzegania – Komisja**

Opinia z dnia 6 grudnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej systemu wczesnego ostrzegania (sprawa 2005-120)

**Zamówienia publiczne – Trybunał Sprawiedliwości**

Opinia z dnia 16 listopada 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Zamówienia publiczne" (sprawa 2006-398)

**REMEDE – Parlament**

Opinia z dnia 14 listopada 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „REMEDE" (sprawa 2006-301)

**Dobór personelu kontraktowego – EPSO**

Opinia z dnia 14 listopada 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Dobór personelu kontraktowego w kontekście jego rekrutacji przeprowadzanej przez instytucje europejskie oraz w razie potrzeby przez urzędy, organy i agencje wspólnotowe" (sprawa 2005-366)

**PersonaGrata – Rada**

Opinia z dnia 13 listopada 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „PersonaGrata" (moduł zarządzania zasobami ludzkimi) (sprawa 2006-359)

**Nagrywanie rozmów z helpdeskiem – Komisja**

Opinia z dnia 23 października 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Nagrywania rozmów z helpdeskiem" (sprawa 2006-142)

**Akta medyczne – Europejski Bank Centralny**

Opinia z dnia 20 października 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej akt medycznych przechowywanych przez doradcę EBC ds. medycznych oraz zapisywanie informacji medycznych w aktach osobowych (sprawy 2006-240/241)

**Okresowe sprawozdania dotyczące personelu – Europejski Komitet Ekonomiczno-Społeczny**

Opinia z dnia 19 października 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej okresowych sprawozdań dotyczących personelu (sprawa 2006-297)

**Procedura akredytacji – Trybunał Obrachunkowy**

Opinia z dnia 10 października 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Procedura certyfikacji" (sprawa 2006-422)

**Ocena zagrożenia niezależności – Parlament**

Opinia z dnia 25 września 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej oceny zagrożenia niezależności (sprawa 2006-343)

**Udział w strajku – Komisja**

Opinia z dnia 25 września 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej ogólnego podejścia administracyjnego do udziału w strajku (sprawa 2004-222)

**Europejskie CV on-line – Komisja**

Opinia z dnia 14 września 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej europejskiego CV online (sprawa 2006-310)

**Roszczenia związane z systemem ubezpieczeń zdrowotnych – Komisja**

Opinia z dnia 28 lipca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej procedury i systemu roszczeń związanych z systemem ubezpieczeń zdrowotnych w odniesieniu do tłumaczy ustnych wchodzących w skład personelu pomocniczego (sprawa 2006-160)

**Rejestr wypadków – Rada**

Opinia z dnia 25 lipca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Rejestr wypadków" (sprawa 2005-379)

**Rejestrowanie i przechowywanie umów – Europejski Bank Inwestycyjny**

Opinia z dnia 14 lipca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Rejestrowanie i przechowywanie umów zawieranych przez bank oraz zawieranych między bankiem a konsultantami zewnętrznymi" (sprawa 2004-301)

**Strona intranetowa umowy w sprawie turystyki między UE a Chinami – Komisja**

Opinia z dnia 30 czerwca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej umowy między UE a Chinami – status zatwierdzonego celu wyjazdów turystycznych (*Approved Destination Status – ADS*) (sprawa 2006-192)

**Zarządzanie czasem – Europejski Bank Inwestycyjny**

Opinia z dnia 26 czerwca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Zarządzanie czasem" (sprawa 2004-306)

**Wewnętrzne dochodzenia – OLAF**

Opinia z dnia 23 czerwca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej wewnętrznych dochodzeń prowadzonych przez OLAF (sprawa 2005-418)

**„Sysper2 e-CV" – Komisja**

Opinia z dnia 22 czerwca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „SYSPER2 e-CV, baza danych dotyczących kapitału ludzkiego Komisji" (sprawa 2005-406)

**Molestowanie psychiczne i seksualne – Rada**

Opinia z dnia 9 czerwca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej uregulowań wewnętrznych wprowadzonych w Sekretariacie Generalnym Rady (SGR) w zakresie molestowania psychicznego i seksualnego w pracy (sprawa 2006-93)

**Procedury dyscyplinarne – Trybunał sprawiedliwości**

Opinia z dnia 8 czerwca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej przetwarzania danych w ramach procedur dyscyplinarnych (sprawa 2006-99)

**Akta medyczne / opieka ambulatoryjna – Rada**

Opinia z dnia 29 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Akta medyczne" oraz „Opieka ambulatoryjna – rejestr pacjentów" (sprawy 2004-254 i 2005-363)

**Procedura certyfikacji – Trybunał Obrachunkowy**

Opinia z dnia 29 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Procedura certyfikacji" (sprawa 2006-109)

**Rejestracja linii telefonicznej używanej wyłącznie w nagłych przypadkach – Komisja**

Opinia z dnia 22 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej rejestracji linii telefonicznej używanej w Brukseli w nagłych wypadkach i w sprawach dotyczących bezpieczeństwa (nr 88888) (sprawa 2006-2)

**Dochodzenia administracyjne – Rada**

Opinia z dnia 16 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Decyzja dotycząca prowadzenia dochodzeń administracyjnych i procedury w tym zakresie oraz Komisji Dyscyplinarnej w Sekretariacie Generalnym Rady" (sprawa 2004-250)

**Nagrywanie rozmów telefonicznych – Europejski Bank Inwestycyjny**

Opinia z dnia 8 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej nagrywania rozmów telefonicznych w salach, w których przeprowadzane są rozmowy handlowe (sprawa 2006-102)

**„Program szczepień" – Rada**

Opinia z dnia 5 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Program szczepień" (sprawa 2004-262)

**Monitorowanie rozmów telefonicznych – Europejski Bank Centralny**

Opinia z dnia 5 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej nagrywania, przechowywania i słuchania rozmów telefonicznych w DG-M i DG-P (sprawa 2005-376)

**Konsultacje medyczne – Rada**

Opinia z dnia 4 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Rejestr konsultacji medycznych osób niepracujących w instytucji" nagrywania (sprawa 2005-380)

**Procedura zaproszenia do wyrażania zainteresowania i przetargu – Komitet Regionów**

Opinia z dnia 3 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Procedura zaproszenia do wyrażania zainteresowania i przetargu" (sprawa 2006-52)

**Dobór personelu kontraktowego – EPSO**

Opinia z dnia 2 maja 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Dobór personelu kontraktowego w kontekście jego rekrutacji przeprowadzanej przez instytucje europejskie oraz, w razie potrzeby, przez podmioty, organy i agencje wspólnotowe" (sprawa 2005-365)

**Rejestry medyczne – OHIM**

Opinia z dnia 28 kwietnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej rejestrów medycznych (sprawa 2005-168)

**Nieobecność z powodów zdrowotnych – Centrum Tłumaczeń**

Opinia z dnia 28 kwietnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Przetwarzanie danych związanych z nieobecnościami z powodów zdrowotnych oraz archiwizacja zaświadczeń lekarskich" (sprawa 2005-123)

**Procedura akredytacji – Rada**

Opinia z dnia 18 kwietnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Procedura akredytacji" (sprawa 2006-92)

**Rekrutacja – Centrum Tłumaczeń**

Opinia z dnia 10 kwietnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Procedura doboru do celów rekrutacji personelu" (Cdt-Da-5) (sprawa 2005-124)

**Procedura awansu – Centrum Tłumaczeń**

Opinia z dnia 7 kwietnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Procedura awansu" (Cdt-Da-3) (sprawa 2005-122)

**Awans – Europejski Trybunał Sprawiedliwości**

Opinia z dnia 7 kwietnia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Punkty stosowane w procedurze awansu; oceny i awanse" (sprawa 2004-282)

**Procedura certyfikacji – Rada**

Opinia z dnia 23 marca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Procedura certyfikacji" (sprawa 2006-45)

**Sprawozdanie dotyczące pomocniczych (*freelance*) tłumaczy konferencyjnych – Komisja**

Opinia z dnia 21 marca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej sytemu SERIF (system rejestrowania raportów dotyczących wyników pracy pomocniczych tłumaczy konferencyjnych – *Système d'Enregistrement de Rapports sur les Interprètes Freelance*) (sprawa 2006-1)

**Rejestry medyczne – Europejski Bank Inwestycyjny**

Opinia z dnia 17 marca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej rejestrów medycznych i zarządzania usługami (sprawa 2005-396)

**Zespół ds. nieprawidłowości finansowych – Komisja**

Opinia z dnia 15 marca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Stwierdzanie przez zespół ds. nieprawidłowości finansowych (PIF) istnienia oraz ewentualnych skutków nieprawidłowości finansowych w Komisji Europejskiej" (sprawa 2005-407)

**Pomoc socjalna i finansowa – Komisja**

Opinia z dnia 13 marca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej pomocy socjalnej i finansowej (sprawa 2004-223)

**Sprawy dyscyplinarne – Europejski Bank Centralny**

Opinia z dnia 8 marca 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Sprawy dyscyplinarne (w tym związane z nimi kontrole administracyjne skarg i zażaleń, sprawy prowadzone przez Rzecznika Praw Obywatelskich i Trybunał)" (sprawa 2004-270)

**Kwalifikacje w dziedzinie zarządzania – Europejski Bank Centralny**

Opinia z dnia 7 marca 2006 r. w sprawie wniosku o przeprowadzenie kontroli wstępnej dotyczącej dossier „Ocena kwalifikacji w dziedzinie zarządzania" (sprawa 2004-273)

**Rekrutacja w drodze konkursu stałego personelu – EPSO**

Opinia z dnia 24 lutego 2006 r. w sprawie dossier „Rekrutacja w drodze konkursu stałego personelu instytucji europejskich lub organów, urzędów i agencji wspólnotowych" (sprawa 2004-236)

**Ocena roczna – Europejski Bank Inwestycyjny**

Opinia z dnia 17 lutego 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Przeprowadzenie rocznej oceny wyników pracy" (sprawa 2004-300)

**Dossier dotyczące usług socjalnych – Rada**

Opinia z dnia 6 lutego 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier odnoszących się do usług socjalnych (sprawa 2004-255)

**Rekrutacja – Europejskie Centrum Monitorowania Rasizmu i Ksenofobii**

Opinia z dnia 1 lutego 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej operacji przetwarzania danych do celów rekrutacji (sprawa 2005-132)

**Rejestrowanie rozmów – Rada**

Opinia z dnia 23 stycznia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej rejestrowania rozmów prowadzonych za pośrednictwem linii telefonicznych, telefonów wewnętrznych, środków łączności radiowej użytkowanych przez Centrum Bezpieczeństwa (sprawa 2005-364)

**System elastycznego czasu pracy (*flexitime*) – Rada**

Opinia z dnia 19 stycznia 2006 w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej systemu elastycznego czasu pracy (*flexitime*) (sprawa 2004-258)

**Baza danych SUIVI – Trybunał Sprawiedliwości**

Opinia z dnia 13 stycznia 2006 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej dossier „Baza danych Suivi" (sprawa 2005-212)

Załącznik G

# Wykaz opinii w sprawie wniosków prawodawczych

**Rozporządzenie finansowe**

Opinia z dnia 12 grudnia 2006 r. w sprawie wniosków dotyczących zmiany rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich i przepisów wykonawczych do niego (COM(2006) 213 wersja ostateczna i SEC(2006) 866 wersja ostateczna)

**Ochrona danych w trzecim filarze**

Druga opinia z dnia 29 listopada 2006 r. w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych

**Wzajemna pomoc administracyjna**

Opinia z dnia 13 listopada 2006 r. na temat zmienionego wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie wzajemnej pomocy administracyjnej w celu ochrony interesów finansowych Wspólnoty Europejskiej przed nadużyciami finansowymi i wszelkimi innymi działaniami niezgodnymi z prawem

**Wspólne instrukcje konsularne**

Opinia z dnia 27 października 2006 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego wspólne instrukcje konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczące wiz w związku z wprowadzeniem technologii biometrycznych (COM (2006) 269 wersja ostateczna), Dz.U. C 321 z 29.12.2006, str. 38

**Dochodzenia prowadzone przez OLAF**

Opinia z dnia 27 października 2006 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF)

**Dokumenty pobytowe**

Opinia z dnia 16 października 2006 r. w sprawie zmienionego wniosku dotyczącego rozporządzenia Rady zmieniającego rozporządzenie (WE) nr 1030/2002 ustanawiające jednolity wzór dokumentów pobytowych dla obywateli państw trzecich, Dz.U. C 320 z 28.12.2006, str. 21

**Laissez-passer**

Opinia z dnia 13 października 2006 r. w sprawie projektu rozporządzenia Rady (WE) ustanawiającego postać dokumentu *laissez-passer*, który ma być wydawany członkom i pracownikom instytucji, Dz.U. C 313 z 20.12.2006, str. 36

**Rejestry karne**

Opinia z dnia 29 maja 2006 r. na temat wniosku dotyczącego decyzji ramowej Rady w sprawie organizacji wymiany informacji pochodzących z rejestrów karnych pomiędzy państwami członkowskimi oraz treści tych informacji (COM (2005) 690 wersja ostateczna), Dz.U. C 313 z 20.12.2006, str. 26

**Zobowiązania alimentacyjne**

Opinia z dnia 15 maja 2006 r. w sprawie wniosku dotyczącego rozporządzenia Rady w sprawie właściwości, prawa właściwego, uznawania i wykonywania orzeczeń sądowych oraz współpracy w zakresie zobowiązań alimentacyjnych (COM(2005) 649 wersja ostateczna), Dz.U. C 242 z 7.10.2006, str. 20

**Wymiana informacji w ramach zasady dostępności**

Opinia z dnia 28 lutego 2006 r. na temat wniosku dotyczącego decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności (COM (2005) 490 wersja ostateczna), Dz.U. C 116 z 17.5.2006, str. 8

**Wgląd do danych Systemu Informacji Wizowej (VIS) dla organów odpowiedzialnych za bezpieczeństwo wewnętrzne**

Opinia z dnia 20 stycznia 2006 r. na temat wniosku dotyczącego decyzji Rady w sprawie wglądu do danych Systemu Informacji Wizowej (VIS) dla organów państw członkowskich odpowiedzialnych za bezpieczeństwo wewnętrzne oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw (COM (2005) 600 wersja ostateczna), Dz.U. C 97 z 25.4.2006, str. 6

Załącznik H

# Skład sekretariatu EIOD

***Wydziały pod bezpośrednim zwierzchnictwem EIOD lub zastępcy inspektora:***

- **Nadzór**

Sophie LOUVEAUX
*Administrator / urzędnik ds. prawnych*

Rosa BARCELÓ
*Administrator / urzędnik ds. prawnych*

Zsuzsanna BELENYESSY
*Administrator / urzędnik ds. prawnych*

Eva DIMOVNÉ KERESZTES
*Administrator / urzędnik ds. prawnych*

Maria Veronica PEREZ ASINARI
*Administrator / urzędnik ds. prawnych*

Endre SZABÓ
*Ekspert krajowy / urzędnik ds. prawnych*

Stephen McCARTNEY
*Ekspert krajowy / urzędnik ds. prawnych*

Delphine HAROU (*)
*Asystent ds. nadzoru*

Xanthi KAPSOSIDERI
*Asystent ds. nadzoru*

Sylvie LONGRÉE
*Asystent ds. nadzoru*

Kim Thien LÊ
*Asystent ds. sekretariatu*

Jan DOBRUCKI
*Stażysta (od marca do czerwca 2006 roku)*

Mate SZABÓ
*Stażysta (od marca do czerwca 2006 roku)*

- **Polityka i informacja**

Hielke HIJMANS
*Administrator / urzędnik ds. prawnych*

Laurent BESLAY
*Administrator / urzędnik ds. technologii*

Bénédicte HAVELANGE
*Administrator / urzędnik ds. prawnych*

Alfonso SCIROCCO
*Administrator / urzędnik ds. prawnych*

Michaël VANFLETEREN
*Administrator / urzędnik ds. prawnych*

Per SJÖNELL (*)
*Administrator / rzecznik prasowy*

Martine BLONDEAU (*)
*Asystent ds. dokumentacji*

Andrea BEACH
*Asystent ds. sekretariatu*

Theodora TOUTZIARAKI
*Stażysta (od października 2006 roku do lutego 2007 roku)*

(*) Zespół ds. informacji.

**Sekcja Personel/Budżet/Administracja**

Monique LEENS-FERRANDO
*Kierownik sekcji*

Giuseppina LAURITANO
*Administrator / kwestie regulaminowe*
*Urzędnik ds. audytu i ochrony danych*

Vittorio MASTROJENI
*Asystent ds. zasobów ludzkich*

Anne LEVÊCQUE
*Asystent ds. zasobów ludzkich*

Anne-Françoise REINDERS
*Asystent ds. zasobów ludzkich*

Raja ROY
*Asystent ds. finansów i księgowości*

Valérie LEAU
*Asystent ds. księgowości*

Stéphane RENAUDIN
*Stażysta (od października 2006 roku do lutego 2007 roku)*

Załącznik I

# Wykaz porozumień administracyjnych i decyzji

Przedłużenie obowiązywania porozumienia administracyjnego podpisanego przez sekretarza generalnego Parlamentu Europejskiego, Rady i Komisji oraz przez Europejskiego Inspektora Ochrony Danych.

## Wykaz porozumień o gwarantowanym poziomie usług zawartych przez EIOD z innymi instytucjami

- Porozumienia o gwarantowanym poziomie usług zawarte z Komisją (Biuro ds. Staży Dyrekcji Generalnej ds. Edukacji i Kultury Komisji Europejskiej; DG ADMIN i DG EMPL)
- Porozumienie o gwarantowanym poziomie usług zawarte z Radą
- Porozumienie o gwarantowanym poziomie usług zawarte z Europejską Szkołą Administracji (ESA)
- Porozumienie administracyjne zawarte pomiędzy Europejskim Inspektorem Ochrony Danych a Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA)
- Porozumienie w sprawie harmonizacji kosztów międzyinstytucjonalnych kursów językowych

## Wykaz decyzji przyjętych przez EIOD

Decyzja EIOD z dnia 12 stycznia 2005 r. ustanawiająca ogólne przepisy wykonawcze dotyczące dodatków rodzinnych

Decyzja EIOD z dnia 27 maja 2005 r. ustanawiająca ogólne przepisy wykonawcze dotyczące programu stażowego

Decyzja EIOD z dnia 15 czerwca 2005 r. ustanawiająca ogólne przepisy wykonawcze dotyczące pracy w niepełnym wymiarze godzin

Decyzja EIOD z dnia 15 czerwca 2005 r. ustanawiająca przepisy wykonawcze dotyczące urlopu

Decyzja EIOD z dnia 15 czerwca 2005 r. ustanawiająca ogólne przepisy wykonawcze dotyczące kryteriów mających zastosowanie do ustalenia stopnia zaszeregowania w momencie mianowania lub podjęcia pracy

Decyzja EIOD z dnia 15 czerwca 2005 r. w sprawie przyjęcia elastycznego czasu pracy z możliwością odbioru przepracowanych nadgodzin

Decyzja EIOD z dnia 22 czerwca 2005 r. w sprawie przyjęcia wspólnych zasad ubezpieczenia urzędników Wspólnot Europejskich od ryzyka wypadku i choroby zawodowej

Decyzja EIOD z dnia 1 lipca 2005 r. ustanawiająca ogólne przepisy wykonawcze dotyczące urlopu rodzinnego

Decyzja EIOD z dnia 15 lipca 2005 r. w sprawie przyjęcia wspólnych zasad ubezpieczenia zdrowotnego urzędników Wspólnot Europejskich

Decyzja EIOD z dnia 25 lipca 2005 r. ustanawiająca przepisy wykonawcze dotyczące urlopu przyznawanego urzędnikom z przyczyn osobistych oraz urlopu bezpłatnego dla personelu zatrudnianego na czas określony i personelu kontraktowego Wspólnot Europejskich

Decyzja EIOD z dnia 25 lipca 2005 r. w sprawie działań zewnętrznych i kadencji

Decyzja EIOD z dnia 26 października 2005 r. ustanawiająca ogólne przepisy wykonawcze dotyczące dodatku na gospodarstwo domowe przyznawanego w drodze decyzji szczególnej

Decyzja EIOD z dnia 26 października 2005 r. ustanawiająca ogólne przepisy wykonawcze określające miejsce pochodzenia

Decyzja EIOD z dnia 7 listopada 2005 r. ustanawiająca szczególne dla EIOD procedury kontroli wewnętrznej

Decyzja EIOD z dnia 10 listopada 2005 r. określająca zasady oddelegowania do EIOD ekspertów krajowych

Decyzja EIOD z dnia 16 stycznia 2006 r. zmieniająca decyzję EIOD z dnia 22 czerwca 2006 r. w sprawie przyjęcia wspólnych zasad ubezpieczenia urzędników Wspólnot Europejskich od ryzyka wypadku i choroby zawodowej

Decyzja EIOD z dnia 16 stycznia 2006 r. zmieniająca decyzję EIOD z dnia 15 lipca 2005 r. w sprawie przyjęcia wspólnych zasad ubezpieczenia zdrowotnego urzędników Wspólnot Europejskich

Decyzja EIOD z dnia 26 stycznia 2006 r. w sprawie przyjęcia zasad dotyczących procedury przyznawania pomocy finansowej w formie dodatku do renty lub emerytury żyjącego małżonka, który cierpi z powodu poważnej lub przewlekłej choroby lub który jest niepełnosprawny

Decyzja EIOD z dnia 8 lutego 2006 r. w sprawie utworzenia komitetu pracowniczego w ramach EIOD

Decyzja EIOD z dnia 9 września 2006 r. w sprawie przyjęcia przepisów ustanawiających procedurę stosowania art. 45 ust. 2 regulaminu pracowniczego

Europejski Inspektor Ochrony Danych

**Sprawozdanie roczne 2006**

Luksemburg: Urząd Oficjalnych Publikacji Wspólnot Europejskich

2007 — 92 str. — 21 x 29,7 cm

ISBN 978-92-95030-26-8

QT-AA-07-001-PL-N