ISSN 1830-9518

Sprawozdanie roczne

2007

Europejski Inspektor
Ochrony Danych

Sprawozdanie roczne

2007

Europejski Inspektor
Ochrony Danych

Adres do korespondencji: Rue Wiertz 60, B-1047 Bruksela
Adres siedziby: Rue Montoyer 63, Bruksela, Belgia
E-mail: edps@edps.europa.eu
Internet: www.edps.europa.eu
Tel.: (32-2) 283 19 00
Faks: (32-2) 283 19 50

Europe Direct to serwis, który pomoże Państwu znaleźć odpowiedzi na pytania dotyczące Unii Europejskiej.

Numer bezpłatnej infolinii (*):

00 800 6 7 8 9 10 11

(*) Niektórzy operatorzy telefonii komórkowej nie udostępniają połączeń z numerami 00 800 lub pobierają za nie opłaty.

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

Dane katalogowe znajdują się na końcu niniejszej publikacji.

Luksemburg: Urząd Oficjalnych Publikacji Wspólnot Europejskich, 2008

ISBN 978-92-95030-50-3

Spis treści

Podręcznik użytkownika

Bezpośrednio po tekście podręcznika zamieszczono określenie misji i przedmowę przygotowaną 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 2007 r. i przedstawia cele na 2008 r.

Rozdział 2 – Nadzór, obszernie opisuje działania realizowane w celu zapewnienia wykonywania przez instytucje i organy WE obowiązków związanych z ochroną danych oraz monitorowania w tym kontekście tych instytucji i organów. Po ogólnym przeglądzie przedstawiono funkcję urzędników ds. ochrony danych (DPO) w administracji UE. Ten rozdział obejmuje analizę kontroli wstępnych (zarówno pod względem ilościowym, jak i merytorycznym), skarg (w tym współpracę z Europejskim Rzecznikiem Praw Obywatelskich), dochodzeń, polityki w zakresie kontroli oraz porad dotyczących środków administracyjnych, którymi zajmowano się w 2007 r. 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; koncentruje 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. Szczegółowo traktuje wyzwania, jakim w niedalekiej przyszłości będą musiały sprostać istniejące ramy ochrony danych.

Rozdział 4 – Współpraca, opisuje działania realizowane w ramach kluczowych forów, takich jak Grupa Robocza art. 29, w ramach wspólnych organów nadzoru trzeciego filaru UE, a także podczas europejskiej oraz międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych.

Rozdział 5 – Komunikacja, przedstawia działalność EIOD w zakresie przekazywania informacji i osiągnięcia w tej dziedzinie, a także pracę służby prasowej. Stanowi również przegląd wykorzystania różnych narzędzi komunikacji, takich jak strona internetowa, biuletyny, materiały informacyjne i imprezy służące zwiększeniu świadomości.

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

Sprawozdanie uzupełnia szereg **załączników**, które zawierają przegląd stosownych ram prawnych, przepisy rozporządzenia (WE) nr 45/2001, wykaz skrótów i akronimów, statystyki dotyczące kontroli wstępnych, wykaz urzędników ds. ochrony danych w poszczególnych instytucjach i organach UE, a także skład sekretariatu EIOD i wykaz porozumień administracyjnych i decyzji przyjętych przez EIOD.

Dostępne jest również **Streszczenie** niniejszego sprawozdania; jego celem jest przedstawienie – w skróconej formie – najważniejszych wydarzeń w działalności EIOD w 2007 r.

Osoby, które pragną uzyskać więcej informacji na temat EIOD, zachęcamy do odwiedzenia naszej strony internetowej, która pozostaje głównym narzędziem komunikacji: http://www.edps.europa.eu. Na stronie tej można również zaprenumerować nasz biuletyn.

Papierowe egzemplarze sprawozdania rocznego, jak również jego streszczenia, można zamówić u EIOD bezpłatnie. Dane kontaktowe znajdują się na naszej stronie internetowej w części „Contact" ([1]).

([1]) http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/12

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 Unii Europejskiej. EIOD jest odpowiedzialny za:

- monitorowanie i zapewnienie przestrzegania przepisów rozporządzenia (WE) 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");
- współpracę 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 UE, 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 czwarte roczne sprawozdanie z mojej działalności w charakterze Europejskiego Inspektora Ochrony Danych (EIOD), zgodnie z rozporządzeniem (WE) 45/2001 Parlamentu Europejskiego i Rady oraz z art. 286 Traktatu WE.

Niniejsze sprawozdanie obejmuje 2007 r. jako trzeci pełny rok działalności EIOD w charakterze 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.

Celem traktatu lizbońskiego podpisanego pod koniec 2007 r. jest zadbanie o to, aby Karta praw podstawowych UE stała się dokumentem prawnie wiążącym dla wszystkich instytucji i organów, a także dla państw członkowskich, w trakcie wykonywania przez nie prawa Unii. Oba dokumenty zapewniają skuteczniejszą ochronę danych osobowych; zawierają również zasady niezależnego nadzoru.

Stanowi to ważny punkt odniesienia w historii Unii Europejskiej, który należy jednak traktować również jako wyzwanie. Podstawowe zabezpieczenia zawarte w traktatach muszą zostać praktycznie wprowadzone w życie. Powyższe ma zastosowanie w przypadku przetwarzania danych przez instytucje i organy, ale także wtedy gdy podmioty te opracowują zasady i polityki mogące mieć wpływ na prawa i wolności obywateli w Europie.

Sprawozdanie dowodzi, że – nawet przy zasadach obowiązujących w 2007 r. – w dziedzinie nadzoru osiągnięto istotne postępy. Nacisk położony na mierzenie wyników zaowocował inwestycjami w zakresie spełniania wymogów dotyczących ochrony danych w większości instytucji i organów Wspólnoty. Są powody do zadowolenia, jednak aby osiągnąć pełną zgodność z przepisami, niezbędne są dalsze starania.

W dziedzinie konsultacji położono duży nacisk na potrzebę wypracowania jednolitych i skutecznych ram ochrony danych zarówno w obszarze pierwszego, jak i trzeciego filaru UE; osiągnięte wyniki nie zawsze były jednak satysfakcjonujące. W sprawozdaniu podkreślono również fakt, że konsultacyjną funkcję EIOD wykorzystuje się coraz częściej w różnych politykach.

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

Pragnę wreszcie wyrazić szczególne podziękowanie – również w imieniu Joaquína Bayo Delgado, zastępcy inspektora ochrony danych – członkom naszego personelu. Nieprzeciętne zalety naszego personelu nieustannie przyczyniają się do rosnącej skuteczności naszych działań.

Peter Hustinx
Europejski Inspektor Ochrony Danych

1. Bilans i perspektywy

1.1. Ogólny przegląd 2007 r.

Ramy prawne, w obrębie których działa Europejski Inspektor Ochrony Danych (EIOD) ([2]), przewidują wiele zadań i uprawnień umożliwiających podstawowe rozróżnienie trzech głównych funkcji. Funkcje te nadal służą jako strategiczne platformy działań EIOD i są odzwierciedleniem jego misji:

- funkcja nadzorcza – polega na monitorowaniu i zapewnieniu poszanowania przez instytucje i organy wspólnotowe ([3]) istniejących zabezpieczeń prawnych podczas przetwarzania danych osobowych;
- funkcja konsultacyjna – polega 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 – obejmuje 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, gdzie przedstawiono główne działania EIOD i postępy osiągnięte w 2007 r. Znaczenie informacji dotyczących tych działań oraz waga przekazywania tych informacji w pełni uzasadniają ich oddzielne potraktowanie w rozdziale 5, dotyczącym komunikacji. Większość tych działań opiera się na skutecznym zarządzaniu zasobami finansowymi, ludzkimi i innymi, co zostanie omówione w rozdziale 6.

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

([3]) Pojęcia „instytucje" i „organy" pojawiające się w rozporządzeniu (WE) 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_pl.htm.

Traktat lizboński, podpisany w dniu 13 grudnia 2007 r., zakończył okres rozważań nad rolą, strukturą i funkcjonowaniem Unii Europejskiej. W dniu 12 grudnia 2007 r. w Strasburgu podpisano nieco zmieniony tekst Karty praw podstawowych UE. Chociaż karta nie jest już częścią traktatu, będzie dokumentem prawnie wiążącym dla wszystkich instytucji i organów UE, a także dla państw członkowskich, w trakcie stosowania przez nie prawa Unii. Ochrona danych osobowych, w tym potrzeba niezależnego nadzoru, jest wyraźnie wyeksponowana w obu dokumentach; zgodnie z zamierzeniami kwestia ta będzie miała skutki horyzontalne. EIOD będzie uważnie śledził rozwój wydarzeń w tej dziedzinie.

Wzmocniona ochrona danych osobowych przewidziana w traktacie lizbońskim daje również instytucjom sposobność pokazania, w jaki sposób należy taką ochronę zapewniać w praktyce. EIOD od samego początku podkreślał, że wiele polityk UE jest uzależnionych od zgodnego z prawem przetwarzania danych osobowych oraz że skuteczną ochronę danych osobowych, jako jedną z podstawowych wartości leżących u podstaw polityk UE, należy postrzegać jako warunek ich powodzenia. EIOD będzie nadal działał w tym ogólnym duchu; z zadowoleniem stwierdza również, że takie działanie spotyka się z coraz większym poparciem.

Kontrole wstępne pozostały głównym aspektem nadzoru w 2007 r. Z terminem pomiaru postępów w wykonywaniu rozporządzenia (WE) nr 45/2001, który według ustaleń EIOD przypadał na wiosnę 2007 r., wiązał się imponujący wzrost liczby powiadomień dotyczących przeprowadzenia kontroli wstępnej, a co za tym idzie liczby stosownych opinii wydanych przez EIOD. Całkowita liczba dopuszczalnych skarg również znacznie wzrosła. Wszystkie instytucje i organy Wspólnoty, w tym niedawno ustanowione agencje, zadbały o to, aby został w nich wyznaczony urzędnik ds. ochrony danych (zob. rozdział 2).

Rozwój działań konsultacyjnych przebiegał zadowalająco. Szczególny nacisk położono na potrzebę wypracowania jednolitych i skutecznych ram ochrony danych zarówno w obszarze pierwszego, jak i trzeciego filaru. W tym ostatnim przypadku wyniki nie były jednak satysfakcjonujące. W związku z wykazem wniosków Komisji, który opublikowano pod koniec 2006 r., EIOD zajmował się coraz szerszym zakresem obszarów polityki, co pociągało za sobą wzrost liczby opinii, uwag i innych działań na różnych etapach procesu prawodawczego. Uwagę należało także poświęcić pewnej liczbie interesujących spraw sądowych (zob. rozdział 3).

We współpracy z krajowymi organami nadzoru koncentrowano się na roli Grupy Roboczej Art. 29, co zaowocowało przyjęciem ważnych dokumentów dotyczących kwestii o strategicznym znaczeniu. EIOD odgrywał również istotną rolę w skoordynowanym nadzorowaniu systemu Eurodac. Działania w tej dziedzinie będzie można wykorzystać podczas prac nad innymi dużymi systemami informacyjnymi. Dużo uwagi poświęcono także lepszej współpracy w ramach trzeciego filaru. EIOD zajmował się również działaniami podejmowanymi w następstwie tzw. inicjatywy londyńskiej, której celem jest zwiększenie świadomości w zakresie ochrony danych i zwiększanie efektywności tej ochrony (zob. rozdział 4).

1.2. Wyniki w 2007 r.

W sprawozdaniu rocznym z 2006 r. wspomniano, że na 2007 r. wybrano wymienione poniżej cele główne. Większość z nich została w pełni lub częściowo zrealizowana.

- **Rozmiar sieci DPO**

Sieć urzędników ds. ochrony danych osiągnęła stan docelowy i objęła działalnością wszystkie instytucje i organy Wspólnoty. EIOD w dalszym ciągu udzielał silnego wsparcia i przedstawiał wytyczne w zakresie rozwoju funkcji urzędników ds. ochrony danych, ze szczególnym uwzględnieniem nowo mianowanych urzędników.

- **Kontynuacja kontroli wstępnych**

Liczba kontroli wstępnych związanych z przeprowadzanymi w omawianym okresie operacjami przetwarzania danych znacznie wzrosła, choć większość instytucji i organów musi nadal pracować, by wywiązać się ze swoich obowiązków w tym zakresie. Wyniki kontroli wstępnych są regularnie przekazywane DPO i innym stosownym podmiotom.

- **Inspekcje i kontrole**

EIOD rozpoczął mierzenie postępów w zakresie wykonania rozporządzenia (WE) nr 45/2001 od wiosny 2007 r. Wszystkie instytucje i organy wzięły udział w realizowaniu tego zadania, koncentrowano się jednak na poszczególnych etapach rozwoju. Wyniki – zarówno ogólne, jak i dotyczące poszczególnych przypadków – zostały przedstawione w sprawozdaniu; w rozdziale 2 znajduje się ich podsumowanie.

- **Nadzór wideo**

EIOD zakończył badania nad praktykami dotyczącymi nadzoru wideo zarówno na poziomie UE, jak i w poszczególnych państwach członkowskich; zajął się również różnymi przypadkami wiążącymi się z poszczególnymi instytucjami lub organami. Na podstawie tych działań zostanie sporządzony projekt wytycznych, który w 2008 r. zostanie zamieszczony na stronie internetowej EIOD.

- **Zagadnienia horyzontalne**

Opinie na temat kontroli wstępnych i decyzje w sprawie skarg są przedmiotem stałej analizy pod kątem zagadnień horyzontalnych. Pierwsze dokumenty zawierające wytyczne dla wszystkich instytucji i organów Wspólnoty zostaną opublikowane w 2008 r. Zagadnienia dotyczące przechowywania danych medycznych lub dyscyplinarnych zostały omówione ze stosownymi organami.

- **Konsultacje w sprawie prawodawstwa**

EIOD wydawał opinie na temat wniosków dotyczących nowego prawodawstwa i zapewniał odpowiedni monitoring. Funkcja doradcza obejmuje szerszy wachlarz tematów, a jej podstawą jest systematyczny spis i wybór priorytetów, których przygotowanie w pełni wspierają stosowne służby Komisji; EIOD pełni tę funkcję drugi rok.

- **Ochrona danych w trzecim filarze**

EIOD zwracał szczególną uwagę na opracowanie i terminowe przyjęcie ogólnych ram ochrony danych w trzecim filarze. Regularnie zajmował się także wnioskami dotyczącymi wymiany danych osobowych pomiędzy poszczególnymi państwami, zwłaszcza

w kontekście konwencji z Prüm. W obu przypadkach wyniki były niestety ograniczone.

- **Przekazywanie informacji na temat ochrony danych**

EIOD udzielał silnego wsparcia działaniom podejmowanym w następstwie tzw. inicjatywy londyńskiej, mającej na celu „przekazywanie informacji na temat ochrony danych i zwiększanie jej efektywności". Obejmowały one starania mające na celu wymianę najlepszych praktyk w dziedzinie egzekwowania prawa oraz rozwoju strategicznego z organami ds. ochrony danych z różnych krajów na całym świecie.

- **Regulamin wewnętrzny**

Przygotowanie regulaminu wewnętrznego obejmującego poszczególne funkcje i działania EIOD pochłonęło więcej czasu niż się spodziewano. Osiągnięto zadowalające postępy w zakresie opracowywania wewnętrznych podręczników dotyczących różnych przypadków. W 2008 r. zostanie przyjęty i opublikowany regulamin wewnętrzny wraz z informacjami praktycznymi dla zainteresowanych stron dostępnymi na stronie internetowej.

- **Zarządzanie zasobami**

EIOD udoskonalał zarządzanie zasobami finansowymi i ludzkimi w drodze odnowienia struktury budżetowej, przyjęcia wewnętrznych procedur w dziedzinie oceny personelu oraz opracowania polityki szkoleń. Kolejne przykłady ulepszeń w tej dziedzinie to wdrożenie systemu kontroli wewnętrznej i wyznaczenie urzędnika ds. ochrony danych.

1.3. Cele na 2008 r.

Na 2008 r. wybrano następujące główne cele. Wyniki osiągnięte w trakcie ich realizacji zostaną przedstawione w sprawozdaniu w przyszłym roku.

- **Rozmiar sieci DPO**

EIOD nadal będzie silnie wspierać urzędników ds. ochrony danych działających w poszczególnych instytucjach i organach, w szczególności w niedawno ustanowionych agencjach; będzie także zachęcał do dalszej wymiany wiedzy fachowej i najlepszych praktyk między takimi urzędnikami.

- **Rola kontroli wstępnych**

EIOD zamierza zakończyć kontrole wstępne przeprowadzane w omawianym okresie operacji przetwarzania danych w odniesieniu do większości instytucji i organów oraz położyć nacisk na realizację stosownych zaleceń. Wyniki kontroli wstępnych zostaną przekazane DPO i innym stosownym podmiotom.

- **Wytyczne horyzontalne**

Opracowane zostaną wytyczne dotyczące istotnych kwestii wspólnych dla większości instytucji i organów (np. przetwarzanie danych dotyczących zdrowia, zapewnienie dostępu podmiotom danych oraz sposób postępowania z nadzorem wideo). Wytyczne te będą szeroko dostępne. Dla zainteresowanych stron zostanie zorganizowana seria seminariów.

- **Pomiar zgodności**

EIOD będzie kontynuował mierzenie postępów w wykonywaniu rozporządzenia (WE) nr 45/2001, któremu będą towarzyszyć różnego rodzaju kontrole we wszystkich instytucjach i organach; coraz częściej będą przeprowadzane kontrole na miejscu. EIOD opublikuje również ogólną politykę w zakresie kontroli.

- **Duże systemy**

EIOD, wraz z krajowymi organami nadzoru, będzie w dalszym ciągu rozwijał skoordynowany nadzór nad Eurodac; w niedalekiej przyszłości będzie również rozwijał wiedzę fachową niezbędną do nadzorowania innych dużych systemów, takich jak SIS II i VIS.

- **Opinie na temat prawodawstwa**

Na podstawie systematycznego spisu stosownych tematów i priorytetów EIOD będzie w dalszym ciągu, w stosownym terminie, wydawał opinie lub zgłaszał uwagi na temat wniosków dotyczących nowego prawodawstwa; zapewni także odpowiedni monitoring.

- **Traktat lizboński**

EIOD nadal będzie śledził wydarzenia związane z traktatem lizbońskim i bacznie analizował jego wpływ na ochronę danych; w razie potrzeby będzie w przedmiotowej kwestii doradzał.

- **Informacje *on-line***

EIOD zamierza aktualizować i poszerzać informacje na swojej stronie internetowej, a także udoskonalać biuletyn elektroniczny.

- **Regulamin wewnętrzny**

EIOD przyjmie i opublikuje regulamin wewnętrzny, obejmujący poszczególne funkcje i działania inspektora. Praktyczne narzędzia dla zainteresowanych podmiotów będą dostępne na stronie internetowej.

- **Zarządzanie zasobami**

EIOD będzie konsolidował i w dalszym stopniu rozwijał niektóre z działań związanych z zasobami finansowymi i ludzkimi; poprawi również inne, wewnętrzne procedury pracy. Dla przyszłych pracowników będzie potrzebna dodatkowa powierzchnia biurowa.

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 (WE) nr 45/2001 („rozporządzenie") określa i przyznaje szereg obowiązków i uprawnień EIOD, umożliwiających mu sprawowanie nadzoru.

Kontrole wstępne pozostały głównym aspektem nadzoru w 2007 r. Zadanie to obejmuje analizę działań instytucji i organów w dziedzinach, które mogą stwarzać szczególne zagrożenie dla podmiotów danych, zgodnie z art. 27 rozporządzenia. Jak wyjaśniono poniżej, kontrolowanie obecnie przeprowadzanych operacji przetwarzania danych, w połączeniu z planowanymi operacjami, zapewnia dokładny obraz przetwarzania danych osobowych w instytucjach i organach. EIOD przeprowadził kontrole wstępne operacji przetwarzania danych w większości istotnych kategorii. Szczególną uwagę poświęcono systemom międzyinstytucjonalnym, a także sytuacjom, w których instytucje i organy wspólnie korzystają z określonych zasobów, z myślą o usprawnieniu i uproszczeniu procedur. Opinie EIOD pozwalają administratorom danych dostosowywać przeprowadzane przez nich operacje przetwarzania danych w taki sposób, aby były one zgodne z rozporządzeniem. EIOD dysponuje również innymi metodami, takimi jak rozpatrywanie skarg, prowadzenie dochodzeń i inspekcji oraz udzielanie porad dotyczących środków administracyjnych.

Jeśli chodzi o uprawnienia nadane EIOD, w 2007 r., podobnie jak w latach poprzednich, nie było konieczne wydanie żadnego nakazu, ostrzeżenia ani zakazu, jako że administratorzy danych wykonywali zalecenia EIOD lub wyrażali zamiar ich wykonania, podejmując niezbędne kroki. Szybkość reakcji różni się w poszczególnych przypadkach. EIOD opracował systematyczny monitoring wykonywania zaleceń.

Joaquín Bayo Delgado, zastępca inspektora

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.

Inspektorzy ochrony danych podczas 20. posiedzenia w Brukseli (8 czerwca 2007 r.)

Od kilku lat DPO spotykają się regularnie, aby wymieniać doświadczenia i omawiać zagadnienia horyzontalne. Ta nieformalna sieć okazała się pożyteczna z punktu widzenia współpracy. Funkcjonowała ona także w 2007 r.

W 2007 r. DPO Europolu został przyjęty do sieci w charakterze obserwatora.

EIOD uczestniczył w części każdego z posiedzeń z udziałem DPO zorganizowanych: w marcu 2007 r. (AESM, Lizbona), czerwcu 2007 r. (Rada, Bruksela) i w październiku 2007 r. (Urząd Harmonizacji Rynku Wewnętrznego – OHIM, Alicante). 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 z najważniejszych kwestii poruszonych podczas przeprowadzania kontroli wstępnych. W szczególności doprecyzowano zakres zastosowania art. 27, uwzględniając mianowicie takie przypadki, jak systemy łączności elektronicznej, systemy audytu wewnętrznego i dochodzenia prowadzone przez DPO. Posiedzenia te dały również EIOD okazję do nakreślenia postępów osiągniętych w zakresie rozpatrywania spraw dotyczących kontroli wstępnej oraz do przekazania szczegółowych informacji na temat ustaleń poczynionych w wyniku przeprowadzania kontroli wstępnych (zob. pkt 2.3 poniżej).

EIOD wykorzystał posiedzenia DPO do przekazania tym urzędnikom informacji na temat inspekcji „wiosna 2007" (zob. pkt 2.6.1). Wyjaśniono cel tej inspekcji, opisano metody jej przeprowadzania i zarysowano ukierunkowane działania, które mogą zostać podjęte w jej następstwie. Posiedzenia DPO dały także tym urzędnikom sposobność do przekazania informacji zwrotnych na temat wpływu tej inspekcji na ich instytucje oraz umożliwiły EIOD uwzględnienie pewnych czynników.

Utworzono „kwartet DPO" złożony z czterech DPO (z Rady, Parlamentu Europejskiego, Komisji Europejskiej i OHIM) z myślą o koordynowaniu sieci tych urzędników. EIOD ściśle współpracował z tym kwartetem, w szczególności nad przygotowywaniem porządków posiedzeń.

Równolegle z czerwcowym posiedzeniem w Brukseli EIOD, z pomocą kilku doświadczonych DPO, 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. Wyjaśniono również główne zadania DPO, a także przedstawiono prezentację dotyczącą formularzy powiadomienia, rejestrów powiadomień DPO oraz narzędzi informatycznych.

W 2007 r. grupa robocza ds. terminów przechowywania danych, ds. blokowania i ds. usuwania danych

odbyła sześć posiedzeń roboczych. Brali w nich udział zastępca EIOD oraz dwóch członków personelu. Opracowano projekt dokumentu w sprawie wniosków z pracy tej podgrupy; będzie on rozpowszechniany w 2008 r. przez członków grupy roboczej wśród wybranych osób w ich instytucjach lub organach (np. wśród informatyków). Członkowie grup również przygotowali i omówili dokument poświęcony stosownym zasadom dotyczącym terminów i blokowania.

W ramach inspekcji „wiosna 2007" EIOD położył nacisk na obowiązek prawny wyznaczenia DPO, jaki ma każda instytucja i każdy organ UE (zob. pkt 2.6.1).

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 r., 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 konkretne 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 ([4]);
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 nieuwzględnionych w odpowiednim ustawodawstwie krajowym lub legislacji wspólnotowej;
d) operacje przetwarzania w celu pozbawienia jednostki prawa, świadczenia lub wyłączenia jej z umowy.

Kryteria opracowane w latach poprzednich nadal były stosowane podczas interpretacji tego przepisu zarówno podczas podejmowania decyzji, zgodnie z którą dane powiadomienie od DPO nie podlega kontroli wstępnej, jak i podczas doradzania w sprawie konsultacji dotyczącej 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 wypadku 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 od 7 do 10 dni ([5])), jaki DPO danej instytucji lub organu

([4]) *Sûreté* w języku francuskim, tzn. środki przyjęte w ramach postępowania prawnego.
([5]) Dni roboczych, gdy zbiegają się z okresami wakacyjnymi.

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.

W przypadkach spraw dotyczących kontroli *ex post* zgłoszonych przed wrześniem 2007 r., w związku z olbrzymią liczbą spraw (zob. wykres w pkt 2.3.3), z obliczeń wyłączono sierpień zarówno w odniesieniu do instytucji/organów, jak i EIOD.

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 musi być ogólnodostępny.

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.

Aby zachować zgodność z zasadą przejrzystości, wszystkie informacje są zawarte w publicznym rejestrze (z wyjątkiem środków bezpieczeństwa, które nie są wymieniane w rejestrze) i są ogólnodostępne.

Opinia, po tym jak zostanie wydana przez EIOD, jest 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 stanowisko końcowe EIOD przyjmuje postać opinii, o której należy powiadomić administratora danych odnośnej 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. Jedynie w dwóch opiniach wydanych w 2007 r. (właściwe sprawy dotyczące kontroli wstępnej 2007-373 i 2007-680, zob. poniżej) wnioski były odmienne – operacje przetwarzania stanowiły naruszenie przepisów rozporządzenia i należało wykonać pewne zalecenia, aby odpowiednio dostosować te operacje.

Po raz pierwszy w 2007 r. przedmiotem powiadomienia stały się zmiany w operacjach, które wcześniej zostały poddane kontroli wstępnej. Dla tych spraw opracowano skróconą formę opinii.

Opracowano podręcznik rozpatrywania spraw, aby zagwarantować, podobnie jak w innych obszarach, pracę całego zespołu na takiej samej podstawie oraz przyjmowanie opinii EIOD 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).

Zebranie zespołu inspektorów

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.

1) Dokumentacja medyczna (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.

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

Rozporządzenie weszło w życie 1 lutego 2001 r. Jego art. 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 (tzn. do 1 lutego 2002 r.). Mianowanie EIOD i jego zastępcy nabrało mocy 17 stycznia 2004 r.

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 r. 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 w ich odnośnych instytucjach sytuacji od 2004 r. w zakresie operacji przetwarzania objętych art. 27. Po otrzymaniu informacji od wszystkich DPO sporządzono, a następnie poprawiono, wykaz spraw podlegających kontroli wstępnej *ex post.*

W latach 2005 i 2006 kategorie te traktowano jako kategorie priorytetowe, jednak aby w pełni skoncentrować się na dotrzymaniu terminu „wiosna 2007", nie stosowano ich już do ustalania hierarchii ważności, a wyłącznie do celów systematycznych kontroli. Właściwe sprawy dotyczące kontroli wstępnej nigdy nie podlegały powyższej kategoryzacji, ponieważ muszą być rozpatrywane przed rozpoczęciem danej operacji przetwarzania.

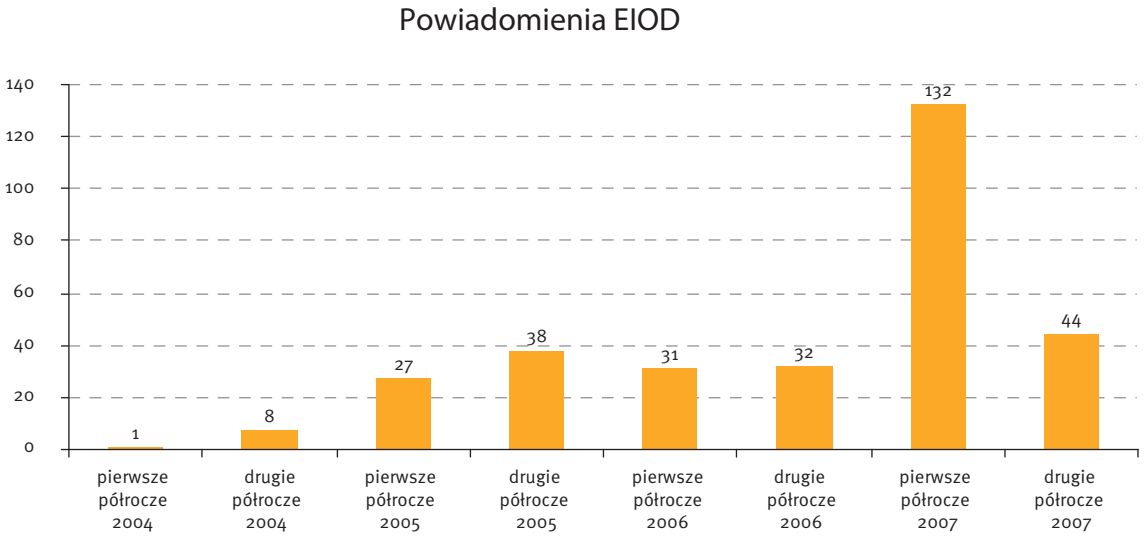
2.3.3. Analiza ilościowa

Powiadomienia dotyczące przeprowadzenia kontroli wstępnej

Jak wspomniano w sprawozdaniu rocznym, zarówno za 2005, jak i 2006 r., EIOD nieustannie zachęcał urzędników ds. ochrony danych do zwiększania liczby powiadomień o przeprowadzeniu kontroli wstępnej kierowanych do EIOD.

Jako termin otrzymania powiadomień podlegających kontroli wstępnej przez EIOD – były to przypadki *ex post* – przyjęto wiosnę 2007 r., aby skłonić instytucje i organy Wspólnoty do intensywniejszych starań służących pełnemu wywiązaniu się z obowiązku dotyczącego powiadomień.

Skutkiem powyższego działania był istotny wzrost liczby powiadomień. 132 powiadomienia między 1 stycznia 2007 r., a 30 czerwca 2007 r. w porównaniu do ogólnej liczby 137 przed tym okresem (32 w drugiej



Rada Unii Europejskiej	3 sprawy
Komisja Europejska	19 spraw
Europejski Bank Centralny (EBC)	5 spraw
Europejski Trybunał Sprawiedliwości (ETS)	5 spraw
Europejski Bank Inwestycyjny (EBI)	1 sprawa
Parlament Europejski	11 spraw
Centrum Tłumaczeń dla organów Unii Europejskiej (CdT)	1 sprawa
Europejski Urząd Doboru Kadr (EPSO) (*)	1 sprawa
Trybunał Obrachunkowy (CoA)	3 sprawy
Komitet Regionów (CoR)	4 sprawy
Europejski Rzecznik Praw Obywatelskich	7 spraw
Urząd Harmonizacji Rynku Wewnętrznego (OHIM)	7 spraw
Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF)	25 spraw (14 opinii)
Wspólnotowy Urząd Ochrony Odmian Roślin (CPVO)	1 sprawa
Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA)	1 sprawa
Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA)	1 sprawa
Europejska Agencja Leków (EMEA)	2 sprawy
Europejska Agencja ds. Bezpieczeństwa na Morzu (EMSA)	2 sprawy
Europejska Fundacja Kształcenia (ETF)	2 sprawy

(*) EPSO korzysta z usług DPO Komisji.

połowie 2006 r.) plus 44 powiadomienia w drugiej połowie 2007 r. Rzeczywistym skutkiem ustalenia terminu „wiosna 2007" było zatem wpłynięcie 208 (132 + 32 + 44) powiadomień z 313, które wpłynęły ogółem między 2004 r. a końcem 2007 r.

Opinie na temat spraw dotyczących kontroli wstępnej wydane w 2007 r.

W 2007 r. wydano 90 opinii ([6]) dotyczących powiadomień o przeprowadzeniu kontroli wstępnej.

Tych 101 spraw zakończonych formalną opinią stanowi wzrost czynności związanych z kontrolą wstępną o 77,19% w porównaniu z 2006 r. Takie obciążenie pracą jest z pewnością związane ze wspomnianym wyżej terminem wyznaczonym na wiosnę 2007 r. ([7]).

Z tych 101 spraw dotyczących kontroli wstępnej (90 opinii) tylko 11 to właściwe sprawy dotyczące kontroli wstępnej, tzn. zainteresowane instytucje (Trybunał Obrachunkowy, Parlament, EPSO, Europejski Rzecznik Praw Obywatelskich, EFK, EBC, EBI i OLAF po jednym przypadku oraz trzy Komisja) zastosowały procedurę obowiązującą w wypadku przeprowadzania kontroli wstępnych przed rozpoczęciem operacji przetwarzania.

([6]) Ze 101 powiadomień – z przyczyn praktycznych i z uwagi na fakt, że niektóre sprawy były powiązane – 15 powiadomień z OLAF potraktowano łącznie w czterech różnych opiniach. Dlatego na 101 powiadomień wydano 90 opinii.

([7]) Zob. pkt 2.3.7 dotyczący pozostałych 31 spraw sfinalizowanych w 2007 r.

- Z 11 spraw dotyczących kontroli wstępnej 4 (trzy sprawy zgłoszone przez Komisję i jedna przez EFK) były związane z systemem *flexitime* (system elastycznego czasu pracy);
- 2 z 11 były związane z nienależytym wykonywaniem obowiązków przez pracowników;
- pozostałe odnosiły się do uzależnienia awansu od spełnienia wymogu dotyczącego znajomości trzeciego języka, zarządzania urlopami, zasad dotyczących postępowania sprawdzającego, rejestrów medycznych i zarządzania usługami oraz systemu powiadamiania o nadużyciach (zob. także pkt 2.3.5).

Należy zauważyć, że wspomniane dwie operacje przetwarzania, które naruszały rozporządzenie (jedna związana z konkretnym systemem *flexitime,* a druga z rejestrami medycznymi), należą do wspomnianych 11 właściwych spraw dotyczących kontroli wstępnej. Pozostałe 90 spraw (79 opinii) to sprawy dotyczące kontroli wstępnej *ex post.*

Poza wspomnianymi 101 sprawami, w związku z którymi została wydana opinia, EIOD zajmował się również 31 sprawami, które uznano za niepodlegające kontroli wstępnej. Spośród tych raczej licznych spraw, tzw. spraw niepodlegających kontroli wstępnej (23,48% ogólnej liczby 132 spraw sfinalizowanych w 2007 r.), 11 należało do kategorii e-monitoringu. Analizę tych 31 spraw przedstawiono w pkt 2.3.7.

Analiza według instytucji/organu

Większość instytucji i organów powiadamiała o operacjach przetwarzania mogących stwarzać szczególne zagrożenie. Monitoring powiadomień złożonych przez DPO jest ważnym działaniem w zakresie wydawania opinii dotyczących kontroli wstępnej realizowanym w 2007 r. Komisja Europejska dokonała pod tym względem istotnego postępu, chociaż wciąż oczekuje się wpłynięcia znacznej liczby powiadomień. Parlament Europejski, OLAF i Europejski Rzecznik Praw Obywatelskich również złożyły dużą liczbę powiadomień. Jeżeli chodzi o agencje UE – OHIM bardzo aktywnie powiadamiał o operacjach przetwarzania. Inne agencje zaczęły już powiadamiać o operacjach przetwarzania danych. Związane z tym opinie zostaną wydane w 2008 r. (zob. poniżej ppkt – Powiadomienia dotyczące przeprowadzenia kontroli wstępnych otrzymane przed 1 stycznia 2008 r. i będące w toku).

Analiza według kategorii

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

Kategoria pierwsza (dokumentacja medyczna)	166 spraw
Kategoria druga (ocena personelu)	41 spraw
Kategoria trzecia (podejrzenie popełnienia przestępstwa)	14 spraw
Kategoria czwarta (usługi socjalne)	8 spraw
Kategoria piąta (e-monitoring)	4 sprawy
Inne obszary	7 spraw

Kategoria pierwsza obejmuje dokumentację medyczną jako taką oraz jej różnoraką zawartość (pięć spraw), zwolnienia lekarskie (trzy sprawy), procedurę orzekania o inwalidztwie (jedna sprawa), żłobki dzienne (jedna sprawa), systemy ubezpieczeń zdrowotnych (jedna sprawa), dozymetrię promieniowania (jedna sprawa) oraz cztery sprawy związane z danymi dotyczącymi zdrowia. Odsetek spraw w tej kategorii zmniejszył się (26,5% spraw w 2005 r., 24,6% spraw w 2006 r. i 17,77% spraw w 2007 r.), dzięki nim EIOD miał jednak okazję, żeby udzielić porad dotyczących zawartości dokumentacji medycznej. W 2007 r. EIOD przeanalizował sprawę związaną z dozymetrią promieniowania we Wspólnym Centrum Badawczym; kilka następnych spraw również zostanie poddanych analizie.

Kategoria druga, dotycząca oceny personelu (41 spraw z 90), pozostaje najliczniejsza; udział procentowy tych spraw jest stosunkowo stabilny (56% spraw w 2005 r., 40,4% w 2006 r. i 45,55% w 2007 r.). Dziesięć spraw było związanych z rekrutacją (stażystów, oddelegowanych ekspertów krajowych, wyższych urzędników, rekrutacją do Europejskiego Banku Centralnego – EBC oraz do Wspólnotowego Urzędu Ochrony Odmian Roślin – CPVO), pięć spraw było związanych z oceną pracowników, trzy z awansem, dwie z niekompetencją personelu (obie to właściwe sprawy dotyczące kontroli wstępnej), osiem dotyczyło procedur certyfikacji i atestacji, cztery dotyczyły systemu *flexitime* (wszystkie to właściwe sprawy dotyczące kontroli wstępnej), dwie dotyczyły wcześniejszej emerytury, a siedem to inne kwestie.

Jeżeli chodzi o **kategorię trzecią** (dotyczącą przestępstw i podejrzenia o popełnienie przestępstwa),

odnotowano znaczny wzrost liczby spraw (14 opinii, co stanowi 15,55% ogólnej liczby spraw), należy jednak podkreślić, że kategoria ta obejmuje prawie wszystkie sprawy zgłoszone przez OLAF (zob. pkt 2.3.4). W kwestii postępowania dyscyplinarnego wydano tylko dwie opinie, jako że większość instytucji już w poprzednich latach przesłała powiadomienia dotyczące tych spraw.

W wypadku **kategorii czwartej** (usługi socjalne), liczba powiadomień czterokrotnie wzrosła (osiem opinii, co stanowi 8,88% ogólnej liczby opinii). Wszystkie najważniejsze instytucje, a także OHIM, dopełniły obowiązku dotyczącego powiadomień w tym zakresie. Wydaje się, że większość agencji nie jest w stanie zapewnić swoim pracownikom tego rodzaju usług.

Jeżeli chodzi o **kategorię piątą** (e-monitoring), wydano jedynie cztery opinie, ponieważ EIOD uznał, że większość powiadomień odnoszących się do e-monitoringu dotyczy spraw niepodlegających kontroli wstępnej – sprawy te nie wiążą się bowiem z konkretnymi zagrożeniami (naruszeniem tajemnicy, o czym mówi art. 27 ust. 1 rozporządzenia, lub podejrzeniem o popełnienie przestępstwa, o czym mowa w art. 27 ust. 2 lit. a), lub oceną aspektów osobistych, o czym mówi art. 27 ust. 2 lit. b)). Analiza tych spraw dokonana przez EIOD zaowocowała jednak wydaniem licznych zaleceń (zob. pkt 2.3.7).

Jeżeli chodzi o powiadomienia, których nie obejmują przedstawione kategorie, EIOD nadal analizował kwestie finansowe, takie jak PIF (zespół ds. nieprawidłowości finansowych – Parlament i Trybunał Sprawiedliwości), system wczesnego ostrzegania (Parlament i OLAF) oraz zaproszenie do składania ofert (Rada). EIOD zajmował się ponadto kwestią uczestnictwa w strajku (Rada) i zasadami dotyczącymi postępowania sprawdzającego (EBC).

Harmonogram działalności EIOD oraz instytucji i organów

Trzy wykresy znajdujące się w załączniku E obrazują harmonogram działalności EIOD oraz instytucji i organów Wspólnoty. Szczegółowo przedstawiają one liczbę dni, których EIOD potrzebował, aby sporządzić opinie, liczbę dni dodatkowych wymaganych przez EIOD oraz liczbę dni zawieszenia biegu terminu (czas niezbędny do otrzymania informacji od instytucji i organów).

Liczba dni, których EIOD potrzebował, aby sporządzić opinie: liczba ta zmniejszyła się o 1,73%, czyli o jeden dzień w stosunku do 2006 r. (55,5 dnia w 2005 r., 57,9 w 2006 r. i 56,9 w 2007 r.). Jest to liczba nader zadowalająca, zważywszy na coraz większą liczbę powiadomień przesyłanych EIOD i ich coraz bardziej złożony charakter.

Liczba dni dodatkowych dla EIOD: liczba ta zmniejszyła się o 15,74%, tzn. prawie o jeden dzień w stosunku do 2006 r. (3,3 dnia w 2005 r., 5,4 dnia w 2006 r. i 4,55 dnia w 2007 r.). Chociaż maksymalne przedłużenie może sięgnąć dwóch miesięcy (art. 27 ust. 4 rozporządzenia) – zazwyczaj nie przekraczało miesiąca.

Liczba dni zawieszenia biegu terminu: od połowy 2006 r. obejmuje ona zawieszenie na 7 lub 10 dni przeznaczone na uwagi i dalsze informacje od DPO na temat końcowego projektu. W wypadku spraw dotyczących kontroli *ex post* zgłoszonych przed 1 września 2007 r. z obliczeń nie wyłączono sierpnia. Wzrost między 2005 r. (średnio 29,8 dni na dossier) a 2006 r. (średnio 72,8 dni na dossier) wynosi 3,21 %. Biorąc pod uwagę fakt, że w 2005 r. termin ten wynosił średnio 29,8 dni na dossier, EIOD jest zaniepokojony długimi terminami, jakich potrzebowały instytucje czy organy na uzupełnienie informacji, zwłaszcza w trzech przypadkach (odpowiednio 185, 200 i 203 dni). 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 pokazują, że w 2007 r. niektóre instytucje i organy bardzo znacznie zwiększyły liczbę dni zawieszenia biegu terminu (np. Parlament Europejski, KR, ETO, CdT, niektóre zwiększyły tę liczbę w mniejszym stopniu, np. EBC i Komisja), podczas gdy innym udało się tę liczbę zmniejszyć (np. OHIM, EBI, Trybunał Sprawiedliwości, Rada).

Powiadomienia dotyczące przeprowadzenia kontroli wstępnej otrzymane przed 1 stycznia 2008 r. i będące w toku

Do końca 2007 r. w trakcie analizy znajdowało się **69 spraw dotyczących kontroli wstępnej**. Z tej liczby 4 powiadomienia przesłano w 2006 r., a 65 powiadomień w 2007 r. Z tych 69 spraw będących w toku – do końca lutego 2008 r. sfinalizowano 25 spraw i wydano dotyczące ich opinie.

OLAF	4 sprawy
Parlament	4 sprawy
Rada	9 spraw
Komisja Europejska	23 sprawy
Europejski Bank Centralny	1 sprawa
EKES i KR	3 sprawy
Europejski Bank Inwestycyjny	3 sprawy
Trybunał Obrachunkowy	2 sprawy
Europejski Trybunał Sprawiedliwości	2 sprawy
Europejski Rzecznik Praw Obywatelskich	1 sprawa
Europejskie Centrum Rozwoju Kształcenia Zawodowego (CEDEFOP)	1 sprawa
CPVO	2 sprawy
EFSA	1 sprawa
EMCDDA	1 sprawa
EMEA	7 spraw
EMSA	2 sprawy
EPSO	1 sprawa
OHIM	1 sprawa
CdT	1 sprawa

Analiza według instytucji i organu

Jak zauważono wcześniej w związku z terminem „wiosna 2007", więcej agencji rozpoczęło proces powiadamiania (CEDEFOP, EMCDDA, EMEA – która przesłała siedem powiadomień – i EMSA) lub kontynuowało ten proces (CdT, EFSA i CPVO). EIOD zachęca pozostałe agencje i organy do podobnego działania.

Istotne są również liczby odnoszące się do Rady i Komisji. Jeżeli chodzi o Komisję, 16 z 27 powiadomień nadeszło z różnych ośrodków Wspólnego Centrum Badawczego (WCB) i dotyczy głównie dwóch kwestii – dozymetrii promieniowania i kontroli dostępu – ze względu na bardzo szczególny charakter WCB (jest to jedna z dyrekcji DG ds. Badań Naukowych o dużym zakresie autonomii).

Analiza według kategorii

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

Kategoria pierwsza (dokumentacja medyczna)	20 spraw
Kategoria druga (ocena personelu)	25 spraw
Kategoria trzecia (podejrzenie popełnienia przestępstwa)	4 sprawy
Kategoria czwarta (usługi socjalne)	–
Kategoria piąta (e-monitoring)	3 sprawy
Inne obszary	17 spraw

W **kategorii pierwszej** przesyłanie powiadomień ma charakter ciągły, co prowadzi do następujących wniosków:

- kategoria ta obejmuje 28,98% spraw będących w toku na początku 2008 r.;
- jedna sprawa dotycząca dokumentacji medycznej Komisji odgrywa międzyinstytucjonalną rolę w szczególnych aspektach (np. archiwizacji dokumentacji medycznej);
- spośród 20 spraw dotyczących kontroli wstępnej osiem nadeszło z różnych ośrodków WCB; odnoszą się one także do różnych dziedzin, takich jak indywidualna dokumentacja medyczna (dla wszystkich ośrodków WCB), pierwsza pomoc i wypadki, zwolnienia lekarskie, procedura orzekania o inwalidztwie oraz trzy sprawy związane z dozymetrią promieniowania;
- EIOD z zadowoleniem przyjmuje fakt, że CPVO i EMEA również przesyłają powiadomienia w tej dziedzinie;
- EIOD nadal czeka na powiadomienie, które ma przesłać Urząd Administrowania i Wypłacania Należności Indywidualnych (PMO), zgodnie z uwagą zawartą w poprzednim sprawozdaniu rocznym.

Kategoria druga, tematyczna (ocena personelu), nadal obejmuje większość przypadków – dokładnie jedną trzecią. Osiem z tych spraw wiąże się z procedurami naboru (wykorzystywanie przez instytucje list rezerwowych EPSO) oraz z procedurami rekrutacji stosowanymi przez agencje. Wszystkie procedury, które mają zostać ocenione, są stosowane przez agencje (EMCCDA, CPVO, EMEA, EMSA i EFSA). Dwa inne powiadomienia są związane z systemem *flexitime* (zob. pkt 2.3.5). W 2008 r. EIOD będzie miał także po raz pierwszy sposobność do przeanalizowania powiadomienia w dziedzinie polityki szkoleń (Rada 2007-584).

Jeżeli chodzi o **kategorię trzecią** (przestępstwa i podejrzenia o popełnienie przestępstwa), EIOD zajmuje się sprawami zgłoszonymi przez OLAF oraz procedurami dyscyplinarnymi i dochodzeniami administracyjnymi stosowanymi przez CEDEFOP. EIOD zachęca pozostałe agencje do przesyłania powiadomień dotyczących ich spraw.

W wypadku **kategorii czwartej** (usługi socjalne) EIOD nie wyraża zdziwienia z powodu braku rozpatrywanych powiadomień, ponieważ agencje wyjaśniły w kontekście terminu „wiosna 2007 i później" (zob. pkt 2.6), że często nie są w stanie zapewnić swoim pracownikom tego rodzaju usług.

Kategoria piąta (e-monitoring) nadal ma szczególne znaczenie. W 2007 r. EIOD zorganizował szereg spotkań poświęconych e-monitoringowi oraz zorganizował interaktywne ćwiczenia dotyczące zwiększania świadomości w tej dziedzinie. Podsumowanie wyników tych ćwiczeń znajdzie się we wnioskach, które zostaną opublikowane w 2008 r.

Inne obszary (24,63% spraw) obejmują trzy główne dziedziny: zaproszenia do składania ofert, systemy nadzoru wideo i systemy kontroli dostępu do danych. Dwie ostatnie dziedziny mają szczególne znaczenie: w 2008 r. ukaże się dokument dotyczący nadzoru wideo (zob. pkt 2.9); kontrola dostępu jest z kolei bardzo delikatną kwestią, z którą czasami wiąże się technologia identyfikacji radiowej (RFID) lub technologie biometryczne. EIOD będzie mieć ponadto po raz pierwszy okazję do wydania opinii na temat osób zajmujących eksponowane stanowiska polityczne w EBI, co również jest bardzo delikatnym zagadnieniem.

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 również podlegają kontroli wstępnej. W tej kategorii EIOD zbadał również takie kwestie, jak procedura orzekania o inwalidztwie, dozymetria promieniowania i żłobki.

Te zróżnicowane sprawy dotyczące kontroli wstępnej dały EIOD okazję, żeby dogłębnie przeanalizować kwestie związane z przetwarzaniem danych medycznych przez instytucje i agencje Wspólnoty. EIOD zakwestionował istotność niektórych spraw podnoszonych podczas wizyt lekarskich poprzedzających zatrudnienie oraz rocznych wizyt lekarskich w kontekście celu takich wizyt. Po przeanalizowaniu funkcji prewencyjnej badania lekarskiego poprzedzającego zatrudnienie EIOD zaleca, aby badanie takie nie służyło zasadniczo do żadnych celów prewencyjnych bez zgody podmiotu danych. EIOD zalecił także usunięcie z kwestionariuszy medycznych pytań dotyczących członków rodziny, którzy nie mają żadnych powiązań genetycznych z osobą zainteresowaną.

EIOD jest zdania, że roczne badania medyczne można uważać za zapobiegawcze wyłącznie za zgodą osoby zainteresowanej. Roczne badania medyczne generalnie nie mogą służyć potwierdzeniu zdolności do pracy, dopuszcza się jednak przeprowadzanie konkretnych badań i certyfikacji w ograniczonej liczbie ściśle określonych przypadków, na przykład jeżeli pracownik miał kontakt z substancją niebezpieczną.

Okresy przechowywania danych medycznych były również przedmiotem zaleceń zawartych w opiniach EIOD dotyczących kontroli wstępnych w związku z opinią EIOD przedstawioną kolegium szefów administracji (2006-532) ([8]). W szczególności dane medyczne dotyczące niezatrudnionych kandydatów zgromadzone podczas wizyt lekarskich poprzedzających zatrudnienie powinny być przechowywane jedynie przez określony czas.

Na kwestię jakości danych zawartych w dokumentacji medycznej zwrócono także uwagę w kontekście różnych spraw dotyczących kontroli wstępnej. Zdaniem EIOD, chociaż trudno mówić o dokładności danych medycznych, na mocy zasady jakości danych, podmiot danych może wnioskować o dodanie do akt opinii innego lekarza lub wszelkich innych stosownych informacji, aby zapewnić aktualizację danych.

W kontekście opinii na temat sprawy dotyczącej kontroli wstępnej związanej ze zwrotem wydatków medycznych (Komisja 2004-238) podniesiono szczegółową kwestię przekazywania danych osobowych. Jeżeli chodzi o procedury odwoławcze przewidziane

([8]) Zob. sprawozdanie roczne EIOD za 2006 rok, s. 35. Zob. także wspólny wykaz przechowywanych dossier w pkt 2.7 poniżej.

w art. 90 ust. 2 regulaminu pracowniczego urzędników Wspólnot Europejskich EIOD zalecił usunięcie – w procesie przekazywania danych komitetowi zarządzającemu – informacji umożliwiających identyfikację osoby, ponieważ nie są one potrzebne komitetowi do sporządzania sprawozdań.

Nabór to – z oczywistych powodów – często wykonywana we wszystkich instytucjach i organach operacja przetwarzania. W 2006 r. przeanalizowano procedurę naboru międzyinstytucjonalnego stosowaną przez EPSO, w rezultacie czego EIOD wydał stosowną opinię (2004-0236). W 2007 r. Parlament i EBC przesłały powiadomienia dotyczące przeprowadzenia kontroli wstępnej w kwestii wykorzystywania list rezerwowych EPSO. OLAF także przesłał powiadomienie w sprawie swojej procedury naboru pracowników czasowych z konkretnych list rezerwowych. Zgłoszono wątpliwości co do zasady proporcjonalności w polityce OLAF w zakresie postępowania sprawdzającego dotyczącego pracowników, którzy nie muszą mieć dostępu do bardzo poufnych informacji na podstawie obowiązującego prawodawstwa wspólnotowego.

EIOD przeprowadził także kontrolę wstępną komisyjnej procedury naboru wyższych urzędników (2007-0193). W swojej opinii EIOD przypomina, że kandydaci powinni mieć możliwość dostępu do swoich pełnych akt obejmujących siatki ocen i oceny, które ich dotyczą, sporządzone przez różne komitety właściwe do dokonywania oceny tych kandydatów. EIOD jest świadomy, że reguła ta ma pewne ograniczenia; chodzi tutaj o zasadę tajności prac komisji konkursowych zgodnie z art. 6 załącznika III regulaminu pracowniczego. Zgodnie z art. 20 ust. 1 lit c) rozporządzenia nie należy podawać żadnych ocen wystawionych przez poszczególnych członków komisji ani informacji porównujących podmiot danych z innymi kandydatami.

Ocena personelu: Sprawa awansów zawodowych w systemie Sysper 2 w Komisji dała okazję, żeby wydać zalecenia dotyczące zatrzymywania danych oraz żeby zwrócić się do Komisji o ocenę potrzeby wprowadzania do systemu informacji o toczącym się postępowaniu dyscyplinarnym jako przyczynie zawieszenia awansu ([9]).

([9]) W związku ze skargą (sprawa 2007-529, zob. poniżej) EIOD mógł ponadto wydać inne zalecenie dotyczące rzetelności przetwarzania, prosząc o bardziej szczegółową procedurę w odniesieniu do „punktów priorytetowych".

W dokumentach medycznych zawsze znajdują się dane szczególnie chronione

Różne instytucje i agencje nadal przesyłały do EIOD sprawy dotyczące procedury certyfikacji i procedury akredytacji. Zalecenia wydane przez EIOD odnoszą się w szczególności do okresów przechowywania danych z uwzględnieniem środków odwoławczych oraz nowych wniosków składanych przez tę samą osobę.

Dwie opinie odnoszące się do spraw dotyczących kontroli wstępnej są związane z procedurą wcześniejszego przejścia na emeryturę stosowaną przez Komisję (2006-577) i przez OHIM (2007-575). W innych obszarach zalecenia dotyczą okresu przechowywania danych oraz prawa dostępu podmiotu danych do sprawozdania komisji odpowiedzialnej za stwierdzenie, które osoby są uprawnione do przejścia na wcześniejszą emeryturę, z zastrzeżeniem pewnych ograniczeń zgodnie z art. 20 ust. 1 lit. c) rozporządzenia. EIOD wyraził również zastrzeżenia co do konieczności publikacji wykazu osób, które wystąpiły z wnioskiem o wcześniejszą emeryturę.

W różnych obszarach oceny pracowników wydano także kilka opinii dotyczących badania stresu w pracy w OHIM, specjalnych doradców, specjalnych odszko-

dowań, wykazu w zakresie obserwacji wyborów oraz przeniesień pracowników.

Procedury stosowane przez OLAF: EIOD wydał 12 opinii dotyczących procedur stosowanych przez OLAF (jedna z nich jest rzeczywistą sprawą dotyczącą kontroli wstępnej – system powiadamiania o nadużyciach, zob. pkt 2.3.5 poniżej). Jedna opinia (wspólne sprawy 2006-544, 2006-545, 2006-546, 2006-547) dotyczyła następczych działań natury sądowej, dyscyplinarnej, administracyjnej i finansowej. Cztery operacje przetwarzania danych odnoszą się do przetwarzania danych osobowych, odbywającego się w ramach trzeciego etapu dochodzeń prowadzonych przez OLAF, tzw. fazy monitorowania, w którym dopilnowuje się, aby właściwe organy Wspólnoty lub organy krajowe stosowały się do zaleceń OLAF. Ogólnie procedury są zgodne z zasadami określonymi w rozporządzeniu o ochronie danych. EIOD wydał jednak kilka zaleceń dotyczących przede wszystkim konieczności wprowadzenia do systemu pewnych danych, obowiązku ustalenia konieczności przekazywania danych oraz informacji udzielanych podmiotom danych. EIOD zalecił także, aby OLAF, po zakończeniu dziesięciu lat swojej działalności, dokonał oceny dwudziestoletniego okresu przechowywania danych. EIOD podkreślił, że jego zdaniem zalecenia te należy uwzględnić podczas aktualizowania podręcznika rozpatrywania spraw przez OLAF.

Inna opinia dotyczyła wszystkich dochodzeń i operacji zewnętrznych (2007-047, 048, 049, 050 i 072). Dochodzenia zewnętrzne są dochodzeniami administracyjnymi prowadzonymi poza organami Wspólnoty; mają one wykrywać nadużycia lub inne przypadki nieprawidłowego postępowania osób fizycznych lub prawnych mające wpływ na finansowe interesy Wspólnot Europejskich. Wyniki dochodzeń zewnętrznych OLAF-u są przekazywane właściwym organom krajowym lub wspólnotowym, aby umożliwić prowadzenie działań o charakterze sądowym, administracyjnym, prawodawczym lub finansowym wynikających z tych ustaleń. EIOD zwrócił się do OLAF o dołączenie do dossier adnotacji, na podstawie której w danym wypadku byłoby wymagane przekazanie danych osobowych, oraz o zapewnienie (w ramach ogólnej zasady) danej osobie prawa dostępu do własnych danych osobowych i prawa do ich poprawiania. W tym kontekście OLAF musi zadbać o to, aby wszelkie ograniczenia, o których mowa w art. 20 rozporządzenia, dotyczące prawa dostępu podmiotu danych do własnych danych osobowych lub prawa do ich poprawiania spełniały warunek niezbędności odnoszący się do poszczególnych przypadków, a także aby art. 20 ust. 3, 4 i 5 rozporządzenia były należycie uwzględniane. OLAF musi ponadto przestrzegać zasady poufności tożsamości demaskatorów i informatorów podczas prowadzonych przez ten organ dochodzeń zewnętrznych.

EIOD przeprowadził również kontrolę wstępną czynności związanych z przetwarzaniem prowadzonych przez Komitet Nadzoru (2007-0073). Celem takiego przetwarzania jest wzmocnienie niezależności OLAF przez regularne monitorowanie prowadzonych działań dochodzeniowych, zgodnie z art. 11 rozporządzenia 1073/99. EIOD zalecił między innymi, aby Komitet Nadzoru miał dostęp do akt systemu zarządzania sprawami (CMS – *case management system*) (bieżącymi, zamkniętymi i niebędącymi przedmiotem zainteresowania OLAF) wyłącznie w poszczególnych przypadkach. Kiedy Komitet Nadzoru występuje z wnioskiem o taki dostęp, do akt systemu zarządzania sprawami należy dołączyć informację określającą powody, które uzasadniłyby udzielenie takiego dostępu. Komitet Nadzoru musi ponadto przestrzegać zapisów art. 12 rozporządzenia dotyczącego zainteresowanych osób, w tym demaskatorów, świadków i informatorów.

Reasumując, EIOD przeprowadził dogłębną analizę czynności OLAF związanych z przetwarzaniem w dziedzinie danych związanych z podejrzeniem popełnienia przestępstwa i w stosowanych przypadkach wydał zalecenia. Odnotowano następujące dalsze przykłady:

- system powiadamiania o nadużyciach (2007-481);
- pule informacji i danych wywiadowczych oraz bazy danych wywiadowczych (wspólne sprawy 2007-027 i 2007-028);
- sprawy związane z pomocą w postępowaniach karnych (2007-203);
- system informacji celnej (2007-177);
- system informacji służący zwalczaniu nadużyć finansowych (AFIS – *anti-fraud information system*) (wspólne sprawy 2007-084, 2007-085, 2007-086, 2007-087);
- usługi związane z bezpłatnym telefonowaniem (2007-003).

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.

EIOD wydał szereg opinii dotyczących kontroli wstępnej w tej dziedzinie. EIOD zalecił w szczególności, aby pracownik socjalny, który przetwarza dane osobowe, był właściwie poinformowany o wymogu przestrzegania zasady określonej w art. 4 ust. 1 lit. c) rozporządzenia, mianowicie, że dane osobowe muszą być „prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone lub dalej przetworzone". Zasady tej należy przestrzegać w stosunku do danych dostarczonych przez wnioskodawcę oraz w stosunku do osobistych notatek pracownika socjalnego.

Powtarzające się zalecenie w opiniach dotyczących kontroli wstępnej odnoszącej się do usług socjalnych mówiło o najwyższej ostrożności niezbędnej we wszystkich kontaktach pracownika socjalnego ze służbami zewnętrznymi ze względu na naturę przekazywanych danych. EIOD stwierdził także, że prawo do poprawy danych w ramach akt socjalnych będących w posiadaniu pracownika socjalnego oznacza w szczególności, że podmiot danych ma prawo do wyrażenia swojego stanowiska, zwłaszcza jeżeli subiektywna ocena dokonana przez pracownika socjalnego mogłaby mieć pewien wpływ na korzystanie przez zainteresowaną osobę z jej praw.

E-monitoring: Choć EIOD nie zajął jeszcze ostatecznego stanowiska w sprawie e-monitoringu (zob. pkt 2.8 poniżej), w tej dziedzinie przyjęto kilka opinii. Wydano dwie opinie dotyczące procedury dochodzenia prowadzonego przez EBC w sprawie korzystania z telefonów biurowych i służbowych telefonów komórkowych (2004-271 i 2004-272). Obie opinie zawierały zalecenie dotyczące okresu przechowywania danych o połączeniach, który zasadniczo nie powinien być dłuższy niż sześć miesięcy, z zastrzeżeniem pewnych konkretnych wyłączeń. Dane o połączeniach można przetwarzać do celów statystycznych, w takich przypadkach muszą one jednak być anonimowe.

EIOD wydał także opinię dotyczącą dyskretnego monitorowania w sposób wybiórczy (dwa lub trzy razy w roku) połączeń służbowych z centralą telefoniczną OHIM i jego centrum informacji (2007-128), w szczególności aby ocenić jakość świadczonych usług, zwiększyć zadowolenie klientów, a także aby przeszkolić nowych pracowników. Zdaniem EIOD takiego przetwarzania można było dokonać na podstawie art. 5 lit. a) rozporządzenia, ponieważ zasadniczo przetwarzanie to można było uznać za konieczne do osiągnięcia opisanych celów, z zastrzeżeniem pewnych kwestii szczegółowych związanych ze szkoleniem. EIOD podkreślił również, że należy udoskonalić metodę gwarantowania dokładności danych.

Stwierdzono, że wiele spraw przekazanych do EIOD odnoszących się do e-monitoringu nie kwalifikowało się do kontroli wstępnej, gdyż dane przetwarzano jedynie w celu zarządzania danymi billingowymi i danymi o połączeniach; nie były one więc związane z konkretnymi zagrożeniami ani podejrzeniami o popełnienie przestępstwa ani oceną (zob. pkt 2.3.7).

(Zagadnienia związane z nadzorem wideo poruszono w pkt 2.9).

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 2007 r. EIOD otrzymał powiadomienia o 11 sprawach dotyczących „właściwej" ([10]) kontroli wstępnej. Spośród tych 11 spraw dwie dotyczyły nienależytego wykonywania obowiązków przez pracowników, a cztery systemu *flexitime*.

Trybunał Obrachunkowy wprowadził procedurę, na podstawie której podejmowano by działania w razie zaobserwowania oznak nienależytego wykonywania obowiązków przez pracowników oraz działania służące rozwiązaniu tego problemu (sprawa 2006-534). Analiza przeprowadzona przez EIOD zaowocowała przede wszystkim wydaniem zaleceń dotyczących informacji, które należy przekazać pracownikom, zawierającym odniesienie do konkretnej decyzji oraz do decyzji wykonawczej Trybunału dotyczącej ochrony danych, a także do ustalenia okresu zatrzymywania danych. Zalecenia związane ze sprawą Parlamentu Europejskiego (sprawa 2006-572) dotyczyły kilku kwestii, między innymi przechowywania danych związanych z zakończonymi lub przerwanymi procedurami naprawczymi lub przetwarzania w tym kontekście danych dotyczących zdrowia.

([10]) Tzn. spraw dotyczących jeszcze nierozpoczętej operacji przetwarzania.

Systemy administrowania czasem pracy dają dostęp do danych na temat ludzkich działań i innych kwestii prywatnych

W 2007 r. duże znaczenie miały **systemy zarządzania czasem**. EIOD otrzymał ogólne powiadomienie od Komisji (sprawa 2007-063) dotyczące zarządzania czasem, modułu Sysper 2 (systemu zarządzania personelem), do którego włączono funkcję *flexitime,* a także dwie szczegółowe sprawy dotyczące systemu *flexitime* przesłane przez dwie dyrekcje generalne (sprawa 2007-218 dla Dyrekcji Generalnej ds. Społeczeństwa Informacyjnego i Mediów (DG INFSO) oraz sprawa 2007-680 dla Dyrekcji Generalnej ds. Rolnictwa i Rozwoju Obszarów Wiejskich (DG AGRI)); te dwie sprawy stanowiły modyfikacje sprawy będącej przedmiotem głównego powiadomienia. Kwalifikowały się one do przeprowadzenia kontroli wstępnej na podstawie art. 27 ust. 2 lit. a) (dane odnoszące się do zdrowia) oraz art. 27 ust. 2 lit. b) (operacje przetwarzania zmierzające do oceny wydajności pracowników, ich kompetencji i możliwości pracy).

Komisyjny system zarządzania czasem był właściwą sprawą dotyczącą kontroli wstępnej tylko w części dotyczącej ***flexitime***; w wyniku jego analizy wydano zalecenia związane ze stosowaniem osobistego numeru identyfikacyjnego pracowników, aby zagwarantować spójność w systemie, z informacją o obowiązkowym lub dobrowolnym charakterze danych zebranych od pracowników oraz z rozróżnieniem w ramach całkowitej liczby nadgodzin.

DG INFSO dodała do wniosku dotyczącego *flexitime* dodatkowy, ważny element w formie mikroprocesora RFID stanowiącego część osobistego identyfikatora niezbędnego do wprowadzania danych o wejściu i wyjściu pracownika. Włączenie do systemu *flexitime* takiej technologii powoduje wzrost konkretnych zagrożeń już występujących w systemie. We wnioskach EIOD zalecił wprowadzenie do planowanego systemu kilku modyfikacji w zakresie bezpieczeństwa przez wprowadzenie rozwiązania przejściowego, a także w zakresie sformułowania oświadczenia o ochronie danych osobowych, pewnych środków organizacyjnych oraz w odniesieniu do zainteresowanych podmiotów danych.

Jeżeli chodzi o szczegóły systemu *flexitime* w DG AGRI – EIOD stwierdził, że w sprawie będącej przedmiotem powiadomienia dochodzi do naruszenia zapisów rozporządzenia (WE) nr 45/2001, ponieważ oczekiwany cel (polegający na umożliwieniu kilku osobom w dziale – wielu więcej niż tylko kierownik działu – określania nieobecności pracownika, aby jak najszybciej znaleźć dla niego zastępstwo) można osiągnąć za pomocą innych, mniej ingerencyjnych środków. Ponadto celu przedstawionego przez DG AGRI nie można osiągnąć za pomocą proponowanego systemu *flexitime*.

Czwartą sprawę związaną z zarządzaniem czasem przesłał EFK (sprawa 2007-209). Baza danych rejestrująca czas ma dostarczać dyrekcji EFK informacji o czasie, jaki poszczególne osoby i zespoły poświęciły na realizację różnych zadań i projektów. Główne zalecenia dotyczyły jakości danych (trudno było zapewnić ich wysoką jakość ze względu na sposób, w jaki utworzono system) oraz ograniczenia celu – informacje należało wykorzystywać jedynie do zarządzania projektem, a nie do dokonywania indywidualnych ocen.

Kolejną opinię dotyczącą właściwej kontroli wstępnej wydano w sprawie kwestii związanej z zarządzaniem czasem – była to sprawa EBI odnosząca się do rejestrów medycznych i zarządzania czasem (sprawa 2007-373). Pierwotnie sprawę tę przesłano z prośbą o konsultację

dotyczącą potrzeby przeprowadzenia kontroli wstępnej, ponieważ wcześniej wydano dwie opinie (2005-396 „Rejestry medyczne" i 2004-306 „Zarządzanie czasem"), a zamiarem EBI było udostępnienie wszystkich danych związanych z nieobecnością z powodu choroby niepotwierdzonej zwolnieniem lekarskim, przechowywanych przez lekarza Centrum Zdrowia Pracy (OHC) za pomocą narzędzia służącego do zarządzania czasem. Po raz pierwszy EIOD miał wydać nową opinię, opierając się na zmianach dokonanych w kwestii będącej przedmiotem wcześniejszej kontroli wstępnej.

W opinii EIOD stwierdził, że EBI naruszałby pewne zapisy rozporządzenia (zgodność przetwarzania z prawem, zasadę jakości danych, przetwarzanie szczególnych kategorii danych), jeżeli nie zadbałby o to, aby od pracowników wymagano dobrowolnego i jednoznacznego wyrażenia zgody na dostęp lekarzy OHC do danych dotyczących ich nieobecności z powodu choroby niepotwierdzonej zwolnieniem lekarskim. Gdy pracownika prosi się o wyrażenie takiej zgody, należy zadbać o to, aby był on w pełni świadomy tego, że zgodę taką może w każdej chwili wstrzymać lub następnie wycofać bez uzasadniania takiej decyzji i bez żadnych konsekwencji. Należy również wyjaśnić, że informacje te podawane są jedynie w celach zapobiegawczych.

Spośród pozostałych właściwych spraw dotyczących kontroli wstępnej EIOD zwraca uwagę na następujące przypadki:

- sprawa EPSO (2007-088) dotycząca oceny możliwości pracy w trzecim języku, która zawiera zalecenie odnoszące się do dokonywania przez przetwarzających automatycznej korekty;
- sprawa Europejskiego Rzecznika Praw Obywatelskich (2007-134) dotycząca zarządzania urlopami; w tym wypadku wydano pewne zalecenia związane z danymi dotyczącymi zdrowia oraz informacji kierowanych do podmiotów danych;
- sprawa EBC (2007-371) odnosząca się do zasad dotyczących postępowania sprawdzającego (czynności związanych z przetwarzaniem danych, które EBC prowadzi w kontekście realizacji procedur postępowania sprawdzającego, aby stwierdzić, czy dana osoba spełnia warunki wydania jej poświadczenia bezpieczeństwa osobowego, czy nie), w którym należy unikać zbyt dużej ilości danych;
- sprawa OLAF (2007-481) związana z systemem powiadamiania o nadużyciach (system internetowy, który OLAF udostępnił społeczeństwu, aby łatwiej gromadzić informacje wykorzystywane w walce z nadużyciami, korupcją i innymi nielegalnymi działaniami mającymi wpływ na finansowe interesy Wspólnoty) obejmująca dwie istotne kwestie: informowanie zainteresowanych osób o otrzymywanych informacjach oraz ochrona informatorów i demaskatorów.

2.3.6. Konsultacje dotyczące potrzeby przeprowadzenia kontroli wstępnej

W 2007 r. liczba konsultacji dotyczących potrzeby przeprowadzenia kontroli wstępnej przez EIOD była w dalszym ciągu znaczna. 20 konsultacji w 2007 r. w porównaniu z 15 w 2006 r. Kilka przypadków, o których mowa powyżej, było wcześniej przedmiotem konsultacji: „Rejestry medyczne i zarządzanie czasem", „System *flexitime* – DG INFSO", „Dane przetwarzane przez doradcę społecznego", „Przeniesienia pracowników" itp.

Inne sprawy, które, jak stwierdzono, podlegają kontroli wstępnej, takie jak „Nagroda roczna", „Dochodzenia w zakresie bezpieczeństwa", „Konsultanci niezależni", „Wykorzystywanie list rezerwowych EPSO" oraz „Baza zawierająca dane dotyczące ekspertów EFSA", nie stały się jeszcze formalnie przedmiotem powiadomienia EIOD po przekazaniu przez tę instytucję informacji zwrotnych na temat potrzeby przeprowadzenia kontroli wstępnej.

Uznano, że operacja przetwarzania danych dotyczących „osób zajmujących eksponowane stanowiska polityczne w EBI" podlega kontroli wstępnej, ponieważ obejmuje dane związane z wyrokami skazującymi za przestępstwa lub podejrzeniami o popełnienie przestępstwa.

Sprawa związana z „Zasadami regulującymi wchodzenie dzieci pracowników do budynków OHIM" miała charakter szczególny w tym sensie, że choć początkowo twierdzono, że podlega ona przeprowadzeniu kontroli wstępnej, to później sprawę wycofano. Agencja rzeczywiście zmieniła te zasady w taki sposób, że już nie wiążą się one z przetwarzaniem danych osobowych.

Stwierdzono, że operacja przetwarzania związana z zarządzaniem dostępem do Internetu w Trybunale Sprawiedliwości nie podlega kontroli wstępnej.

Rzeczywiście jej celem nie było ocenianie postępowania, nie doszło tam również do naruszenia poufności komunikacji.

Z tego samego powodu nie uznano, że „telefoniczna" operacja przetwarzania w Radzie podlega kontroli wstępnej, jako że nie wiązała się ona z naruszeniem poufności komunikacji.

Kolejną interesującą decyzją w tej dziedzinie jest sprawa ETS dotycząca systemu poczty elektronicznej. System ten nie podlega kontroli wstępnej, ponieważ nie zastosowano żadnego regularnego ani wyrywkowego monitoringu ukierunkowanego na wykrywanie nadużywania elektronicznego systemu przesyłania wiadomości. Nie istnieje żadna operacja przetwarzania zmierzająca do oceny aspektów osobistych, takich jak możliwości, wydajność lub postępowanie pracowników.

Chociaż operacja przetwarzania stosowana w Radzie dotycząca „przygotowania do podróży" mogłaby wiązać się z danymi dotyczącymi zdrowia, stwierdzono, że nie podlega ona kontroli wstępnej. Oczywiste jest, że celem przetwarzania nie jest przetwarzanie danych medycznych; dane takie mogą być przetwarzane tylko w pewnych odosobnionych wypadkach oraz za zgodą podmiotu danych.

2.3.7. Powiadomienia dotyczące spraw niepodlegających kontroli wstępnej

W 2007 r. EIOD zajmował się również 31 sprawami, które uznano za niepodlegające kontroli wstępnej (23,48% spraw sfinalizowanych przez EIOD). Decyzję tę podjęto po dokładnej analizie powiadomienia.

Niemniej jednak w wyniku tej analizy w większości wypadków EIOD wydał pewne zalecenia. Jedenaście z tych spraw dotyczy e-monitoringu, dwie systemu *flexitime*, cztery kontroli dostępu, a pozostałe kwestii pracowniczych (wstępne zaszeregowanie, dowód tożsamości, wniosek dotyczący działalności zewnętrznej, przedłużanie umów, zasada dotycząca bezprawnego wykorzystywania poufnych informacji) lub różnych innych dziedzin, takich jak akredytacja lub dochodzenia prowadzone przez DPO z OLAF.

Jeżeli chodzi o kategorię **e-monitoringu,** większość takich powiadomień ([11]) przesłano EIOD do kontroli wstępnej na podstawie art. 27 ust. 1 rozporządzenia.

Należy przypomnieć, że łączność elektroniczna może podlegać kontroli wstępnej EIOD w dwóch głównych wypadkach:

- Artykuł 27 ust. 1 rozporządzenia stanowi, że kontroli wstępnej podlegają wszelkie operacje przetwarzania, mogące przez swój zakres lub swoje cele stworzyć konkretne zagrożenia dla praw i wolności podmiotów danych. Rozdział IV rozporządzenia zawiera szczegółowy zapis dotyczący poufności komunikacji (art. 36). W razie naruszenia poufności komunikacji może zaistnieć konkretne zagrożenie dla praw i wolności podmiotów danych, a co za tym idzie, taka operacja przetwarzania podlega kontroli wstępnej EIOD;
- Artykuł 27 ust. 2 rozporządzenia zawiera wykaz operacji przetwarzania danych, które mogą stworzyć takie zagrożenia. Wykaz obejmuje między innymi:
  — przetwarzanie danych „dotyczących podejrzeń o popełnienie przestępstwa, przestępstw lub środków bezpieczeństwa" (art. 27 ust. 2 lit. a));
  — operacje przetwarzania zmierzające do oceny aspektów osobistych odnoszących się do podmiotu danych, włącznie z jego możliwościami, wydajnością lub postępowaniem.

Jeżeli funkcjonuje mechanizm monitorowania sieci łączności do celów art. 27 ust. 2 lit. a) lub art. 27 ust. 2 lit. b) rozporządzenia, takie operacje przetwarzania muszą podlegać kontroli wstępnej EIOD.

Oznacza to, że nie wszystkie systemy łączności elektronicznej muszą podlegać kontroli wstępnej. Jeżeli nie zostaje naruszona poufność komunikacji oraz jeżeli infrastruktura informatyczna nie jest wykorzystywana do monitorowania postępowania pracowników, często

([11]) Powiadomienia dotyczące systemu poczty elektronicznej lub telefonii (EKES i KR 2006-507 i 2006-508), telefonicznej i telefaksowej infrastruktury, sieci i systemu telefonicznego i telefaksowego, statystyk internetowych, baz zawierających dane o rozmowach telefonicznych, danych billingowych (Komisja, sprawy 2007-358, 2007-359, 2007-367 i 2007-374), telefonii stacjonarnej i komórkowej (Trybunał Sprawiedliwości, sprawy 2007-438 i 2007-439), rejestru rozmów telefonicznych (EBI, sprawa 2004-302) oraz fakturowania korzystania z usług GSM do celów prywatnych (OLAF, sprawa 2007-204).

nie ma powodu, aby dany systemy łączności elektronicznej poddawać kontroli wstępnej.

Niemniej jednak EIOD wydawał zalecenia dotyczące okresu zatrzymywania danych o połączeniach i danych billingowych zgodnie z art. 37 ust. 2 rozporządzenia, a także zalecenia odnoszące się do informacji, które mają być przekazane podmiotom danych.

Jeżeli chodzi o **kontrolę dostępu**, zgodnie z art. 27 ust. 2 lit. b) złożono trzy powiadomienia ([12]). Po przeprowadzeniu analizy EIOD stwierdził, że w żadnym z tych przypadków nie miała miejsca ocena. Wydano jednak zalecenia dotyczące dokładnego celu przetwarzania. Powiadomienie dotyczące czwartej sprawy ([13]) wpłynęło na podstawie art. 27 ust. 2 lit. a) i art. 27 ust. 2 lit. d), przepisy te nie miały jednak zastosowania w tym konkretnym przypadku. Artykuł 27 ust. 2 lit. a) miał zastosowanie w wyjątkowych okolicznościach, a wykaz wyłączeń, którego nie sporządził administrator danych, sprawił, że art. 27 ust. 2 lit. d) nie miał zastosowania.

Uznano, że dwie sprawy dotyczące **zarządzania czasem** ([14]) nie kwalifikowały się do kontroli wstępnej, ponieważ nie wiązały się z oceną pracowników, a raczej odnosiły się do oceny działań OLAF lub WCB. Przetwarzanie informacji do celów monitorowania działań instytucji UE z myślą o lepszym planowaniu przydziału środków znajduje się poza zakresem zastosowania art. 27 ust. 2 rozporządzenia. Wiele zaleceń dotyczących sprawy WCB odnosiło się do ograniczenia celu, do jakości danych, informacji, które mają być przekazywanych podmiotom danych oraz okresu zatrzymywania danych.

2.3.8. 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 wypadku 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 oraz podjąć dalsze kroki, aby zapewnić przestrzeganie zaleceń. W wypadku niestosowania się do decyzji EIOD ma on prawo przekazać sprawę do ETS 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 danych, ograniczenia celu oraz prawa dostępu i prawa do poprawy danych. 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 r. w oficjalnym piśmie przesyłanym wraz z opinią EIOD zwraca się do danej instytucji o informowanie go w terminie trzech miesięcy o środkach przedsięwziętych w celu realizacji zaleceń.

W 2007 r. EIOD zamknął 38 spraw, czyli ponaddwukrotnie więcej niż w 2006 r., na co z pewnością wpływ miał systematyczny monitoring zaleceń EIOD.

2.3.9. Wnioski i przyszłość

Jasne jest, że kontrole wstępne, zarówno „właściwe", jak i *ex post,* pozostawały jedną z głównych czynności w ramach nadzorczej funkcji EIOD. Na samym początku zdecydowano, że zastosowanie *ex post* art. 27 rozporządzenia byłoby znakomitą metodą monitorowania instytucji i agencji europejskich pod względem przetwarzania danych osobowych w obszarach najbardziej narażonych na zagrożenia; decyzja ta okazała się słuszna.

Wnioski dotyczące 2007 r. można podsumować w sposób następujący:

- termin określony jako „wiosna 2007" zaowocował ogromnym wzrostem liczby powiadomień od wielu urzędników ds. ochrony danych, zwłaszcza w pierwszej połowie roku, kiedy to wpłynęło ponad 42% wszystkich powiadomień (132 z 313, od 2004 r. do 31 grudnia 2007 r.);

([12]) Komisja (2007-375, 2007-376 i 2007-381).
([13]) Komisja (2004-235).
([14]) Komisyjny system rejestracji czasu (2007-503) WCB i system zarządzania czasem stosowany przez OLAF (2007-300).

- w związku z tym zespół EIOD ds. nadzoru pracował pod wielką presją; praca ta przyniosła bardzo zadowalające wyniki, jako że liczba przygotowanych opinii nie wpłynęła w żaden sposób na okres ich opracowania (w tym liczbę dni dodatkowych) ani na ich jakość;
- Niemniej jednak wiele pozostaje do poprawienia w zakresie ram czasowych, w jakich instytucje i agencje reagują na wnioski EIOD o dalsze informacje.
- ponieważ w wypadku spraw dotyczących kontroli *ex post* nie istnieją konkretne obszary priorytetowe, zakres tematów podlegających kontroli EIOD znacznie się poszerzył (zarządzanie czasem, sprawy OLAF, przetwarzanie międzyinstytucjonalne itd.);
- podobnie jak w poprzednim roku w dwóch opiniach zawarto wnioski, zgodnie z którymi w sprawach będących przedmiotem kontroli doszło do naruszenia rozporządzenia i należało wprowadzić istotne zmiany, aby zapewnić przestrzeganie zasad ochrony danych;
- zalecenia nadal koncentrowały się głównie na kwestiach zatrzymywania danych, prawa do informacji i prawa dostępu do danych.

Przyszłe działania będą się koncentrować na następujących zagadnieniach:

- instytucje powinny sfinalizować swoje procedury dotyczące powiadomień *ex post*, agencje zaś powinny uczynić istotny krok w kierunku realizacji takiego samego celu w 2008 r.;
- kontynuowane będzie systematyczne monitorowanie realizacji zaleceń na podstawie informacji od administratora danych; towarzyszyć mu będą także inspekcje na miejscu. Działania te obejmą również pełne wdrożenie procedury powiadamiania urzędników ds. ochrony danych oraz pełne przestrzeganie obowiązku powiadamiania EIOD o właściwych sprawach dotyczących kontroli wstępnej przed rozpoczęciem operacji przetwarzania danych;
- nowe podejście oparte na ustalaniu norm i przesyłaniu do kontroli wstępnej wyłącznie spraw odbiegających od tych norm będzie korzystne dla niektórych dziedzin, takich jak nadzór wideo;
- kryteria, które do tej pory ustalono, zostaną podsumowane według kategorii z myślą o zapewnieniu spójności wszystkich opinii oraz udzieleniu instytucjom i organom wytycznych dotyczących realizowania przez nie zasad ochrony danych.

2.4. Skargi

2.4.1. Wprowadzenie

Artykuł 41 ust. 2 rozporządzenia 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) ([15]).

Każda osoba fizyczna może wnieść skargę do EIOD na podstawie art. 32 i 33 rozporządzenia, niezależnie od narodowości czy miejsca zamieszkania ([16]). Skargi mogą także wnosić członkowie personelu instytucji i agencji europejskich, do których stosuje się regulamin pracowniczy, na podstawie art. 90 lit. b) regulaminu pracowniczego ([17]).

Skargi są dopuszczalne wyłącznie wtedy, gdy pochodzą od osoby fizycznej i dotyczą naruszenia zasad ochrony danych przez instytucję bądź 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 on stronie skarżącej potwierdzenie odbioru bez uszczerbku dla dopuszczalności sprawy, chyba że bez potrzeby dalszej analizy widać, iż skarga jest wyraźnie niedopuszczalna. EIOD zwraca się również do strony skarżącej o dostarczenie mu informacji na temat innych ewentualnych działań przed sądem krajowym, ETS lub Rzecznikiem Praw Obywatelskich (niezależnie od tego, czy są one w toku, czy nie).

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

([16]) 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". Art. 33: „Każda osoba zatrudniona w instytucji lub organie Wspólnoty może złożyć skargę do europejskiego inspektora ochrony danych, dotyczącą domniemanego naruszenia przepisów rozporządzenia 45/2001 regulującego przetwarzanie danych osobowych, bez użycia oficjalnych dróg".

([17]) Każda osoba, do której stosuje się niniejszy Regulamin pracowniczy, może złożyć do Europejskiego Pełnomocnika ds. Ochrony Danych wniosek lub zażalenie, w rozumieniu art. 90 ust. 1 i 2, w ramach jego kompetencji.

Jeśli dana sprawa jest dopuszczalna, EIOD rozpocznie jej wyjaśnianie, w szczególności przez skontaktowanie się z zainteresowaną instytucją bądź organem lub przez zwrócenie się do strony skarżącej o dodatkowe informacje. EIOD ma prawo uzyskać od stosownego administratora danych lub instytucji bądź organu dostęp do wszystkich danych osobowych oraz wszystkich informacji niezbędnych do przeprowadzenia dochodzenia. Ma również prawo do uzyskania dostępu do wszelkich pomieszczeń, w których administrator lub instytucja bądź organ Wspólnoty prowadzą działalność.

W razie 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. W tym przypadku EIOD może:

- nakazać administratorowi danych zastosowanie się do wniosków o wykonywanie pewnych praw podmiotu danych;
- ostrzec lub upomnieć administratora danych;
- nakazać sprostowanie, zablokowanie, usunięcie lub zniszczenie wszystkich danych;
- nałożyć zakaz przetwarzania;
- przekazać sprawę zainteresowanej instytucji wspólnotowej lub PE, Radzie i Komisji;
- przekazać sprawę do Trybunału Sprawiedliwości ([18]).

Gdyby decyzja miała obejmować przyjęcie środków przez instytucję bądź organ, EIOD monitoruje to odpowiednio z zainteresowaną instytucją bądź organem.

W 2007 r. EIOD otrzymał 65 skarg. Z tych 65 spraw tylko 29 zostało uznanych za dopuszczalne i zostało poddanych dalszej analizie przez EIOD. Poniżej przedstawiono krótką analizę niektórych z nich.

2.4.2. Sprawy uznane za dopuszczalne

Gromadzenie nadmiernej ilości danych dotyczących gości

Do EIOD wpłynęła skarga od jednego z członków grupy odwiedzającej Komisję Europejską; skarga ta dotyczyła publikacji numeru paszportu i daty urodzenia każdego członka grupy (sprawa 2006-0578). Po przeanalizowaniu sytuacji EIOD stwierdził, że była to nadmierna ilość danych, ponieważ nie była zgodna z zasadą adekwatności danych określoną w art. 4 ust. 1 lit. b) i c). W następstwie dochodzenia EIOD zaprzestano stosowania takiej praktyki, wobec czego EIOD uznał sprawę za zakończoną. W związku z tą skargą EIOD skorzystał z okazji, aby przypomnieć Komisji o jej obowiązku polegającym na udzielaniu kierownikom lub koordynatorom grup pewnych informacji, po to aby zapewnić rzetelne przetwarzanie danych.

Otrzymano także skargę dotyczącą przetwarzania danych osobowych przez Parlament Europejski w związku z obecnością na przesłuchaniu (sprawa 2007-0430). Skarżącą poproszono o podanie pewnych informacji, aby mogła uczestniczyć w przesłuchaniu, takich jak imię, nazwisko i data urodzenia. Kiedy osoba ta pojawiła się na przesłuchaniu, stwierdziła z oburzeniem, że daty urodzenia każdego z uczestników były powszechnie dostępne, ponieważ podano je na wykazie delegatów rozdawanym podczas posiedzenia. Po przeprowadzeniu dochodzenia EIOD stwierdził, że dane takie były niezbędne do wydania identyfikatorów przez dział ochrony Parlamentu Europejskiego, lecz rzeczywiście udostępnienie ich wszystkim uczestnikom nie było konieczne; sytuacja ta zostanie w przyszłości dokładnie zbadana.

Dostęp do danych

Do EIOD wpłynęła skarga jednego z młodszych ekspertów pracujących w przedstawicielstwie Komisji Europejskiej dotycząca ograniczonego dostępu do akt osobowych, jakiego mu udzielono; sytuacja taka stanowiła naruszenie art. 13 rozporządzenia (sprawa 2007-0127). Skarżący żalił się również na fakt, że Komisja bez jego zgody kontaktowała się z jego poprzednimi pracodawcami, tak więc nie był poinformowany o źródle danych; zakwestionował on także przekazanie przez DG RELEX jego danych osobowych przedstawicielstwu Komisji, w którym pracował.

Po przeanalizowaniu faktów EIOD stwierdził, że pewne ograniczenia prawa do dostępu były uzasadnione na podstawie art. 20 ust. 1 lit. c), zwłaszcza gdy były one konieczne, by chronić poprzednich pracodawców. Jeżeli chodzi o kontaktowanie się z poprzednimi pracodawcami bez zgody zainteresowanego, EIOD stwierdził, że skoro sam skarżący dostarczył pełnych informacji o swoich poprzednich pracodawcach i podpisał formularz podania, potwierdzając prawdziwość, kompletność i rzetelność podanych informacji, uzasadnione było założenie, że pracodawca może skontak-

([18]) Zob. art. 47 rozporządzenia 45/2001.

tować się z poprzednimi miejscami pracy, aby uzyskać potwierdzenie informacji zawartych w podaniu skarżącego. W kwestii przesłania danych z DG RELEX do przedstawicielstwa Komisji EIOD stwierdził, że przekazanie takie było niezbędne do zgodnego z prawem wykonania zadań przez przedstawicielstwo Komisji, zgodnie z art. 7 ust. 1 rozporządzenia.

Skarżący ten złożył także skargę do Europejskiego Rzecznika Praw Obywatelskich. EIOD przesłał zatem Europejskiemu Rzecznikowi Praw Obywatelskich wyniki swoich dochodzeń, aby uniknąć powielania działań.

Kolejna skarga wpłynęła od urzędnika Komisji, który upomniał się o przysługujące mu prawo do dostępu do protokołu *(procès verbal)* sporządzonego po rozmowie kwalifikacyjnej; brał on w niej udział, ubiegając się o aktualnie zajmowane stanowisko (sprawa 2007-0250). W tym kontekście prawo dostępu do danych należy rozumieć jako dostęp do danych osobowych skarżącego zawartych w protokole zespołu oceniającego. Po przeprowadzeniu dochodzenia EIOD ustalił, że nie sporządzono żadnego protokołu i w związku z tym nie zapisano żadnych danych osobowych w trakcie oceny rozmowy kwalifikacyjnej. Prawo dostępu do danych określone w art. 13 rozporządzenia nie mogło zatem mieć dalszego zastosowania. EIOD zamknął sprawę, podkreślając, że ogólną zasadą dobrej administracji jest zapisywanie ostatecznej oceny rozmowy kwalifikacyjnej lub egzaminu ustnego.

W skardze złożonej na Komisję Europejską chodziło o prawo dostępu do dokumentów przygotowawczych związanych z przyznawaniem punktów priorytetowych (w ramach procedury awansu) (sprawa 2007-0529). Odmówiono udzielenia dostępu do tych danych na podstawie regulaminu pracowniczego, uwzględniając tajność prac komisji konkursowej.

EIOD stwierdził w tej sprawie, że art. 6 załącznika III regulaminu pracowniczego (tajność prac komisji konkursowej) należy interpretować wraz z art. 20 ust. 1 lit. c) rozporządzenia. Prawo dostępu podmiotu danych do informacji nie zagraża niezależności i swobodzie dyrektorów, dane nie powinny jednak umożliwiać powiązania ich z żadną konkretną osobą. Niemniej jednak wnioski te nie mogły mieć zastosowania do skarżącego, jako że przedmiotowe dokumenty zostały wcześniej zniszczone, więc Komisja nie była w stanie udzielić do nich dostępu. EIOD poprosił zatem o nową szczegółową notatkę dotyczącą przyznawania punktów priorytetowych i zarządzania nimi, aby wykonać zapisy art. 4 ust. 1 lit. a) (rzetelność) i art. 12 (informacje, których należy udzielić) rozporządzenia.

Skarga złożona przeciwko Trybunałowi Obrachunkowemu dotyczyła prawa dostępu – na podstawie art. 13 – do ocen pracowników i dokumentacji uzasadniającej sprawozdania dotyczące personelu, jak również do ewentualnych wtórnych akt osobowych (sprawa 2006-597).

W wyniku dalszych próśb o wyjaśnienie sytuacji skierowanych zarówno do administratora danych, jak i do skarżącego, EIOD stwierdził, że procedura oceny stosowana w Trybunale Obrachunkowym (wcześniej skontrolowana przez EIOD w sprawie 2005-0152) nie wymaga żadnej dokumentacji uzasadniającej ustalenia zawarte w sprawozdaniach dotyczących oceny personelu. EIOD nie znalazł dowodów na istnienie wtórnych akt osobowych. Jeżeli chodzi o wniosek o zablokowanie danych, zdaniem EIOD żaden z warunków określonych w art. 15 rozporządzenia koniecznych do zablokowania danych nie miał w tym przypadku zastosowania.

Przekazywanie i kopiowanie poczty elektronicznej

Przeciwko OLAF wpłynęła skarga dotycząca przekazania osobistej wiadomości poczty elektronicznej, która była zaadresowana przez skarżącego do pracownicy OLAF, kierownikowi jej działu i jego zastępcy (sprawa 2007-0188). EIOD stwierdził, że skoro w wiadomości tej nie zaznaczono jej osobistego charakteru, zainteresowany członek personelu OLAF postąpił z nią zgodnie z wewnętrznymi zasadami tej instytucji. Tak więc kompetencje odbiorców jako takie nie naruszały zapisów rozporządzenia.

Ten sam skarżący żalił się również na fakt, że odpowiedź, którą otrzymał od OLAF, została skopiowana do wielu osób, co stanowiło naruszenie art. 7 ust. 1 rozporządzenia. EIOD zgodził się, że art. 7 ust. 1 dopuszcza przekazywanie pewnych danych, jeżeli są one konieczne do zgodnego z prawem wykonywania zadań leżących w zakresie kompetencji odbiorcy. Stanął on jednak na stanowisku, że w rozpatrywanej sprawie konieczność ta nie została jasno uzasadniona w stosunku do wszystkich osób, które otrzymały kopię wiadomości. Wszelkie przypadki przekazania danych

muszą ponadto być zgodne z innymi przepisami rozporządzenia, w szczególności podmiot danych musi wiedzieć, kto jest odbiorcą oraz jakie są kategorie odbiorców danych (art. 11 ust. 1 lit. c)), a w tym przypadku tak nie było.

EIOD współpracuje obecnie z OLAF, aby uniknąć powtórzenia się tego rodzaju sytuacji.

Wymóg podawania informacji dotyczących kart kredytowych

Dwóch członków personelu Parlamentu Europejskiego złożyło skargę dotyczącą wymogu podawania numeru prywatnej lub służbowej karty kredytowej, aby zapewnić rezerwację wyjazdów służbowych (sprawa 2007-0338). Po przeprowadzeniu dochodzenia EIOD doszedł do wniosku, że Parlament Europejski nie potrzebował kart kredytowych do dokonania rezerwacji hoteli; nie były one też potrzebne akredytowanemu biuru podróży. Hotele wymagają jednak podania numeru karty kredytowej, aby zapewnić rezerwację. Parlament rzeczywiście wymaga podania takiego numeru wyłącznie w przypadku, gdy członek personelu nie może zarezerwować pokoju w ramach ustalonego limitu kosztów i musi udokumentować koszty od akredytowanego biura podróży za pomocą formularza rezerwacji, w którym trzeba podać numer karty kredytowej. Od tego czasu Parlament podjął kroki prowadzące do usunięcia z formularza rezerwacji części, w której umieszcza się numer karty kredytowej.

Co do służbowej karty kredytowej podanie jej numeru zależy od indywidualnego wyboru dokonanego przez danego członka personelu. Wszelkie przetwarzanie danych osobowych dotyczące służbowej karty kredytowej zależy więc od jednoznacznego wyrażenia zgody członka personelu i jest zgodne z prawem na mocy art. 5 lit. d) rozporządzenia.

Przetwarzanie danych szczególnie chronionych

Do EIOD wpłynęła skarga pracownika EBC dotycząca niewłaściwej operacji przetwarzania danych dotyczących zdrowia w ramach administrowania zwolnieniami lekarskimi (sprawa 2007-0299). Skarżący był zdania, że przetwarzano – bez dostatecznego uzasadnienia konieczności takiego działania zgodnie z art. 10 ust. 2 lit. b) – szczególne kategorie danych osobowych, o których mowa w art. 10 ust. 1. Po przeanalizowaniu faktów EIOD stwierdził, że EBC miał prawo skorzystać z wyjątków określonych w art. 10 ust. 2 lit. b). Podstawą takiego wniosku był fakt, że przetwarzanie danych było konieczne do celów wypełnienia konkretnych praw i zobowiązań administratora danych w dziedzinie obowiązującego prawa pracy.

Prawo do poprawy danych

Pod koniec 2006 r. rozpatrywano skargę urzędnika Komisji dotyczącą prawa do poprawy danych (sprawa 2006-0436). W 2007 r. EIOD otrzymał potwierdzenie, że zastosowano tymczasowe rozwiązanie, tak aby umożliwić skarżącemu uzupełnienie danych osobowych w przebiegu pracy zawodowej *(historique de carrière)* w systemie Sysper2. Komisja wyjaśniła także, dlaczego zablokowanie danych osobowych skarżącego zakłóciłoby w rezultacie każdą operację przetwarzania w systemie Sysper2 danych skarżącego, np. wypłatę jego wynagrodzenia. EIOD zamknął tę skargę, a jednocześnie otworzył nową sprawę, aby monitorować techniczne wyjaśnienie trudności, jakie napotykała Komisja w dokonywaniu sprostowań i blokowaniu danych osobowych w bazie danych systemu Sysper2.

Wpłynęła skarga od osoby, która twierdziła, że w jej wyciągach wypłat emerytury od 9 listopada 2006 r. do chwili obecnej pojawiało się słowo „inwalidztwo". Ujawnienie danych dotyczących jej zdrowia było źródłem wielu problemów w kontaktach z trzema bankami. Po złożeniu skargi do EIOD, DG ADMIN ostatecznie usunęła słowo „inwalidztwo" z wyciągów skarżącej.

Obowiązek udzielania informacji

Podmiot danych złożył skargę przeciwko OLAF (sprawa 2007-0029). Skarżący twierdził, że dane, które go dotyczyły, a których on nie udostępnił, były gromadzone, przechowywane i przekazywane stronom trzecim w ramach sprawozdania końcowego OLAF z prowadzonych spraw, o czym zainteresowany nie został stosownie poinformowany (art. 12 rozporządzenia). Jako podstawę swojej skargi skarżący podawał również art. 13 rozporządzenia. Gdy skarżący zwrócił się do OLAF o udzielenie mu dostępu do swoich danych, otrzymał egzemplarz sprawozdania końcowego OLAF z prowadzonych spraw, z którego jednak usunięto wszelkie dane osobowe, łącznie z danymi skarżącego. Ponadto skarżący twierdził, że jego zdaniem sprawozdanie końcowe OLAF z prowadzonych spraw przedstawia jego postępowanie w sposób wybiórczy

i tendencyjny, pragnął więc skorzystać ze swojego prawa do poprawy danych (art. 14 rozporządzenia).

Po przeanalizowaniu sprawy EIOD stwierdził, że OLAF nie przestrzegał obowiązków, które nakładają art. 11 i 12 rozporządzenia. Ponadto EIOD był zdania, że skarżący powinien otrzymać taki egzemplarz sprawozdania końcowego z prowadzonych spraw, w którym widoczne byłyby wszelkie operacje przetwarzania jego danych – w ten sposób spełnione byłyby wymogi art. 13 rozporządzenia (bez zaczernienia fragmentów zawierających jego dane osobowe). EIOD dodał, że oceni prośbę o poprawę danych, po tym jak skarżący otrzyma dostęp do danych i w przypadku gdy będzie on nadal domagał się takiej oceny.

Publikacja w sprawozdaniu rocznym za 2005 r.

W dniu 1 lipca 2005 r. do EIOD wpłynęła skarga przeciwko OLAF – odnosząca się do 2002 r. oraz początku 2004 r. – która dotyczyła różnych kwestii objętych rozporządzeniem, zwłaszcza nierzetelnego przetwarzania danych osobowych oraz przekazywania przez OLAF nieprawidłowych danych dotyczących skarżącego w kontekście dochodzenia prowadzonego w spawie jego domniemanego udziału w aferze łapówkarskiej (sprawa 2005-0190).

W dniu 1 grudnia 2005 r. zastępca EIOD przyjął decyzję dotyczącą tej skargi. Zgodził się on wprawdzie, że zajęcie się tą skargą leżało w kompetencjach EIOD, ponieważ dotyczyła ona kwestii, które są objęte zakresem zastosowania rozporządzenia 45/2001; niemniej jednak EIOD nie był w stanie podjąć żadnych dalszych działań, które mogłyby doprowadzić do pożądanej zmiany sytuacji. Sprawę tę skrótowo wspomniano w sprawozdaniu rocznym za 2005 r.

W 2006 r. skarżący złożył skargę do Europejskiego Rzecznika Praw Obywatelskich dotyczącą sposobu postępowania z jego pierwotną skargą. W drugiej skardze wyraził on zastrzeżenia co do krótkiego przedstawienia tej sprawy w sprawozdaniu rocznym za 2005 r., stwierdzając, że było ono nieprawidłowe i przedwczesne. Jeżeli chodzi o drugą skargę, EIOD zgodził się przedstawić zaktualizowaną wersję sprawy wraz z właściwym i kompletnym opisem skargi, tak jak przedstawiono powyżej. Na początku 2008 r. pierwsza skarga była wciąż rozpatrywana przez Europejskiego Rzecznika Praw Obywatelskich.

2.4.3. Sprawy niedopuszczalne: główne przyczyny niedopuszczalności

Z 65 skarg otrzymanych w 2007 r. 36 uznano za niedopuszczalne z uwagi na brak właściwości EIOD w tym zakresie. Znakomita większość tych skarg nie dotyczyła przetwarzania danych osobowych przez instytucję lub organ WE, a odnosiła się wyłącznie do przetwarzania danych 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 właściwa w przypadku, gdy dane państwo członkowskie nie wykonuje prawidłowo dyrektywy 95/46/WE.

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 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 Rzecznika Praw Obywatelskich

Nikiforos Diamandouros, Joaquín Bayo Delgado i Peter Hustinx na konferencji prasowej

mogą obejmować kwestie ochrony danych. Podobnie skargi wnoszone do EIOD mogą dotyczyć skarg, które były już, w części lub w całości, przedmiotem decyzji Rzecznika Praw Obywatelskich.

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 r. podpisano protokół ustaleń między Europejskim Rzecznikiem Praw Obywatelskich a EIOD. W praktyce powyższy protokół w każdym stosownym przypadku skutkował użyteczną wymianą informacji między EIOD a Europejskim Rzecznikiem Praw Obywatelskich. Europejski Rzecznik Praw Obywatelskich konsultował się z EIOD w sprawach dotyczących ochrony danych i informował EIOD o swoich decyzjach związanych ze sprawami, które również wpłynęły do EIOD lub miały wpływ na kwestie ochrony danych. W przypadku jednej ze skarg, kiedy to skarżący postanowił także złożyć skargę do Europejskiego Rzecznika Praw Obywatelskich, wyniki dochodzenia przeprowadzonego przez EIOD zostały przesłane Europejskiemu Rzecznikowi Praw Obywatelskich, aby uniknąć powielania działań.

EIOD służył radą Europejskiemu Rzecznikowi Praw Obywatelskich w sprawie kilku skarg związanych z dostępem do dokumentów zgodnie z częściami C i D protokołu ustaleń. Stosowne ustalenia przesłano Europejskiemu Rzecznikowi Praw Obywatelskich, który uwzględnił je w swoich decyzjach. Skargi te dały EIOD sposobność do dalszego rozwijania polityki zmierzającej do osiągnięcia równowagi między publicznym dostępem do dokumentów a ochroną danych w świetle dokumentu bazowego EIOD z lipca 2005 r. (opublikowanego na stronie internetowej), w przypadkach gdy dostęp do informacji jest wyraźnie przedmiotem publicznego zainteresowania. Skargi obejmowały prośby o dostęp do dodatkowych systemów emerytalnych dla posłów do Parlamentu Europejskiego, zestawienia rachunków wszystkich posłów do Parlamentu Europejskiego jednego z państw członkowskich oraz przedłużenie oddelegowania urzędnika (w obrębie Komisji).

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 EIOD we właściwym czasie.

Przedstawiciele personelu uczestniczyli w warsztatach poświęconych rozpatrywaniu spraw zorganizowanych w Helsinkach w kwietniu 2007 r. i w Lizbonie w listopadzie 2007 r. przez krajowe organy ds. ochrony danych. Podczas tych warsztatów EIOD przedstawił prezentacje dotyczące publicznego dostępu do dokumentów i ochrony danych w administracji UE, a także na temat dochodzeń wewnętrznych prowadzonych przez OLAF oraz sądowego badania komputerów.

EIOD skorzystał również w pełni z tej okazji, aby wymienić doświadczenia i zebrać informacje na temat bieżących zagadnień dotyczących ochrony danych w kontekście krajowym. EIOD podniósł między innymi kwestię wprowadzania w życie w państwach członkowskich dyrektywy 2005/60/WE w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu, która jest istotna dla rozpatrywanej aktualnie sprawy dotyczącej kontroli wstępnej.

2.5. Postępowania wyjaśniające

Artykuł 46 lit. b) rozporządzenia przewiduje, że EIOD może przeprowadzać dochodzenia, także z własnej inicjatywy. EIOD przeprowadził wiele dochodzeń, z których kilka zasługuje na szczególną uwagę w niniejszym sprawozdaniu (zob. również pkt 2.9 dotyczący nadzoru wideo).

Audyt bezpieczeństwa OLAF

W 2007 r. EIOD otrzymał od OLAF liczne powiadomienia dotyczące czynności związanych z przetwarzaniem danych, przeprowadzanych z użyciem tej samej infrastruktury informatycznej. Narzędzia te, które były początkowo zainstalowane w centrum danych Komisji Europejskiej, są teraz przeniesione do siedziby OLAF i zarządzane bezpośrednio przez jego personel.

Aby zapewnić spójne podejście do środków bezpieczeństwa stosowanych przez OLAF, EIOD postanowił przeprowadzić inspekcję w zakresie bezpieczeństwa i przeanalizował środki OLAF w tej dziedzinie w ujęciu horyzontalnym zamiast osobno dla każdego

powiadomienia w sprawie kontroli wstępnej. Analizie tej towarzyszyła specjalna inspekcja w zakresie bezpieczeństwa, co także przyczyniło się do lepszego uwzględnienia wymogów poufności związanych z tymi środkami bezpieczeństwa.

Głównym celem inspekcji było zebranie informacji na temat wdrażanych lub planowanych środków w zakresie bezpieczeństwa i ochrony danych oraz porównanie ich z wymogami w tej dziedzinie, aby ocenić ich zgodność z normami prawnymi i technicznymi.

Po przedstawieniu wytycznych w formie zaleceń EIOD wyraził ogromne zadowolenie ze środków w zakresie bezpieczeństwa wprowadzonych przez OLAF do systemów i aplikacji informatycznych pozostających w jego gestii.

Ocena wdrożenia tych środków bezpieczeństwa zostanie przeprowadzona w 2008 r. i towarzyszyć jej będzie przewidywany przez OLAF szczegółowy audyt bezpieczeństwa, w którym – w charakterze obserwatora – weźmie udział także EIOD.

SWIFT

Dnia 1 lutego 2007 r. EIOD wydał opinię w sprawie roli EBC w sprawie SWIFT (dostęp władz USA do danych bankowych w ramach walki z terroryzmem). W opinii położono nacisk na rolę EBC jako organu nadzorującego, użytkownika i decydenta.

Jednocześnie, w kontekście skoordynowanych działań organów ds. ochrony danych UE, EIOD zwrócił się również do głównych instytucji wspólnotowych o wyjaśnienia dotyczące wykorzystywanych systemów płatności i stosunków umownych ze SWIFT.

Dnia 14 lutego 2007 r. Parlament Europejski przyjął wspólną rezolucję w sprawie danych dotyczących przelotu pasażerów (PNR) oraz SWIFT. Jeżeli chodzi o SWIFT, Parlament Europejski poparł opinię EIOD i wezwał EBC i inne stosowne instytucje do dopilnowania, by europejskie systemy płatności były w pełni zgodne z europejskim prawem dotyczącym ochrony danych.

Wiosną 2007 r., na wniosek EIOD, EBC przedstawił sprawozdanie na temat działań podjętych w celu zastosowania się do opinii, natomiast inne instytucje przedstawiły wyjaśnienia dotyczące zasad dotyczących ochrony danych w ramach ich systemów płatności.

Na podstawie otrzymanych informacji EIOD zalecił stosownym instytucjom wspólnotowym podjęcie działań gwarantujących pełne dotrzymanie przez nie zobowiązań na mocy rozporządzenia (WE) nr 45/2001, szczególnie przekazanie wystarczających informacji członkom personelu i innym osobom, z którymi łączą je stosunki umowne.

W szerszym kontekście, jako członek Grupy Roboczej Art. 29, EIOD bacznie monitorował postępy osiągnięte w tej sprawie, takie jak:

- przystąpienie SWIFT do zasad bezpiecznego transferu danych osobowych *(safe harbor),* aby objąć nimi przekazywanie danych do celów handlowych do centrum operacyjnego w USA;
- wyjaśnienia i zapewnienia przedstawione przez Departament Skarbu USA dotyczące podstawowych aspektów – np. celów, proporcjonalności, nadzoru i mechanizmów odszkodowawczych – dotyczących dostępu do danych SWIFT i ich przetwarzania w związku z sądowymi nakazami wydania dokumentów;
- ważne zmiany w strukturze usług płatniczych SWIFT, których wprowadzenie zapowiadane jest w dłuższym okresie: nowe centrum operacyjne zlokalizowane w Szwajcarii będzie dopilnowywać, by wiadomości przesyłane między podmiotami w Europie pozostawały na tym kontynencie i by nie powstawały ich lustrzane kopie w Stanach Zjednoczonych.

W 2008 r. EIOD w koordynacji z innymi organami ds. ochrony danych zamierza dalej pobudzać i uważnie śledzić postępy w tej dziedzinie.

2.6. Polityka w zakresie kontroli

2.6.1. Wiosna 2007 i okres późniejszy

Zgodnie z art. 41 ust. 2 rozporządzenia (WE) 45/2001 EIOD jest odpowiedzialny za monitorowanie i zapewnienie stosowania rozporządzenia. W marcu 2007 r. EIOD zapoczątkował procedurę mającą na celu dokonanie oceny przestrzegania rozporządzenia w różnych instytucjach i agencjach oraz utrzymanie tzw. efektu wiosny 2007 (zob. pkt 2.3).

Pierwsza część operacji zapoczątkowanej w 2007 r. miała formę pism skierowanych do dyrektorów wszystkich instytucji i agencji z prośbą o podsumowanie postępów dotychczas osiągniętych w poszczególnych działach administracji UE.

EIOD rozsyłał te pisma stopniowo, według daty ustanowienia poszczególnych agencji lub instytucji.

W przypadku niektórych agencji pierwszym krokiem było zwrócenie się do ich dyrektorów o wyznaczenie urzędnika ds. ochrony danych (DPO). W marcu 2007 r. dziesięć agencji operacyjnych nie miało jeszcze wyznaczonego DPO. Kopie pism zostały przesłane do właściwych dyrekcji generalnych Komisji, aby podkreślić konieczność zapewnienia DPO odpowiednich zasobów niezbędnych do pełnienia ich obowiązków.

Od czasu wysłania tych pism wszystkie agencje operacyjne wyznaczyły DPO, choć w przypadku jednej z agencji wyznaczenie to ma jedynie charakter tymczasowy. Ponadto w listopadzie 2007 r. EIOD został poinformowany o wyznaczeniu DPO w Europejskim Funduszu Inwestycyjnym, którego funkcję do tej pory sprawował DPO z Europejskiego Banku Inwestycyjnego.

Do tych instytucji i agencji, w których istniało już stanowisko DPO, przesłano w kwietniu 2007 r. pisma z prośbą o udzielenie informacji dotyczących czterech następujących zagadnień:

1) status DPO;
2) spis operacji, w ramach których przetwarzano dane osobowe;
3) spis operacji przetwarzania danych wchodzących w zakres art. 27 rozporządzenia (WE) nr 45/2001;
4) dalsze wdrażanie rozporządzenia.

Do szefa administracji EIOD, jako instytucji również podlegającej rozporządzeniu (WE) nr 45/2001, przesłano specjalną notę z prośbą o udzielenie informacji na temat spisu operacji przetwarzania danych, spisu operacji przetwarzania danych podlegających kontroli wstępnej oraz dalszych środków wdrażania.

2.6.2. DPO

Wyznaczenie DPO

Jak już wspomniano powyżej, wszystkie instytucje i agencje wspólnotowe wyznaczyły DPO. Większe instytucje (Komisja Europejska, Parlament Europejski, Rada Unii Europejskiej i Europejski Trybunał Sprawiedliwości) wyznaczyły także zastępcę DPO. W większości wypadków zastępca jest zatrudniony na pełen etat. Niektóre instytucje wyznaczyły również koordynatorów ds. ochrony danych lub osoby do kontaktu.

Niezależność DPO

W dokumencie przedstawiającym stanowisko EIOD w sprawie DPO ([19]) podkreślono, że niezależny status DPO w instytucjach i agencjach mogłyby naruszyć niektóre elementy, mianowicie fakt, że nie są oni zatrudnieni na pełen etat (a zatem istnieje potencjalny konflikt interesów dotyczący czasu przeznaczonego na pełnienie obowiązków DPO), a także pozycja DPO w hierarchii oraz osoba, której powinien on podlegać.

Większe instytucje (Komisja, Parlament i Rada) mają DPO zatrudnionych na pełen etat. OHIM tymczasowo wyznaczył DPO na pełen etat na okres od lutego do grudnia 2007 r., aby mógł on skoncentrować się na kwestiach związanych z jego stanowiskiem. Wszystkie inne instytucje i agencje zatrudniają DPO na część etatu, nie określając jednak wyraźnie czasu, jaki osoba ta ma przeznaczać na wykonywanie zadań DPO. W większości tych przypadków DPO jest jednocześnie radcą prawnym.

EIOD podkreślił także, że niezależność jest kwestią powiązaną z pozycją DPO w hierarchii oraz z osobą, której on podlega. Większość instytucji i agencji przedstawiła w tym względzie gwarancje polegające na podporządkowaniu stanowiska DPO bezpośrednio sekretarzowi generalnemu lub dyrektorowi lub na przedkładaniu EIOD do uprzedniej konsultacji oceny prac DPO.

Odpowiedni personel i zasoby

EIOD podkreślił potrzebę odpowiedniego personelu i zasobów umożliwiających DPO wykonywanie jego zadań (w tym systemów informatycznych, zasobów ludzkich, szkoleń, zasobów finansowych).

Większość instytucji i agencji przedstawiła stosowne informacje na temat zasobów i personelu udostępnionego DPO, aby umożliwić mu pełnienie jego obowiązków. W niektórych wypadkach wyznaczono zastępcę

([19]) Zob. dokument EIOD przedstawiający jego stanowisko w sprawie roli urzędników ds. ochrony danych (DPO) w zapewnianiu skutecznego stosowania rozporządzenia (WE) nr 45/2001 (dostępny na stronie internetowej EIOD w części „Consultation").

DPO. W innych wypadkach DPO korzysta z pomocy innych służb, np. służby prawnej.

Jeżeli chodzi o kwestie budżetowe, tylko jedna instytucja wspomniała o przydzieleniu określonego budżetu na DPO. Niektóre instytucje podkreślają jednak, że nigdy nie odmówiły przyznania środków budżetowych na ten cel.

Niektóre instytucje i agencje wspominają o szkoleniach dla DPO, zwykle w postaci udziału w spotkaniach DPO lub w sesjach szkoleniowych organizowanych przez EIOD. Wiele instytucji i agencji zaznaczyło, że utworzyły specjalny system informatyczny na użytek ochrony danych.

2.6.3. Spis operacji przetwarzania danych

Chociaż agencje i instytucje nie są prawnie zobowiązane do sporządzania spisu wszystkich przeprowadzonych przez nie operacji przetwarzania danych, spisy takie stanowią dla EIOD przydatne narzędzie oceny przestrzegania przepisów rozporządzenia. W związku z tym EIOD zwrócił się do instytucji i agencji o utworzenie takiego spisu i o przekazywanie mu sprawozdań z postępu prac w tym zakresie. EIOD poprosił również o przekazanie informacji na temat obowiązku powiadamiania DPO o operacjach przetwarzania danych.

Większość agencji i instytucji sporządziła taki spis (lub jest w trakcie sporządzania), co umożliwia im ocenę przestrzegania rozporządzenia.

2.6.4. Spis spraw dotyczących kontroli wstępnej

W swoim piśmie EIOD poprosił o przegląd sytuacji w zakresie przestrzegania rozporządzenia w dziedzinie kontroli wstępnej. EIOD poprosił o aktualny spis wszystkich operacji podlegających kontroli wstępnej oraz status tych spraw, a także o zaktualizowany status spraw należących do wstępnych obszarów priorytetowych (dokumentacji medycznej, ocen personelu, postępowań dyscyplinarnych, usług socjalnych i e-monitorowania).

Większość instytucji i agencji utworzyła taki spis, umożliwiający EIOD ocenę przestrzegania art. 27 rozporządzenia. Skutkiem zapoczątkowania operacji „wiosna 2007" był ogromny wzrost liczby powiadomień w sprawie kontroli wstępnej *ex post*, o których wspomniano powyżej (zob. pkt 2.3.4). W niektórych przypadkach powiadomiono o wszystkich sprawach dotyczących kontroli *ex post* w instytucji. Operacja dała także instytucjom i agencjom sposobność do zaktualizowania i przekazania EIOD informacji na temat statusu niektórych nierozstrzygniętych spraw i operacji przetwarzania danych w obszarach priorytetowych.

2.6.5. Dalsze wdrażanie

EIOD zwrócił się również do instytucji i agencji wspólnotowych o przekazanie informacji zwrotnych w sprawie dalszego wdrażania rozporządzenia, w tym przyjęcia przepisów wykonawczych, oraz poszerzania wiedzy personelu o ochronie danych. Poprosił instytucje i agencje o przesłanie wzorów oświadczeń o ochronie danych osobowych, z których korzystają, oraz informacji zwrotnych o ogólnych praktykach w zakresie sposobów, jak podmioty danych mogą korzystać ze swoich praw.

Artykuł 24 ust. 8 rozporządzenia przewiduje, że dalsze przepisy wykonawcze dotyczące urzędnika ds. ochrony danych będą przyjęte przez każdą instytucję lub organ. Dotyczą one w szczególności zadań, obowiązków i uprawnień DPO.

Do tej pory jedynie osiem instytucji i agencji przyjęło przepisy wykonawcze. Cztery instytucje i agencje planują przyjęcie tych przepisów w 2008 r., a dwie agencje planują rozpoczęcie prac nad przepisami. Pozostaje zatem jeszcze wiele instytucji i agencji, które nie przyjęły takich przepisów.

Informacje służące poszerzeniu wiedzy na temat ochrony danych przekazuje się zwykle za pośrednictwem stron intranetowych i internetowych, publikacji rejestrów elektronicznych, broszur informacyjnych i biuletynów. Niektóre instytucje aktywnie organizują szkolenia dla członków personelu lub zapraszają wykładowców z zewnątrz do propagowania ochrony danych wewnątrz instytucji.

Instytucje i agencje zredagowały różne oświadczenia o ochronie danych osobowych, w których zamieszczono informacje zawarte w art. 11 i 12 rozporządzenia. Do najbardziej powszechnych praktyk należy: publikacja oświadczenia o ochronie danych osobowych na stronie intranetowej lub internetowej, informowanie za pośrednictwem indywidualnych komunikatów dla personelu, rozwieszanie zawiadomień o ochronie danych w najbardziej uczęszczanych miejscach lub umieszczanie wymogów w zakresie ochrony danych w dokumentach (np. umowach).

Jeżeli chodzi o sposoby, jak podmioty danych mogą korzystać ze swoich praw, obejmują one zwykle możliwość kontaktu z DPO lub administratorem danych albo wysłania w tym celu wiadomości na ogólny adres elektroniczny. Niektórzy DPO przygotowali również formularze elektroniczne dostępne w intranecie ich instytucji bądź agencji.

2.6.6. Podsumowanie

Operacja „wiosna 2007" pozwoliła EIOD na podsumowanie poziomu przestrzegania przez instytucje i agencje rozporządzenia (WE) nr 45/2001. W tym celu EIOD przygotował ogólne sprawozdanie. Zobowiązał w nim agencje, które jeszcze nie wyznaczyły swojego DPO, do obsadzenia tego stanowiska oraz do uwzględnienia zasobów i personelu niezbędnych do pełnienia przez niego obowiązków. Operacja zachęciła również instytucje i agencje do określenia operacji przetwarzania danych, które zawierają dane osobowe, oraz do ustalenia, które z tych operacji podlegają wstępnej kontroli EIOD. Operacja skłoniła instytucje i agencje do nadrobienia zaległości w sprawach dotyczących kontroli wstępnej *ex post,* czego skutkiem był ogromny wzrost liczby spraw przedłożonych EIOD do kontroli wstępnej w 2007 r.

Operację należy traktować jako zapoczątkowanie przez EIOD stałej praktyki służącej zapewnianiu przestrzegania rozporządzenia, która to praktyka może obejmować kontrole na miejscu oraz regularną wymianę informacji między EIOD a dyrektorami instytucji i agencji w celu oceny dalszych postępów osiągniętych w tej dziedzinie.

2.7. Środki administracyjne

Artykuł 28 ust. 1 rozporządzenia ustanawia prawo EIOD do uzyskiwania informacji o środkach administracyjnych związanych z przetwarzaniem 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).

W ramach konsultacji w sprawie środków administracyjnych planowanych przez instytucje i organy wspólnotowe poruszono rozmaite kwestie problematyczne, w tym zagadnienia odnoszące się do ustanowienia okresów przechowywania niektórych kategorii dossier, dokumentów strategicznych dotyczących Internetu, procedur śledczych związanych z nadużyciami i korupcją, wymiany informacji, przepisów wykonawczych dotyczących ochrony danych i możliwości zastosowania krajowego ustawodawstwa o ochronie danych.

Okresy przechowywania niektórych kategorii dossier

Komisja Europejska zasięgnęła konsultacji EIOD w sprawie projektu wspólnego wykazu przechowywanych dossier. Celem takiego wykazu jest ustalenie okresów przechowywania dokumentów, stosowanych przez dyrekcje generalne i wydziały w przypadku niektórych kategorii dossier, z uwzględnieniem przydatności danego dossier do celów administracyjnych, oraz zobowiązań prawnych.

EIOD przyjął z zadowoleniem fakt odniesienia się do jego opinii dotyczących powiadomień w sprawie kontroli wstępnej w dziedzinie selekcji, dochodzeń wewnętrznych oraz pomocy socjalnej i finansowej, jak również w sprawie przechowywania akt postępowań dyscyplinarnych (sprawa 2007-222).

EIOD poprosił jednak o przedstawienie uzasadnienia w przypadku, między innymi:

- przechowywania dokumentacji zawierającej dane administracyjne i finansowe dotyczące organizacji konferencji informacyjnych;
- przechowywania przez 10 lat dokumentacji dotyczącej realizacji polityki w zakresie zasobów ludzkich, jeżeli dokumentacja taka zawiera dane osobowe;
- przechowywania akt osobowych przez okres do ośmiu lat po wygaśnięciu wszystkich praw osoby zainteresowanej i osób pozostających na jej utrzymaniu do czasu upłynięcia co najmniej 120 lat od jej daty urodzenia.

Procedury dochodzeniowe

OLAF przedłożył EIOD skróconą wersję zmienionego podręcznika OLAF dotyczącego zasad statutowych i proceduralnych tego urzędu, jego procedur dochodzeniowych oraz praw osób i obowiązków dotyczących informowania. EIOD odniósł się do swojej opinii z dnia 23 czerwca 2006 r. w sprawie powiadomienia

w sprawie kontroli wstępnej dotyczącej wewnętrznych dochodzeń prowadzonych przez OLAF (sprawa 2005-418). Zalecono, by w przyszłej wersji podręcznika OLAF zaznaczono, że stosowana jest ogólna zasada dostępu podmiotu danych do jego danych osobowych zawartych w dokumentacji, chyba że zostanie uznane, iż dostęp ten szkodzi dochodzeniu, przy czym decyzje o takich wyjątkach podejmowane są w indywidualnych przypadkach i nigdy nie są stosowane systematycznie. EIOD poprosił o skonsultowanie się z nim przed przyjęciem nowej, dłuższej wersji podręcznika OLAF (sprawa 2007-310).

EIOD wydał opinię w sprawie projektu decyzji Europejskiego Trybunału Sprawiedliwości zmieniającej wcześniejszą decyzję w sprawie warunków prowadzenia wewnętrznych dochodzeń w ramach walki z nadużyciami, korupcją i wszelkimi niezgodnymi z prawem działaniami, które mogą zaszkodzić interesom Wspólnot. EIOD odniósł się do swojej opinii w sprawie wewnętrznych dochodzeń prowadzonych przez OLAF (sprawa 2005-418) i podkreślił, że gwarancje przekazywane podmiotom danych są zgodne z wytycznymi zawartymi w jego opinii. Zalecono jednak wyraźne wskazanie obowiązku zachowania poufnego charakteru tożsamości informatora oraz wyraźne odesłanie do art. 11 i 12 rozporządzenia (WE) nr 45/2001 (sprawa 2007-167).

Wymiana informacji między OLAF a Eurojustem

OLAF przedłożył EIOD projekt porozumienia w sprawie warunków współpracy między OLAF a Eurojustem, w którym głównie określa się tryb wymiany informacji, w tym danych osobowych, między tymi dwoma organami, a także w niektórych przypadkach wzmacnia się lub precyzuje niektóre elementy istniejących ram prawnych. Oprócz pewnych zmian redakcyjnych zasugerowanych przez EIOD zaznaczono, że OLAF powinien przewidzieć prawo podmiotów danych do otrzymywania informacji o przekazywaniu ich danych do Eurojustu oraz o możliwości dalszego przekazania tych danych. Zaznaczono, że takie prawo może istnieć na mocy art. 11 ust. 1 lit. c) i art. 12 ust. 1 lit. c) rozporządzenia (WE) nr 45/2001, chyba że ma zastosowanie wyjątek (sprawa 2007-258).

Dokumenty strategiczne dotyczące Internetu

Z EIOD skonsultował się także DPO Trybunału Obrachunkowego w sprawie dokumentu strategicznego tej instytucji dotyczącego Internetu. EIOD podkreślił, iż biorąc pod uwagę, że z jednej strony monitorowanie korzystania z Internetu opisane w strategii dotyczącej bezpieczeństwa Internetu prowadzi do oceny postępowania użytkowników, a z drugiej strony pociąga za sobą gromadzenie danych związanych z podejrzeniami o popełnienie przestępstwa, monitorowanie takie najprawdopodobniej podlega kontroli wstępnej na mocy art. 27 lit. a) i b) rozporządzenia. Jednym z wielu zaleceń merytorycznych, jakie wydał EIOD, było ustalenie okresu, w którym pliki dziennika będą przechowywane do celów monitorowania, oraz poinformowanie o tym terminie użytkowników w dokumencie strategicznym dotyczącym Internetu (sprawa 2007-593).

EIOD przyjął z zadowoleniem inicjatywę DPO Parlamentu Europejskiego dotyczącą „Protokołu dobrych praktyk w zakresie dochodzeń prowadzonych w przypadku podejrzeń o niezgodne z prawem korzystanie z dostępu do Internetu lub z poczty elektronicznej". EIOD stwierdził, że związany z e-monitoringiem element dochodzeń prowadzonych w przypadku podejrzeń o niezgodne z prawem korzystanie z dostępu do Internetu lub z poczty elektronicznej jest elementem nowym i w związku z tym zalecił przedłożenie protokołu do kontroli wstępnej przez EIOD na mocy art. 27 rozporządzenia. Jedna z uwag EIOD dotyczyła potrzeby określenia stopnia powagi naruszenia, aby uniknąć nieuzasadnionych dochodzeń. Ponadto – do celów informacyjnych – zalecono odniesienie do art. 20 rozporządzenia (warunki, na jakich można odroczyć obowiązek informowania). Za istotne uznano również sprecyzowanie w protokole na wniosek zainteresowanej osoby charakteru prowadzonych dochodzeń. Ponadto EIOD podkreślił, że te same gwarancje ochrony danych mają zastosowanie do ogółu dochodzeń administracyjnych (sprawa 2007-261).

Przepisy wykonawcze w zakresie ochrony danych

EIOD przedstawił uwagi w sprawie projektu przepisów wykonawczych dotyczących ochrony danych we wspólnotowej Agencji Kontroli Rybołówstwa (CFCA). Poza pewnymi zmianami merytorycznymi EIOD przyjął z zadowoleniem podejście CFCA, zgodnie z którym nie ograniczono przepisów wykonawczych do DPO, jak przewidziano w art. 24 ust. 8 rozporządzenia, ale rozwinięto je tak, by dotyczyły również roli administratorów danych oraz praw podmiotów danych (sprawa 2007-651).

EIOD przedłożono również decyzję dyrektora wykonawczego w sprawie przyjęcia przepisów wykonawczych dotyczących ochrony danych w Europejskiej Agencji ds. Bezpieczeństwa na Morzu (EMSA). EIOD zalecił między innymi opisanie zadań, obowiązków i uprawnień DPO, szczególnie uprawnienia do rozpatrywania zapytań i skarg, oraz odniesienie do art. 11 i 12 rozporządzenia (sprawa 2007-395).

Ponadto DPO EMSA zwrócił się o opinię w sprawie projektu przepisów dotyczących ochrony danych w intranecie. EIOD zalecił pewne zmiany redakcyjne w celu zapewnienia spójności z rozporządzeniem (sprawa 2007-397).

Rejestrowanie orzecznictwa krajowego na *portail externe*

Przeprowadzono konsultacje z EIOD w sprawie projektu opinii DPO Trybunału Sprawiedliwości dotyczącej rejestrowania orzecznictwa krajowego na *portail externe,* co budzi wątpliwości w przypadku postępowań w trybie prejudycjalnym w dziedzinie prawa wspólnotowego.

EIOD zaznaczył, że przed opublikowaniem orzecznictwa krajowego na *portail externe* ważne jest określenie potrzeby tej operacji w świetle celów, które mają być osiągnięte. EIOD zalecił Trybunałowi Sprawiedliwości, aby rozważył metodologię anonimizacji orzeczeń sądów krajowych, z uwzględnieniem pożądanego poziomu przejrzystości. Jeżeli nie zostanie zapewniona anonimowość danych, należy uwzględnić art. 5 lit. a) i d) oraz art. 12 rozporządzenia (sprawa 2007-444).

Możliwość zastosowania krajowego ustawodawstwa o ochronie danych

DPO Europejskiej Fundacji na rzecz Poprawy Warunków Życia i Pracy (Eurofound) skonsultował się w sprawie polityki tej agencji w zakresie ochrony danych o pracownikach. Ponieważ siedziba agencji znajduje się w Irlandii, poruszono kwestię zastosowania ustawodawstwa irlandzkiego. Zaznaczono, iż chociaż w orzecznictwie uznano, że immunitet instytucji i organów wspólnotowych nie jest bezwzględny i że prawo krajowe może mieć zastosowanie w pewnych dziedzinach, które nie są objęte prawem UE lub w których nie ma przepisów szczególnych, EIOD nie mógł znaleźć uzasadnienia dla odniesienia do krajowego ustawodawstwa o ochronie danych. Inne wydane przez niego zalecenia dotyczyły okresu przechowywania danych medycznych, danych o postępowaniach dyscyplinarnych i o połączeniach oraz danych dotyczących monitorowania serwera wymiany danych, bezpieczeństwa lub zarządzania połączeniami (sprawa 2007-305).

Inne kwestie

Przedmiotem konsultacji – jako kwestia organizacji wewnętrznej – było również utworzenie sieci korespondentów ds. ochrony danych w Parlamencie Europejskim. EIOD z zadowoleniem przyjął pomysł DPO Parlamentu i zaznaczył, że taka sieć przyniosła bardzo pozytywne wyniki w Komisji Europejskiej, gdzie ułatwiła rozpowszechnianie i monitorowanie przetwarzania danych osobowych oraz pomagała administratorom danych w wykonywaniu ich pracy (sprawa 2007-297).

DPO Europejskiego Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA) zwrócił się o poradę dotyczącą decyzji w sprawie rekompensaty za pracę lub delegacje wykonywane w soboty, niedziele i dni wolne od pracy lub w godzinach od 22:00 do 7:00, a także w sprawie rozwiązań dotyczących elastycznych terminów urlopów. W tym przypadku, ponieważ dane osobowe gromadzone były w ramach tych dwóch procedur, EIOD stwierdził, że rozporządzenie ma zastosowanie. Same decyzje nie wzbudziły żadnych szczególnych wątpliwości w zakresie ochrony danych (sprawa 2007-725).

2.8. E-monitoring

Korzystanie z narzędzi łączności elektronicznej w instytucjach i organach UE generuje dane osobowe, których przetwarzanie skutkuje stosowaniem rozporządzenia 45/2001. Pod koniec 2004 r. 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. Urzędnikom ds. ochrony danych udostępniono projekt dokumentu o e-monitoringu, dotyczącego korzystania z sieci łączności i ich monitorowania, co miało na celu zebranie ich uwag i reakcji.

Te uwagi i reakcje zostały uwzględnione i obecnie włączane są do ostatecznej wersji dokumentu, w którym wzięto także pod uwagę ostatnie wydarzenia w tej

Monitorowanie komunikacji elektronicznej musi się odbywać z poszanowaniem zasad ochrony danych

dziedzinie, takie jak decyzja Europejskiego Trybunału Praw Człowieka, w której uznano, że monitorowanie wykorzystania Internetu przez pracownika stanowi naruszenie praw człowieka ([20]). Zmiana art. 49 przepisów wykonawczych do rozporządzenia finansowego WE, dotyczącego informacji o przesyłaniu danych do celów audytu i przechowywania danych, zostanie również uwzględniona w ostatecznej wersji dokumentu.

Zagadnienia z tej dziedziny pojawiły się również w kontekście innych działań EIOD i omówione zostały w innej części niniejszego sprawozdania (zob. pkt 2.3.4 „Główne zagadnienia w sprawach dotyczących kontroli *ex post*: e-monitoring" oraz pkt 2.7 w odniesieniu do konsultacji w sprawie dokumentów strategicznych dotyczących Internetu).

2.9. Nadzór wideo

W 2007 r. EIOD kontynuował prace nad **wytycznymi w sprawie nadzoru wideo**, aby zapewnić instytucjom i organom UE praktyczną pomoc w zakresie przestrzegania zasad ochrony danych przy wykorzystywaniu systemów nadzoru wideo. Po przeprowadzeniu w 2006 r. ankiety na temat praktyk różnych instytucji i organów wspólnotowych, wiosną 2007 r. EIOD, z pomocą krajowych organów ds. ochrony danych (DPA), przeprowadził międzynarodową ankietę wśród państw członkowskich UE. Ankieta dotyczyła zasad ochrony danych stosowanych wobec praktyk w dziedzinie nadzoru wideo na terytorium UE.

Jednocześnie EIOD nabył dalsze doświadczenia praktyczne w dziedzinie nadzoru wideo wewnątrz instytucji. Kontynuował wspólne prace z Parlamentem Europejskim nad działaniami prowadzonymi w następstwie skargi z 2006 r. dotyczącej praktyk Parlamentu w dziedzinie nadzoru wideo.

EIOD doradzał również w przypadku trzech wniosków o konsultacje związanych z nadzorem wideo, które otrzymał od urzędników ds. ochrony danych z dwóch instytucji. Wszystkie trzy sprawy dotyczyły wykorzystania technologii wideo do celów niezwiązanych z bezpieczeństwem.

Sprawa „centrów informacyjnych" (2006-490) dotyczyła zainstalowania przez jedną z instytucji kamer wideo w jej centrach informacyjnych (obiektach, które oferują odwiedzającym możliwość korzystania z Internetu i komputera). W ramach promowania centrów informacyjnych pochodzące z nich nagrania, w których pokazywano odwiedzających przy stanowiskach komputerowych, były nadawane na żywo na stronach intranetowych tej instytucji. Dodatkowym zamierzonym celem tego działania było ułatwienie pracownikom obsługi monitorowania dostępności stanowisk w centrach informacyjnych. Po przeprowadzeniu analizy proporcjonalności EIOD stwierdził, że takie przetwarzanie danych stanowiło naruszenie prywatności, szczególnie z uwagi na cele, których osiągnięciu miało służyć, i dostępność innych stosownych środków, za pomocą których można było osiągnąć te same cele. EIOD zalecił w związku z tym, by instytucja korzystała z innych metod promowania jej centrów informacyjnych i monitorowania dostępności stanowisk.

Kolejny wniosek o konsultacje w sprawie „stref załadunku" (2006-510) dotyczył proponowanej instalacji kamer w strefach załadunku na parkingach jednej z instytucji, aby móc monitorować dostępność miejsc do celów załadunku i wyładunku. Przekaz miał być udostępniany on-line zespołowi ds. zamówień. W tym przypadku EIOD również zalecił (i) korzystanie z innych metod monitorowania dostępności miejsc lub (ii) umiejscowienie kamer lub ustawienie ich rozdzielczości w taki sposób, by osoby zarejestrowane w nagraniu nie mogły zostać rozpoznane.

Trzecia sprawa („urządzenia wideo w salach konferencyjnych") (2007-132) dotyczyła głównie warunków,

([20]) Sprawa *Copland przeciwko Zjednoczonemu Królestwu*, skarga nr 62617/00.

na jakich należy powiadamiać prelegentów lub uczestników konferencji o tym, że są filmowani i uzyskiwać ich zgodę na takie filmowanie podczas konferencji i innych specjalnych imprez organizowanych na terenie instytucji.

W 2007 r. EIOD otrzymał również od instytucji i organów wspólnotowych liczne powiadomienia w sprawie kontroli wstępnej. Z wyjątkiem planowanych prze OLAF praktyk odnoszących się do telewizji przemysłowej, wszystkie inne powiadomienia dotyczyły spraw kontroli *ex post.*

Komisja, Wspólne Centrum Badawcze w Isprze, Rada oraz Komitet Regionów, wspólnie z Europejskim Komitetem Ekonomiczno-Społecznym, przedłożyły EIOD takie powiadomienia w sprawie kontroli wstępnej *ex post.* Procedura rozpatrywania tych spraw została zawieszona do czasu przyjęcia przez EIOD wytycznych w sprawie nadzoru wideo. EIOD rozpatruje jednak obecnie praktyki OLAF w dziedzinie telewizji przemysłowej, jako sprawę podlegającą faktycznej procedurze kontroli wstępnej.

Na podstawie wyników dwóch wspomnianych ankiet oraz własnych dotychczasowych doświadcze EIOD pod koniec 2007 r. zaczął przygotowywać swój pierwszy przeznaczony do konsultacji projekt wytycznych w sprawie nadzoru wideo. Według planów projekt ten ma zostać ukończony i opublikowany na stronie EIOD wraz z zaproszeniem do przedstawiania uwag przez wszystkie zainteresowane strony. EIOD planuje przyjęcie ostatecznej wersji wytycznych po przeanalizowaniu otrzymanych uwag i wprowadzeniu na ich podstawie dalszych uściśleń i poprawek. Wytyczne skupią się na zagadnieniach istotnych z punktu widzenia praktyk instytucji i organów europejskich, ale będą także opierać się częściowo na krajowych przepisach ustawowych i wykonawczych oraz wytycznych stosowanych w państwach członkowskich UE.

W wytycznych zostaną przedstawione jasne i szczegółowe porady dla mniejszych instytucji i organów ze stosunkowo prostymi systemami nadzoru wideo, które w minimalny sposób naruszają prywatność, co w wielu w przypadkach ograniczy potrzebę przedstawiania EIOD przez ich administratorów operacji przetwarzania danych w celu kontroli wstępnej.

Jednak niektóre bardziej złożone, innowacyjne lub naruszające prywatność systemy, w szczególności

Bezpieczne stosowanie nadzoru wideo wymaga zabezpieczeń w zakresie ochrony danych

systemy nadzoru wideo oparte na nowoczesnych technologiach, pozostaną przedmiotem kontroli wstępnej EIOD. Zgoda będzie przyznawana indywidualnie dla każdego przypadku. Kontrola wstępna, w niektórych przypadkach w skróconej formie, będzie także wymagana, jeżeli administrator, ze względu na szczególne okoliczności danej sprawy, będzie chciał zastosować odstępstwo od jednego lub większej liczby standardowych zaleceń określonych w wytycznych EIOD w sprawie nadzoru wideo.

2.10. 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. Eurodac został utworzony na mocy przepisów szczegółowych, przyjętych na szczeblu europejskim i obejmujących zabezpieczenia w zakresie ochrony danych ([21]).

EIOD nadzoruje przetwarzanie danych osobowych w centralnej bazie danych, którą zarządza jednostka centralna w Komisji, oraz ich przesyłanie do państw

([21]) Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące utworzenia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania konwencji dublińskiej, Dz.U. L 316 z 15.12.2000, s. 1.

członkowskich. Organy ds. ochrony danych w państwach członkowskich nadzorują przetwarzanie danych przez organy krajowe oraz przesyłanie tych danych do jednostki centralnej. Aby zapewnić skoordynowane podejście, EIOD i organy krajowe spotykają się regularnie w celu omówienia wspólnych problemów związanych z funkcjonowaniem Eurodac oraz zalecenia wspólnych rozwiązań. To podejście oparte na „skoordynowanym nadzorze" jak dotąd działa bardzo skutecznie (zob. pkt 4.3).

W 2005 r. EIOD przeprowadził kontrolę sytuacji w zakresie bezpieczeństwa i ochrony danych w jednostce centralnej Eurodac. W swoim sprawozdaniu z lutego 2006 r. EIOD wydał szereg zaleceń w celu udoskonalenia systemu.

Drugim etapem było przeprowadzenie szczegółowego audytu bezpieczeństwa, który rozpoczęto we wrześniu 2006 r. W ramach audytu oceniono, czy wdrażane środki bezpieczeństwa spełniają wymogi określone w obowiązujących przepisach i odpowiadającej im polityce Komisji Europejskiej w zakresie bezpieczeństwa. Oceniono także, czy te środki bezpieczeństwa są nadal zgodne z najlepszymi aktualnymi praktykami. Sprawozdanie końcowe z tego audytu przedstawiono w listopadzie 2007 r.

Zgodnie z porozumieniem między EIOD a Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA), agencja ta umożliwiła kontakty z krajowymi organizacjami eksperckimi i doradzała w sprawie metod przeprowadzenia audytu bezpieczeństwa. W skład zespołu audytorskiego weszli: przedstawiciele EIOD, niemieckiego Federalnego Urzędu Bezpieczeństwa Informacji (BSI) oraz francuskiej Centralnej Dyrekcji Bezpieczeństwa Systemów Informacyjnych (DCSSI). ENISA dokonała przeglądu standardów jakości stosowanych w sprawozdaniu. Chociaż sprawozdanie opatrzone jest klauzulą tajności na poziomie „EU restricted", jego krótkie streszczenie udostępniono na stronie internetowej EIOD ([22]).

EIOD zatwierdził stosowne wnioski i zalecenia. Główny wniosek jest taki, że środki bezpieczeństwa początkowo wdrożone w odniesieniu do Eurodac i sposób ich stosowania w okresie pierwszych czterech lat działalności zapewniają jak dotąd odpowiedni poziom ochrony. Niemniej jednak niektóre elementy systemu i bezpieczeństwo organizacyjne wykazują pewne słabe punkty, które będzie trzeba wyeliminować, aby zapewnić pełną zgodność Eurodac z najlepszymi praktykami oraz wdrożenie najlepszych dostępnych technologii.

EIOD dokona przeglądu wdrażania środków następczych, które zostaną opracowane na podstawie sprawozdania. Oczekuje, że sprawozdanie to zostanie również uwzględnione w systemach VIS, SIS II i innych przyszłych unijnych systemach na dużą skalę.

([22]) Zob. zakładkę „Eurodac" w części „Supervision".

3. Konsultacje

3.1. Wprowadzenie

W 2007 r. EIOD nadal wykonywał swoją funkcję jako doradca w sprawie wniosków dotyczących prawodawstwa UE i innych pokrewnych dokumentów. Funkcja ta została formalnie ustanowiona w art. 28 ust. 2 i art. 41 rozporządzenia (WE) nr 45/2001 (zwane dalej „rozporządzeniem").

Podobnie jak w poprzednich latach działalność konsultacyjna EIOD dotyczyła głównie wpływu wniosków prawodawczych w różnych dziedzinach polityki na poziom ochrony danych. Ta konsultacyjna rola zagwarantowana jest na mocy ogólnych ram prawnych w dziedzinie ochrony danych przyjętych na podstawie Traktatu WE (głównie dyrektywy 95/46/WE) oraz zgodnie z ogólnymi zasadami ochrony danych obowiązującymi na mocy tytułu VI Traktatu UE (tzw. trzeci filar, który jest istotnym obszarem interwencji EIOD).

W większym jednak stopniu niż w latach poprzednich przedmiotem działań EIOD była przyszłość samych ram prawnych w dziedzinie ochrony danych. Po pierwsze, dużej uwagi ze strony EIOD nadal wymagał wniosek dotyczący decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych ([23]). Po drugie, w swojej opinii ([24]) na temat komunikatu Komisji w sprawie wdrażania dyrektywy o ochronie danych ([25]) EIOD wyraził pogląd, że w dłuższej perspektywie zmiany do tej dyrektywy wydają się nieuniknione i zasugerował jak najszybsze przemyślenie przyszłych zmian. Po trzecie, podpisano traktat lizboński mający istotne konsekwencje dla kwestii ochrony danych. Przed finalizacją traktatu EIOD zwrócił uwagę na kilka konkretnych zagadnień, które przedstawił do rozważenia prezydencji portugalskiej.

Ponadto EIOD po raz pierwszy rozważył potrzebę ustanowienia szczegółowych ram prawnych dotyczących ochrony danych w konkretnej dziedzinie (wykorzystania technologii identyfikacji radiowej – RFID), gdyby prawidłowe stosowanie istniejących ogólnych ram prawnych okazało się nieskuteczne. Ta szczególna, całkiem nowa dziedzina może wywrzeć kluczowy wpływ na nasze społeczeństwo i na ochronę w tym społeczeństwie podstawowych praw, takich jak prawo do prywatności i ochrony danych.

Należy także zwrócić uwagę na dwa inne aspekty działalności EIOD w 2007 r.:

- Po raz pierwszy EIOD stwierdził, że nie należy przyjmować instrumentu prawnego zaproponowanego przez Komisję. Konkluzję tę przedstawił w opinii na temat wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (PNR) w celu egzekwowania prawa ([26]).
- Również po raz pierwszy EIOD przedstawił opinię – a właściwie dwie opinie – w sprawie komunikatu Komisji (zob. pkt 3.3.2).

([23]) Wniosek dotyczący decyzji ramowej Rady z dnia 4 października 2005 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (COM(2005) 475 wersja ostateczna).

([24]) Opinia z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych (Dz.U. C 255 z 27.10.2007, s. 1).

([25]) Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 7 marca 2007 r. w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych (COM(2007) 87 wersja ostateczna).

([26]) Opinia z dnia 20 grudnia 2007 r. w sprawie projektu wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa.

Część zespołu konsultantów omawia opinię prawną

W 2007 r. działania EIOD odbywały się w kontekście różnych zmian, których wspólnym mianownikiem był fakt, że wszystkie one przyczyniły się do powstania tzw. społeczeństwa kontrolowanego (*surveillance society*). Mogą one obejmować:

- W dziedzinie wolności, bezpieczeństwa i sprawiedliwości utrzymują się najważniejsze tendencje. Ponownie zaproponowano nowe instrumenty przewidujące stworzenie organom ścigania większych możliwości gromadzenia, przechowywania i wymiany danych osobowych, szczególnie w celu walki z terroryzmem i z przestępczością zorganizowaną.
- Coraz bardziej daje się zauważyć wpływ technologii na prywatność i ochronę danych. Szczególnej uwagi wymagała kwestia zwiększonego wykorzystania danych biometrycznych oraz rozwój technologii identyfikacji radiowej.
- Międzynarodowe przepływy danych zyskują na znaczeniu, nie zawsze jednak można je prześledzić, a w każdym razie nie podlegają one w pełni przepisom UE w dziedzinie ochrony danych, ze względu na ograniczony zakres terytorialny tych przepisów.

Jeżeli chodzi o metody pracy EIOD, 2007 r. był pierwszym rokiem, w którym określono priorytety pracy w publicznie dostępnym dokumencie – spisie na 2007 r. (Inventory 2007) – który opublikowano na stronie internetowej EIOD w grudniu 2006 r.

W porównaniu z 2006 r. wydajność EIOD, mierzona liczbą wydanych opinii, minimalnie wzrosła: w 2007 r. wydano 12 opinii; w 2006 r. – 11. EIOD w większym stopniu wykorzystywał inne narzędzia interwencji, takie jak uwagi (które są również publikowane na stronie internetowej, ale nie w Dzienniku Urzędowym Unii Europejskiej). Takiego wyboru narzędzi nie należy postrzegać jako strukturalnej zmiany w podejściu.

Na koniec należy dodać, że oprócz analizy działań przeprowadzonych w 2007 r. – w niniejszym rozdziale opisano też perspektywy na przyszłość związane z rozwojem technologii oraz prawodawstwa.

3.2. Ramy polityki i priorytety

Dokument strategiczny zatytułowany „EIOD jako doradca instytucji wspólnotowych w zakresie wniosków prawodawczych i dokumentów pokrewnych” ([27]) wytycza główne kierunki działań EIOD w dziedzinie konsultacji.

Dokument ten zawiera trzy elementy: zakres zadań doradczych EIOD, treść interwencji oraz podejście i metody pracy. Dokument strategiczny, wydany w marcu 2005 r., okazał się solidną podstawą działalności EIOD.

Podstawa ta została rozwinięta i udoskonalona w 2007 r. EIOD sprecyzował, że celem jego udziału w procesie prawodawczym UE jest aktywne propagowanie podejmowania środków prawodawczych wyłącznie po należytym uwzględnieniu wpływu takich środków na prywatność i ochronę danych. Oceny skutków regulacji dokonywane przez Komisję muszą w odpowiedni sposób uwzględniać prywatność i ochronę danych. Ponadto decyzje muszą być zawsze przyjmowane ze świadomością ich wpływu na ochronę danych.

Asystent EIOD ds. badań rozpoczął także przygotowywanie sprawozdania w sprawie wspólnych kierunków i zasad opracowywanych przez EIOD w ramach jego działalności konsultacyjnej w dziedzinie bezpieczeństwa, wolności i sprawiedliwości. Sprawozdanie to należy uważać za kolejny krok w propagowaniu spój-

([27]) Dostępny na stronie internetowej EIOD w części „Consultation”.

nego podejścia oraz za zasadniczy element zwiększania skuteczności. Na tym etapie EIOD skoncentrował się na dość ograniczonej tematyce – wolności, bezpieczeństwa i sprawiedliwości – ale w dłuższej perspektywie można rozważyć podobną inicjatywę obejmującą cały obszar działalności EIOD. Prace nad sprawozdaniem zostaną zakończone na początku 2008 r.

Jeżeli chodzi o podejście i metody pracy, 2007 r. okazał się rokiem konsolidacji. Konsultacje z EIOD, które obejmują działania na różnych etapach procedury prawodawczej, stały się zwykłą częścią tej procedury, oczywiście pod warunkiem, że dane wnioski mają lub mogą mieć wpływ na ochronę danych.

Spis

Coroczny spis należy uważać za dodatkową część ram polityki EIOD. Spis składa się z dwóch części:

- wprowadzenie, w którym przedstawiono krótką analizę kontekstu i wyszczególniono priorytety na dany rok;
- załącznik zawierający wykaz odnośnych wniosków Komisji (i związanych z nimi dokumentów), które mogą wymagać reakcji ze strony EIOD; głównym źródłem załącznika jest program działalności legislacyjnej i prac Komisji.

W spisie na 2007 r. wymieniono osiem priorytetów EIOD. Ogólnie mówiąc, EIOD działał zgodnie z wyznaczonymi priorytetami. Po dokładniejszej analizie poszczególnych priorytetów można wyciągnąć poniższe wnioski.

W załączniku do spisu na 2007 r. wymieniono 16 ważnych dokumentów (oznaczonych jako „czerwone"), w sprawie których EIOD zamierzał wydać opinię. Osiągnięto następujące wyniki:

Wydane opinie	**8 dokumentów**
Brak opinii EIOD, ale poparcie dla opinii Grupy Roboczej Art. 29	1 dokument (dane PNR – umowa z USA)
Opinie EIOD przełożone na 2008 r.	2 dokumenty
Wniosek Komisji przełożony na 2008 r.	5 dokumentów

Ponadto wykaz zawierał 22 dokumenty o mniejszym znaczeniu dla EIOD, w sprawie których EIOD zamierzał wydać ewentualnie opinię, zareagować w inny

Priorytet 1: Przechowywanie i wymiana informacji w obszarze wolności, bezpieczeństwa i sprawiedliwości ponownie stanowiły trzon działalności EIOD w 2007 r. (i pozostaną nim tak długo, jak długo prawodawca UE będzie kładł nacisk na nowe instrumenty prawne lub modyfikację instrumentów istniejących w tym obszarze).

Priorytet 2: W związku z komunikatem Komisji w sprawie przyszłości dyrektywy 95/46/WE EIOD wydał obszerną opinię, w której wystąpił o podjęcie rozważań na temat przyszłych zmian.

Priorytet 3: Ściśle śledzono i komentowano zmiany, które miały miejsce w dziedzinie „społeczeństwa informacyjnego". Wspomniano o technologii RFID; EIOD brał udział w zmianie dyrektywy 2002/58/WE (opinia zostanie wydana na początku 2008 r.).

Priorytet 4: Jeśli chodzi o priorytet obejmujący „zdrowie publiczne" jako kluczowy obszar działania EIOD, nie poczyniono zbyt wielkich postępów, głównie ze względu na fakt, że w 2007 r. nie przyjęto istotnych wniosków legislacyjnych. Temat ten pozostanie priorytetem w 2008 r.

Priorytet 5: Prowadzono wiele działań związanych z dziedziną OLAF. Szczególną uwagę zwrócono na wymianę danych osobowych z Europolem (jest o tym mowa w opinii EIOD na temat decyzji w sprawie Europolu) oraz wymianę danych z państwami trzecimi. Istnieje wyraźny związek z nadzorem EIOD nad przetwarzaniem danych przez OLAF.

Priorytet 6: Jeśli chodzi o przejrzystość, działalność doradczą odsunięto w czasie w związku z oczekiwaniem na wyrok Sądu Pierwszej Instancji w sprawie Bavarian Lager (wydany w dniu 8 listopada 2007 r.) Wniosek w sprawie zmiany rozporządzenia (WE) nr 1049/2001 przewidziany jest na wiosnę 2008 r.

Priorytet 7 i 8: Tematy horyzontalne i inne działania (dotyczące metod pracy): poczyniono istotne postępy.

sposób lub jedynie uważnie śledzić rozwój wydarzeń w tej dziedzinie.

Sytuacja na koniec 2007 r. wygląda inaczej:

Stały obszar zainteresowań EIOD (programy badawcze, kwestie ogólne, tematy, takie jak imigracja lub zdrowie publiczne)	8 dokumentów
Interwencje EIOD w 2007 r. (uwagi lub działania nieformalne)	4 dokumenty (spam, cyberprzestępczość, terroryzm, partnerstwo publiczno-prywatne)
Skreślone z wykazu bez dalszych działań EIOD	5 dokumentów
Działania Komisji przełożone na 2008 r.	2 dokumenty
Status podwyższony do „czerwonego" w spisie na 2008 r.	3 dokumenty

Spis na 2008 r.

W grudniu 2007 r. na stronie internetowej opublikowano spis na 2008 r. (druga edycja rocznego spisu). Jest on zasadniczo analogiczny do spisu na 2007 r. Priorytety zostały nieco inaczej uszeregowane: w spisie na 2008 r. wymieniono tylko **sześć priorytetów**, z czego dwa są nowe. W 2008 r. priorytetowo zostaną również potraktowane przygotowania do wejścia w życie traktatu lizbońskiego, a także zewnętrzne aspekty ochrony danych związane z przekazywaniem danych do państw trzecich.

Załącznik do spisu świadczy o tym, że zakres działalności EIOD obejmuje obecnie wiele obszarów polityki. Wymienione w nim wnioski odnoszą się do 13 różnych służb Komisji (ADMIN, EMPL, ENT, ESTAT, INFSO, JLS, MARKT, OLAF, RELEX, SANCO, SG, TAXUD, TREN).

Zwiększyła się również łączna liczba wniosków wymienionych w załączniku. Obecnie w załączniku figuruje 67 tematów podzielonych w następujący sposób:

- 34 tematy zaznaczono jako „czerwone" – o wysokim priorytecie; 33 tematy oznaczono jako „żółte" – obejmujące dokumenty o mniejszym znaczeniu dla EIOD oraz dokumenty, na które EIOD zamierza ewentualnie zareagować;
- 29 tematów można określić mianem wniosków prawodawczych *sensu stricto* (dotyczących rozporządzeń, dyrektyw, decyzji i decyzji ramowych); pozostałe 38 tematów to dokumenty niebędące dokumentami prawodawczymi; należą do nich komunikaty Komisji, zalecenia, programy pracy oraz dokumenty dotyczące umów między UE a państwami trzecimi.

Wzrost liczby wniosków wymienionych w załączniku wynika częściowo z tego, że załącznik oparty jest na programie działalności legislacyjnej i prac Komisji, w którym blisko ze sobą powiązane tematy stanowią odrębne pozycje. Fakt, że 34 tematom przyznano status „czerwonych", nie oznacza, iż liczba opinii EIOD odpowiednio wzrośnie.

3.3. Opinie prawne

3.3.1. Uwagi ogólne

Opinie na temat zagadnień z trzeciego filara

W 2007 r. EIOD przyjął 12 opinii prawodawczych. Podobnie jak w poprzednich latach duża część opinii dotyczy przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Dziedzina ta stanowi obecnie nieco poniżej 50% wszystkich opinii prawodawczych (dokładnie 5 z 12). Wszystkie 5 opinii dotyczyło dokumentów w dziedzinie współpracy policyjnej i sądowej w sprawach karnych (tzw. trzeci filar) i obejmowało fundamentalne zmiany, także z perspektywy ochrony danych. Było tak przede wszystkim w przypadku trzeciej opinii na temat wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Pozostałe opinie dotyczą wniosku w sprawie decyzji dotyczącej Europolu, dwóch inicjatyw w dziedzinie współpracy transgranicznej (dokonujących transpozycji konwencji z Prüm i jej porozumienia wykonawczego na poziomie UE) oraz wniosku dotyczącego europejskiego systemu danych dotyczących przelotu pasażera (PNR).

W ramach trzeciego filara jedną z głównych kwestii było przyjęcie – bez właściwej oceny skuteczności obowiązujących instrumentów prawnych – nowych wniosków ułatwiających przechowywanie informacji przez organy ścigania oraz wymianę informacji między tymi organami. Nowe instrumenty opracowano przed

właściwym wprowadzeniem w życie instrumentów już istniejących. Kwestia ta miała szczególne znaczenie w związku z transpozycją konwencji z Prüm do ram prawnych UE oraz w odniesieniu do systemu danych dotyczących przelotu pasażera.

Brak kompleksowych ram prawnych w zakresie ochrony danych był kolejną kwestią, której EIOD poświęcił szczególną uwagę w swoich opiniach związanych z trzecim filarem. Większość wniosków zawiera pewne przepisy szczególne z zakresu ochrony danych, których celem jest stworzenie ogólnych ram. Jednak nie opracowano jeszcze zadowalających ram prawnych.

Trzecim problemem jest fakt, że zgodnie z przepisami UE do wykonania pewnych zadań państwa członkowskie obowiązkowo ustanawiają krajowe organy, pozostawiając im jednak dużą swobodę w formułowaniu warunków swojego funkcjonowania. Zakłóca to wymianę informacji między państwami członkowskimi i ma wpływ na pewność prawną podmiotu danych, które są przekazywane między organami różnych państw członkowskich.

Wymiana informacji z państwami trzecimi do celów egzekwowania prawa stanowiła osobną kwestię, którą EIOD poruszył w różnych opiniach. EIOD wyraził zaniepokojenie brakiem harmonizacji oraz brakiem gwarancji dotyczących przetwarzania przez państwa trzecie danych osobowych po ich przekazaniu.

Opinie na temat komunikatów

Wydano dwie opinie dotyczące ważnych komunikatów Komisji w sprawie przyszłych ram ochrony danych. W opinii na temat wdrażania dyrektywy o ochronie danych ([28]) EIOD określił pięć perspektyw zmieniającej się sytuacji; jedną z nich są interakcje z technologią. Nowe osiągnięcia technologiczne mają wyraźny wpływ na określanie wymagań dotyczących skutecznych ram prawnych ochrony danych. Ważnym osiągnięciem technologicznym jest technologia identyfikacji radiowej (RFID), która stanowi przedmiot osobnej opinii EIOD ([29]).

([28]) Opinia z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, Dz.U. C 255 z 27.10.2007, s. 1.

([29]) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie identyfikacji radiowej (RFID) w Europie: w stronę ram polityki (COM(2007) 96).

Dwie opinie wydane w sprawie komunikatów Komisji dały EIOD sposobność do zastanowienia się nad przyszłymi perspektywami ochrony danych oraz nadania dynamiki dyskusjom na temat ram ochrony danych w najbliższej przyszłości; potrzeba prowadzenia takich dyskusji jest coraz pilniejsza (zob. pkt 3.7 w sprawie rozwoju sytuacji w przyszłości).

Opinie na temat prawodawstwa z pierwszego filara

Pozostałe pięć opinii wydanych przez EIOD w 2007 r. miało różnorodny charakter i dotyczyło takich obszarów polityki, jak cła, statystyki, transport drogowy, rolnictwo i zabezpieczenia społeczne. Głównym wspólnym mianownikiem jest to, że trzy spośród tych pięciu opinii dotyczą wniosków, które mają ułatwić wymianę danych między organami państw członkowskich (w dziedzinie ceł, transportu drogowego i zabezpieczeń społecznych). Inne omawiane kwestie dotyczyły ujawniania informacji o beneficjentach środków finansowych Wspólnoty, pojęcia poufności danych statystycznych oraz związku przepisów szczegółowych z ogólnymi ramami w dziedzinie ochrony danych.

Wnioski odzwierciedlają bardziej ogólną tendencję. Wymiana informacji między państwami członkowskimi – w tym wymiana danych osobowych – postrzegana jest jako istotne narzędzie rozwoju rynku wewnętrznego. Ułatwianie wymiany informacji, przez pełne wykorzystanie możliwości sieci elektronicznych, może przyczynić się do usunięcia barier. W niektórych przypadkach Komisja określana jest jako organ odpowiedzialny za utrzymywanie i zapewnianie dostępu do infrastruktury technicznej. W tych przypadkach EIOD pełni także funkcję organu nadzorczego.

Ogólnie rzecz biorąc, EIOD powinien zwrócić szczególną uwagę na tę tendencję, aby dopilnować, by w instrumentach ułatwiających wymianę danych osobowych uwzględniano niezbędne zabezpieczenia i gwarancje dla podmiotu danych. W tym względzie kwestią zasadniczą jest także to, by podmiot danych mógł korzystać ze swoich praw w prosty i praktyczny sposób.

3.3.2. Poszczególne opinie

Europejski Urząd Policji (Europol)

Europol powstał w 1995 r. na mocy konwencji zawartej przez państwa członkowskie. Wadą tej konwencji,

z punktu widzenia elastyczności i skuteczności, jest wymóg ratyfikacji wszelkich zmian przez wszystkie państwa członkowskie, wskutek czego proces wprowadzania zmian – jak pokazały doświadczenia z przeszłości – może potrwać i kilka lat.

Celem wniosku dotyczącego decyzji Rady zmieniającej konwencję ([30]), w sprawie którego EIOD wydał opinię 16 lutego 2007 r. ([31]), nie jest zasadnicza zmiana mandatu lub zakresu działalności Europolu, ale przede wszystkim zapewnienie Europolowi nowej i bardziej elastycznej podstawy prawnej. Wniosek zawiera również istotne zmiany, mające usprawnić funkcjonowanie Europolu w przyszłości. Rozszerza on mandat Europolu i zawiera kilka nowych przepisów, zmierzających do usprawnienia funkcjonowania Europolu, na przykład w odniesieniu do wymiany danych między Europolem a innymi organami WE/UE, takimi jak OLAF. Wniosek zawiera również szczegółowe przepisy dotyczące ochrony i bezpieczeństwa danych, uzupełniające ogólne ramy prawne w zakresie ochrony danych w ramach trzeciego filara, których jeszcze nie przyjęto.

W swojej opinii EIOD stwierdza, że decyzji Rady nie należy przyjmować przed przyjęciem ram w dziedzinie ochrony danych, gwarantujących odpowiedni poziom ochrony danych.

Ponadto zasugerował pewne ulepszenia, takie jak:
- zapewnienie rzetelności danych gromadzonych w dziedzinie działalności handlowej;
- stosowanie rygorystycznych warunków i gwarancji w przypadku wzajemnych połączeń baz danych;
- harmonizacja przepisów dotyczących prawa podmiotu danych do dostępu do jego danych oraz ograniczenie wyjątków od tego prawa;
- dodanie zapisów gwarantujących niezależność urzędnika ds. ochrony danych Europolu (który czuwa nad prawidłowym przetwarzaniem danych osobowych w tej instytucji);
- zapewnienie nadzoru EIOD nad przetwarzaniem danych dotyczących personelu Europolu.

([30]) Wniosek z dnia 20 grudnia 2006 r. dotyczący decyzji Rady ustanawiającej Europejski Urząd Policji (Europol) (COM(2006) 817 wersja ostateczna).

([31]) Opinia z dnia 16 lutego 2007 r. w sprawie wniosku dotyczącego decyzji Rady ustanawiającej Europejski Urząd Policji (Europol) (COM(2006) 817 wersja ostateczna), Dz.U. C 255 z 27.10.2007, s. 13.

Prawidłowe stosowanie przepisów prawa celnego i rolnego

Dnia 22 lutego 2007 r. EIOD wydał opinię w sprawie wniosku Komisji dotyczącego rozporządzenia, które przewiduje stworzenie lub aktualizację różnych systemów informatycznych zawierających dane osobowe. Celem tego wniosku jest wzmocnienie współpracy państw członkowskich i Komisji nad unikaniem naruszeń prawodawstwa w dziedzinie ceł i rolnictwa ([32]). Systemy informatyczne obejmują europejski katalog danych, System Informacji Celnej (SIC) i bazę danych identyfikacyjnych rejestru celnego (FIDE).

W swojej opinii EIOD ([33]) sugeruje wprowadzenie do wniosku pewnych zmian, które mają zapewnić jego ogólną zgodność z obowiązującymi ramami prawnymi w dziedzinie ochrony danych oraz skuteczną ochronę danych osobowych. EIOD zasugerował między innymi:
- przeprowadzenie przez Komisję odpowiedniej oceny dotyczącej potrzeby stworzenia europejskiego katalogu danych;
- w przypadku utworzenia europejskiego katalogu danych – umieszczenie w rozporządzeniu przepisów przewidujących przyjęcie uzupełniających przepisów administracyjnych, w których określone zostaną konkretne środki zapewniające poufność informacji;
- zmianę różnych przepisów tak, by uznać nadzorczą rolę EIOD względem SIC i FIDE;
- stworzenie skoordynowanego podejścia do nadzoru nad SIC, w którym uczestniczyłyby organy krajowe i EIOD.

Koordynacja systemów zabezpieczenia społecznego

Dnia 6 marca 2007 r. EIOD wydał opinię na temat wniosku Komisji w sprawie przepisów wykonawczych

([32]) Wniosek z dnia 22 grudnia 2006 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 515/97 w sprawie wzajemnej pomocy między organami administracyjnymi państw członkowskich i współpracy między państwami członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego (COM(2006) 866 wersja ostateczna).

([33]) Opinia z dnia 22 lutego 2007 r. w sprawie wniosku dotyczącego rozporządzenia zmieniającego rozporządzenie Rady (WE) nr 515/97 w sprawie wzajemnej pomocy między organami administracyjnymi państw członkowskich i współpracy między państwami członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego (COM(2006) 866 wersja ostateczna), Dz.U. C 94 z 28.4.2007, s. 3.

w zakresie koordynacji systemów zabezpieczenia społecznego. Wniosek obejmuje szeroki zakres dziedzin zabezpieczenia społecznego (emerytury, świadczenia z tytułu macierzyństwa, renty, świadczenia dla bezrobotnych itp.) ([34]). Jego celem jest unowocześnienie i uproszczenie obowiązujących przepisów przez wzmocnienie współpracy i ulepszenie metod wymiany danych między instytucjami zabezpieczenia społecznego w różnych państwach członkowskich.

EIOD z zadowoleniem przyjął wniosek w zakresie, w jakim sprzyja on swobodnemu przepływowi obywateli oraz poprawie poziomu życia i warunków zatrudnienia obywateli przemieszczających się wewnątrz Unii ([35]). Chociaż prawdą jest, że zabezpieczenia społeczne nie mogłyby istnieć bez wymiany różnego rodzaju danych osobowych, równie rzeczywista jest potrzeba zapewnienia wysokiego poziomu ochrony tych danych. Mając to na uwadze, EIOD zalecił, by:

- przywiązywać najwyższą wagę do podstawowych zasad ochrony danych, takich jak ograniczenie celu oraz proporcjonalność przetwarzanych danych, podmioty upoważnione do przetwarzania danych i okresy przechowywania;
- dbać, by każdy proponowany mechanizm przechowywania i przesyłania danych osobowych miał jasno określone podstawy prawne;
- dostarczać zainteresowanym osobom odpowiednich informacji dotyczących przetwarzania ich danych osobowych;
- pozwolić podmiotom danych na skuteczne korzystanie z ich praw w kontekście transgranicznym.

Współpraca transgraniczna (konwencja z Prüm)

Dnia 4 kwietnia 2007 r. EIOD przedstawił opinię w sprawie inicjatywy 15 państw członkowskich na rzecz objęcia konwencją z Prüm całego terytorium UE, chociaż nie został poproszony o konsultacje w sprawie tego wniosku ([36]).

([34]) Wniosek z dnia 31 stycznia 2006 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie wykonywania rozporządzenia (WE) nr 883/2004 w sprawie koordynacji systemów zabezpieczenia społecznego (COM(2006) 16 wersja ostateczna).

([35]) Opinia z dnia 6 marca 2007 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie wykonywania rozporządzenia (WE) nr 883/2004 w sprawie koordynacji systemów zabezpieczenia społecznego (COM(2006) 16 wersja ostateczna), Dz.U. C 91 z 26.4.2007, s. 15.

([36]) Opinia z dnia 4 kwietnia 2007 r. na temat inicjatywy 15 państw członkowskich w celu przyjęcia decyzji Rady w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną, Dz.U. C 169 z 21.7.2007, s. 2.

Decyzja dotycząca konwencji z Prüm przewiduje korzystanie z DNA

Celem inicjatywy jest intensyfikacja współpracy transgranicznej, szczególnie w celu walki z terroryzmem i przestępczością transgraniczną. Inicjatywa dotyczy wymiany danych biometrycznych (danych o DNA i odciskach palców) i zobowiązuje państwa członkowskie do utworzenia baz danych DNA ([37]).

Chociaż ochrona danych odgrywa istotną rolę w tej inicjatywie, jej postanowienia mają stanowić zasady szczegółowe wobec ogólnych ram w dziedzinie ochrony danych, których jeszcze nie przyjęto. Takie ramy są potrzebne, aby zapewnić obywatelom wystarczający poziom ochrony, gdyż decyzja ta znacznie ułatwi wymianę danych o DNA i odciskach palców.

Ponieważ konwencja z Prüm weszła już w życie w niektórych państwach członkowskich, sugestie EIOD służą głównie poprawieniu tekstu bez zmiany samego systemu wymiany informacji. Odnotowuje on zwłaszcza, że:

- podejście do różnych rodzajów danych osobowych jest właściwe: im większej ochrony dane wymagają, tym węższy jest zakres celów, w których mogą być wykorzystywane, i tym bardziej ograniczony jest dostęp do nich;
- podczas przyjmowania przepisów Rada powinna uwzględnić ocenę skutków regulacji i klauzulę dotyczącą oceny; ostrzegł, że system opracowany dla niewielkiej liczby ściśle współpracujących państw członkowskich nie musi wcale właściwie funkcjonować w skali ogólnoeuropejskiej;

([37]) Inicjatywa z Prüm, Dz.U. C 71 z 28.3.2007, s. 35.

- w inicjatywie nie wskazano kategorii osób, których dane zostaną ujęte w bazach danych DNA, i nie ograniczono w niej okresu przechowywania danych.

Finansowanie wspólnej polityki rolnej

Analizowany wniosek ma na celu spełnienie wymogu publikowania informacji na temat beneficjentów funduszy wspólnotowych. W ramach realizacji europejskiej inicjatywy na rzecz przejrzystości rozporządzenie Rady (WE, Euratom) nr 1995/2006 z dnia 13 grudnia 2006 r. ([38]), które także było przedmiotem opinii EIOD, wprowadziło ten wymóg do rozporządzenia finansowego.

Główny aspekt przeanalizowany przez EIOD w jego opinii z dnia 10 kwietnia 2007 r. dotyczy faktu, że państwa członkowskie powinny zapewnić coroczną publikację *ex post* beneficjentów funduszy europejskich oraz kwot otrzymanych przez każdego beneficjenta z tych funduszy, które należą do budżetu Wspólnot Europejskich.

W swojej opinii EIOD poparł wprowadzenie zasady przejrzystości do prawodawstwa i podkreślił, że należy przestrzegać aktywnego podejścia do praw podmiotów danych. Ponadto, to aktywne podejście mogłoby polegać na wcześniejszym informowaniu podmiotów danych, w momencie gromadzenia ich danych osobowych, że dane te zostaną podane do wiadomości publicznej, oraz na zapewnieniu poszanowania prawa podmiotu danych do dostępu do jego danych oraz jego prawa do sprzeciwu.

Ponadto EIOD proponuje wprowadzenie przepisu szczegółowego, który ułatwi przestrzeganie art. 12 rozporządzenia (WE) nr 45/2001. Celem tej zmiany jest informowanie podmiotów danych o przetwarzaniu ich danych osobowych przez instytucje i organy odpowiedzialne za audyt i kontrolę.

Ochrona danych w trzecim filarze (trzecia opinia EIOD)

Dnia 20 kwietnia 2007 r. prezydencja niemiecka skonsultowała się z Parlamentem Europejskim w sprawie zmienionego wniosku dotyczącego decyzji ramowej Rady ([39]). Celem tej zmiany było przyspieszenie negocjacji w Radzie oraz poprawienie ochrony danych w trzecim filarze. EIOD stwierdził, że zmiany merytoryczne zawarte w zmienionym wniosku, jak i znaczenie samego wniosku, wymagały nowej opinii, która została wydana 27 kwietnia 2007 r. ([40]). W swoich dwóch wcześniejszych opiniach na ten temat EIOD podkreślił potrzebę ogólnych ram ochrony danych w dziedzinie wolności, bezpieczeństwa i sprawiedliwości, w której ściślejsza współpraca policyjna i sądowa nabiera coraz większego znaczenia.

W swojej trzeciej opinii EIOD zajmuje krytyczne stanowisko i zaleca, by nie przyjmować decyzji ramowej bez wprowadzenia istotnych poprawek, szczególnie w odniesieniu do następujących kwestii:

- objęcie zakresem zastosowania decyzji także krajowego przetwarzania danych, tak by dane obywateli były odpowiednio chronione nie tylko wtedy, gdy są wymieniane z innym państwem członkowskim;
- ograniczenie celów, w których dane osobowe mogą być dalej przetwarzane, aby uniknąć sprzeczności z podstawowymi zasadami konwencji nr 108 Rady Europy;
- wymóg odpowiedniego poziomu ochrony w przypadku wymiany danych z państwami trzecimi, zgodnie ze wspólnym standardem UE;
- zapewnienie jakości danych przez rozróżnienie danych faktycznych i tzw. miękkich danych, jak również rozróżnienie kategorii osób, takich jak świadkowie, osoby skazane itd.

Ponadto EIOD zalecił Radzie, by nie negocjowała w sprawie nowych kwestii poruszonych we wniosku – rozszerzenia jego zakresu na przetwarzanie danych z trzeciego filaru przez Europol i Eurojust oraz utworzenia nowego wspólnego organu nadzorczego – z obawy, że niektóre inne istotne elementy wniosku nie zostałyby w wystarczający sposób uwzględnione.

Komunikat w sprawie wdrażania dyrektywy o ochronie danych

Komunikat Komisji w sprawie wdrażania dyrektywy o ochronie danych potwierdza znaczenie dyrektywy 95/46/WE jako kamienia milowego w dziedzinie

([38]) Rozporządzenie Rady (WE, Euratom) nr 1995/2006 z dnia 13 grudnia 2006 r. zmieniające rozporządzenie (WE, Euratom) nr 1605/2002 w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich, Dz.U. L 390 z 30.12.2006, s. 1–26.

([39]) Dokument Rady nr 7315/07 z dnia 13 marca 2007 r.

([40]) Trzecia opinia z dnia 27 kwietnia 2007 r. w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. C 139 z 23.6.2007, s. 1.

ochrony danych osobowych i omawia dyrektywę oraz jej stosowanie ([41]). Głównym przesłaniem komunikatu jest to, że dyrektywy nie należy zmieniać. Należy dalej usprawniać jej wdrażanie za pomocą innych narzędzi politycznych, głównie o charakterze niewiążącym prawnie.

Opinia EIOD z 25 lipca 2007 r. popiera główny wniosek przedstawiony w komunikacie Komisji. Według niego, w krótkim okresie najlepiej nakierować działania na usprawnienie wdrażania dyrektywy ([42]). Jednak w dalszej perspektywie zmiany w dyrektywie wydają się nieuchronne. EIOD zwraca się o określenie już teraz konkretnego terminu przeglądu, aby przygotować propozycje dotyczące zmian. Taki termin byłby wyraźnym bodźcem do rozpoczęcia refleksji nad przyszłymi zmianami. Przyszłe zmiany nie oznaczają konieczności ustalenia nowych zasad, ale raczej oczywistą potrzebę wprowadzenia innych rozwiązań administracyjnych.

W opinii wyróżniono pięć perspektyw przyszłych zmian: pełne wdrożenie dyrektywy, interakcje z technologią, globalne zagadnienia dotyczące prywatności i jurysdykcji, egzekwowanie prawa oraz skutki traktatu lizbońskiego.

Jeśli chodzi o perspektywę pełnego wdrożenia, EIOD wzywa Komisję do rozważenia zestawu zaleceń, które obejmowałyby:

- w niektórych przypadkach – konieczne konkretne działania prawodawcze na poziomie UE;
- dążenie do lepszego wdrażania dyrektywy przez prowadzenie postępowań o naruszenie przepisów;
- wykorzystanie komunikatu wyjaśniającego do omówienia następujących kwestii: pojęcia danych osobowych, definicji roli administratora danych lub przetwarzającego dane, określenia prawa właściwego, zasady ograniczenia celu i niezgodnego z nią wykorzystania danych, podstawy prawnej przetwarzania danych, szczególnie w odniesieniu do jednoznacznego wyrażenia zgody oraz do wyważenia interesów;
- powszechne stosowanie niewiążących prawnie instrumentów, w tym instrumentów zasadzających się na pojęciu „wbudowanej" prywatności i poszanowania prywatności od samego początku *(privacy by design);*
- przedłożenie Grupie Roboczej Art. 29 dokumentu, który zawierałby jasne wskazówki co do podziału ról między Komisję a grupę roboczą.

Statystyki Wspólnoty w zakresie zdrowia

Dnia 5 września 2007 r. EIOD przyjął opinię w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz bezpieczeństwa i higieny pracy ([43]).

Wniosek ma na celu ustanowienie ram dla wszystkich obecnych i przewidywalnych działań w dziedzinie statystyk zdrowia publicznego oraz bezpieczeństwa i higieny pracy, które są prowadzone są przez Eurostat, krajowe urzędy statystyczne oraz inne organy krajowe odpowiedzialne za dostarczanie statystyki publicznej w tych dziedzinach.

Główne zalecenia EIOD odnosiły się do potrzeby zajęcia się różnicami między ochroną danych a poufnością w statystyce, szczególnie pojęciami, które są specyficzne dla każdego z obszarów. Ponadto przeanalizowano kwestię przekazywania danych osobowych do państw trzecich oraz okresów przechowywania danych statystycznych.

Po dyskusjach, które odbyły się między służbami Eurostatu i EIOD, zdecydowano, że zostanie przeprowadzony wspólny przegląd procesów uruchomionych w Eurostacie służących do obsługi indywidualnych danych do celów statystycznych oraz że przegląd ten może spowodować potrzebę przeprowadzenia kontroli wstępnej.

Przewoźnicy drogowi

Dnia 12 września 2007 r. EIOD wydał opinię na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie wspólnych zasad dotyczących warunków wykonywania zawodu przewoźnika drogowego ([44]).

([41]) Komunikat Komisji z dnia 7 marca 2007 r. do Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych (COM(2007) 87 wersja ostateczna).

([42]) Opinia z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, Dz.U. C 255 z 27.10.2007, s. 1.

([43]) Opinia z dnia 5 września 2007 r. na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz bezpieczeństwa i higieny pracy (COM(2007) 46 wersja ostateczna), Dz.U. C 295 z 7.12.2007, s. 1.

([44]) Opinia z dnia 12 września 2007 r. w sprawie wniosku dotyczącego rozporządzenia w sprawie wspólnych zasad dotyczących warunków wykonywania zawodu przewoźnika drogowego, Dz.U. C 14 z 19.1.2008, s. 1.

Rozporządzenie ustanawia warunki dotyczące dobrej reputacji, zdolności finansowej i kwalifikacji zawodowych, które to warunki muszą spełnić przedsiębiorstwa transportu drogowego. Wniosek wprowadza wymóg stworzenia we wszystkich państwach członkowskich krajowych rejestrów elektronicznych ułatwiających wymianę informacji pomiędzy państwami członkowskimi oraz wzajemnego ich połączenia. Zawiera także szczegółowy przepis dotyczący ochrony danych ([45]).

EIOD zalecił zmianę proponowanego rozporządzania w taki sposób, by:
- lepiej zdefiniować takie terminy, jak „dobra reputacja";
- jednoznacznie określić rolę organów krajowych;
- zapewnić spełnienie wymogów dyrektywy 95/46/WE.

Przepisy wykonawcze inicjatywy z Prüm

Dnia 19 grudnia 2007 r. EIOD przedstawił opinię na temat inicjatywy Niemiec dotyczącej ustanowienia przepisów wykonawczych niezbędnych do stosowania decyzji Rady w sprawie konwencji z Prüm ([46]) (EIOD wydał już opinię na temat inicjatywy dotyczącej tej decyzji 4 kwietnia 2007 r.).

Przepisy wykonawcze i załącznik do nich mają szczególne znaczenie, ponieważ określają kluczowe aspekty i narzędzia wymiany danych, które są niezbędne do zapewnienia gwarancji zainteresowanym osobom. Ponadto obecny brak ogólnych ram UE, które zagwarantowałyby zharmonizowaną ochronę danych w sektorze egzekwowania prawa, wymaga zwrócenia szczególnej uwagi na te przepisy.

W swojej opinii EIOD zaleca zwłaszcza:
- połączenie przepisów ogólnych ze szczególnymi, zindywidualizowanymi przepisami w zakresie ochrony danych, co powinno zapewnić zarówno prawa obywateli, jak i skuteczność organów ścigania po wejściu w życie wniosku;
- należyte uwzględnianie i stałe monitorowanie rzetelności w wyszukiwaniu i porównywaniu profilów DNA i odcisków palców, także w świetle większej skali wymiany tych danych;
- stworzenie organom ds. ochrony danych warunków do prawidłowego pełnienia ich funkcji nadzorczych i doradczych na różnych etapach wdrażania.

Komunikat w sprawie identyfikacji radiowej (RFID)

Dnia 20 grudnia 2007 r. EIOD wydał opinię na temat komunikatu Komisji w sprawie identyfikacji radiowej (RFID) ([47]) w Europie, który opublikowano w marcu 2007 r. W opinii poruszono kwestię coraz częstszego stosowania czipów RFID w produktach konsumenckich i innych nowych zastosowań mających wpływ na osoby fizyczne.

EIOD przyjmuje do wiadomości komunikat Komisji w sprawie RFID, ponieważ porusza on główne zagadnienia wynikające z zastosowania tej technologii, uwzględniając jednocześnie aspekty związane z prywatnością i ochroną danych. EIOD zgadza się z Komisją, że w pierwszej fazie działań należy umożliwić stosowanie instrumentów samoregulacyjnych. Dodatkowe środki prawodawcze mogą jednak okazać się konieczne, aby uregulować korzystanie z RFID pod względem ochrony prywatności i ochrony danych.

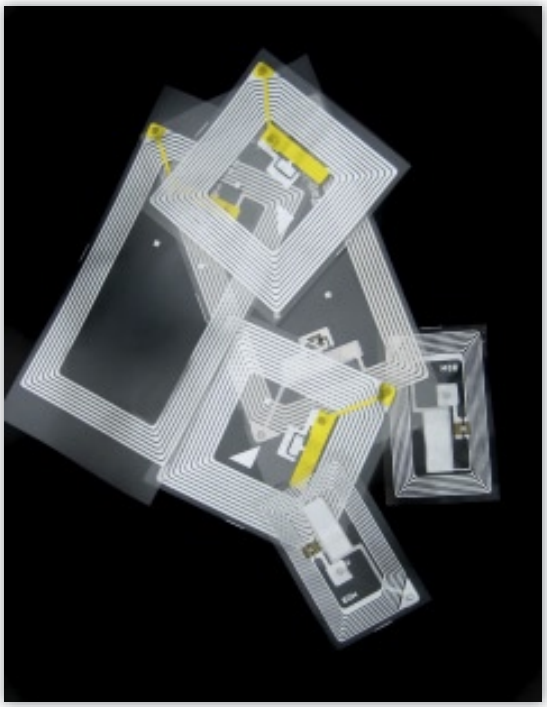
EIOD podkreśla, że systemy RFID mogłyby odegrać kluczową rolę w rozwoju europejskiego społeczeństwa informacyjnego, ale powszechną akceptację technologii RFID powinny ułatwić korzyści ze spójnych zabezpieczeń w zakresie ochrony danych. Samoregulacja może nie wystarczyć do osiągnięcia tego celu. Może zatem zostać wprowadzony wymóg, by instrumenty prawne gwarantowały istnienie rozwiązań technicznych ograniczających zagrożenia dla ochrony danych i prywatności. Obecna dyrektywa o ochronie danych rzeczywiście wystarczy do ochrony prywatności w pierwszej fazie. Należy jednak skutecznie stosować obecne ramy prawne. Nie ma potrzeby zmieniania zasad, ale dodatkowe przepisy szczegółowe mogą okazać się niezbędne, aby zapewnić odpowiednie rezultaty.

EIOD wzywa Komisję do rozważenia w szczególności następujących zaleceń:
- opracowanie, we współpracy z zainteresowanymi stronami, jasnych wskazówek dotyczących sto-

([45]) COM(2007) 263 wersja ostateczna z 6.7.2007.

([46]) Opinia z dnia 19 grudnia 2007 r. na temat inicjatywy Republiki Federalnej Niemiec w sprawie przyjęcia decyzji Rady dotyczącej wdrożenia decyzji 2007/.../WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej.

([47]) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie identyfikacji radiowej (RFID) w Europie: w stronę ram polityki (COM(2007) 96).



Internet przedmiotów: otoczenie, w którym każdy przedmiot ma swój identyfikator kontaktowy, musi być otoczeniem sprzyjającym prywatności

sowania obecnych ram prawnych w kontekście RFID;

- przyjęcie prawodawstwa wspólnotowego regulującego główne kwestie związane z wykorzystaniem RFID, na wypadek gdyby skuteczne stosowanie istniejących ram prawnych nie przyniosło pożądanych rezultatów;
- zawarcie w takich przepisach zasady wyrażenia zgody *(opt-in)* w miejscu sprzedaży jako precyzyjnego i niepodważalnego zobowiązania prawnego;
- określenie „najlepszych dostępnych technologii", które odegrają decydującą rolę w początkowym etapie przyjmowania zasady „wbudowanej" prywatności.

Decyzja ramowa Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa

Wniosek dotyczący decyzji ramowej Rady nakłada na przewoźników lotniczych obowiązek przekazywania danych o wszystkich pasażerach lotów na terytorium państw członkowskich UE lub z terytorium tych państw w celu zwalczania terroryzmu i przestępczości zorganizowanej ([48]).

W swojej opinii z dnia 20 grudnia 2007 r. ([49]) EIOD podkreśla ogromny wpływ, jaki wniosek wywarłby na prawa pasażerów lotów w zakresie prywatności i ochrony danych. EIOD uznaje walkę z terroryzmem za uzasadniony cel, uważa jednak, że nie stwierdzono w wystarczający sposób niezbędnego charakteru i proporcjonalności wniosku. Ponadto EIOD zajmuje krytyczne stanowisko wobec różnych niejasnych aspektów wniosku, w szczególności obowiązujących ram prawnych, tożsamości odbiorców danych osobowych oraz warunków przekazywania danych do państw trzecich.

Opinia skupia się na czterech kluczowych zagadnieniach i zamykają ją następujące wnioski:

- zasadność przetwarzania danych: wniosek nie przewiduje wystarczających elementów, które pozwalałyby na poparcie i wykazanie zasadności przetwarzania danych;
- obowiązujące ramy prawne: odnotowano znaczny brak pewności prawnej, jeżeli chodzi o system ochrony danych, który ma zastosowanie do różnych podmiotów zaangażowanych w przetwarzanie danych osobowych;
- tożsamość odbiorców danych: wniosek nie precyzuje tożsamości odbiorców danych osobowych, co jest niezbędne do oceny gwarancji, jakie ci odbiorcy przedstawią;
- przekazywanie danych do państw trzecich: kwestią kluczową jest spójność warunków transferu danych PNR do państw trzecich oraz podleganie tych warunków ujednoliconemu poziomowi ochrony.

EIOD zaleca ponadto, by nie przyjmować decyzji przed wejściem w życie traktatu lizbońskiego, tak by mogła ona zostać przyjęta według zwykłej procedury prawodawczej przewidzianej w nowym traktacie i zapewniającej pełny udział Parlamentu Europejskiego.

([48]) Wniosek z dnia 6 listopada 2007 r. dotyczący decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa (COM(2007) 654 wersja ostateczna).

([49]) Opinia z dnia 20 grudnia 2007 r. w sprawie projektu wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa.

3.4. Uwagi

Bezpieczeństwo i prywatność

Dnia 11 czerwca 2007 r. EIOD przesłał pisma do ministra sprawiedliwości i ministra spraw wewnętrznych Portugalii. Wezwał w nich przyszłą prezydencję, aby przed przyjmowaniem inicjatyw Rady zapewniała w wystarczającym stopniu uwzględnienie ich implikacji w dziedzinie ochrony danych. EIOD wyraził zaniepokojenie faktem, że wiele umów dotyczących nowych środków antyterrorystycznych zostało zawartych bez pełnego uwzględnienia ich wpływu na prawa podstawowe.

EIOD podkreślił, że komunikaty, takie jak „prawo do prywatności przysługuje dopiero po zagwarantowaniu ochrony życia i bezpieczeństwa", przerodziły się w slogan, sugerujący, że prawa podstawowe i wolności są luksusem, na który – w imię bezpieczeństwa – nie można sobie pozwolić. Z zaniepokojeniem stwierdził, że taki negatywny stosunek wobec praw jednostki do prywatności świadczy najwyraźniej o niezrozumieniu ram prawnych w dziedzinie praw człowieka, które zawsze pozwalały na stosowanie niezbędnych i proporcjonalnych środków w celu zwalczania przestępczości i terroryzmu.

Przyjmując takie podejście, ignoruje się również zebrane w ciągu ostatnich 50 lat doświadczenia związane z naruszaniem praw podstawowych w kontekście walki z terroryzmem w Europie. Nie powinno być wątpliwości co do tego, że skuteczne środki antyterrorystyczne mogą być stosowane bez naruszania praw podstawowych. Istnieją przykłady z przeszłości, z różnych miejsc Europy, na to, że nieskuteczna ochrona praw podstawowych zamiast zapewnienia bezpieczeństwa i stabilności zaburza na dłuższy czas porządek.

EIOD chce zagwarantować, by ochrona danych była uznawana za warunek zgodności z prawem (a także warunek powodzenia) wszelkich nowych inicjatyw w tej dziedzinie, a także wykazać korzyści płynące ze skutecznej ochrony danych dla bezpieczeństwa i egzekwowania prawa w całej Europie.

EIOD zaapelował także do Rady, aby – tak jak Komisja Europejska – korzystała z oferowanych przez niego usług doradczych we wszystkich sprawach dotyczących przetwarzania danych osobowych. Porady udzielone przez EIOD w szerokim zakresie Komisji w sprawie instrumentów UE w pierwszym i trzecim filarze zaowocowały poprawą prawodawstwa, zarówno pod względem jego zgodności z prawem, jak i skuteczności.

Kwestie te omawiano 17 września 2007 r. na spotkaniu z udziałem EIOD i ministra sprawiedliwości Portugalii, który potwierdził swoje zobowiązanie do odpowiedniego poszanowania prywatności i innych podstawowych praw we wszelkich stosownych aktach prawodawczych.

Traktat lizboński

W piśmie wysłanym 23 lipca 2007 r. do prezydium konferencji międzyrządowej (IGC) EIOD zwrócił się o włączenie do postanowień nowego traktatu pewnych konkretnych punktów w zakresie ochrony danych w celu ulepszenia tekstu Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, a także „Deklaracji w sprawie ochrony danych osobowych w dziedzinie współpracy sądowej w sprawach karnych i współpracy policyjnej". Niestety prezydium IGC nie odpowiedziało na sugestie EIOD.

Rozwój sytuacji w zakresie decyzji ramowej o ochronie danych

Zgodnie z trzecią opinią na temat ochrony danych w trzecim filarze EIOD uważnie śledził rozwój debaty politycznej na temat tego kluczowego aktu prawodawczego. EIOD skontaktował się z prezydencją portugalską, aby udzielić jej porad w sprawie pewnych zasadniczych elementów wniosku. Dnia 16 października 2007 r. EIOD przedstawił również uwagi w sprawie kilku istotnych, lecz bardziej technicznych aspektów, których nie powinno się pominąć na etapie finalizowania decyzji ramowej Rady.

EIOD zalecił zwłaszcza:

- uwzględnianie minimalnego poziomu ochrony przewidzianego przez konwencję Rady Europy nr 108, szczególnie w odniesieniu do przetwarzania danych szczególnie chronionych;
- wyjaśnienie związku między ograniczeniem celów, w jakich gromadzone są dane osobowe, a możliwością ich wykorzystania w pewnych przypadkach przez organy ścigania w innych, niezgodnych z założonymi celach;

- zapewnienie pełnego prawa dostępu do danych osobowych, szczególnie w przypadku decyzji automatycznych;
- zagwarantowanie doradczej roli organów ds. ochrony danych, także za pośrednictwem forum na szczeblu UE, na którym organy te mogłyby koordynować swoje działania.

EIOD został również poproszony o przedstawienie swojego stanowiska na forum Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego. W 2008 r. EIOD będzie nadal monitorował ten wniosek i gotowy jest udzielać dalszych porad.

Kontrola nabywania i posiadania broni

W piśmie z dnia 31 października 2007 r. wysłanym do sprawozdawcy Parlamentu Europejskiego odpowiedzialnego za tę sprawę EIOD zareagował na przebieg procedury przyjmowania wniosku dotyczącego dyrektywy regulującej kontrolę nabywania i posiadania broni ([50]).

W trakcie tej procedury poruszona została istotna kwestia ochrony danych, głównie w wyniku poprawki wprowadzonej do sprawozdania przygotowanego przez sprawozdawcę parlamentarnego. Poprawka ta wprowadza obowiązek utrzymywania w każdym państwie członkowskim skomputeryzowanego i scentralizowanego systemu rejestrowania danych, w którym niektóre dane będą przechowywane przez nie mniej niż 20 lat.

W swoim piśmie EIOD poruszył także pewne kwestie budzące niepokój, dotyczące zgodności systemu z dyrektywą 95/46/WE.

Rozporządzenie Rzym II w sprawie prawa właściwego dla zobowiązań pozaumownych

Dnia 28 lutego 2007 r. EIOD wysłał do przewodniczących Rady, Komisji i Parlamentu pismo, w którym wyraził pewne wątpliwości i uwagi dotyczące proponowanego art. 7a (naruszenia prawa prywatności i innych dóbr osobistych) rezolucji legislacyjnej Parlamentu Europejskiego w sprawie wspólnego stanowiska Rady dotyczącego przyjęcia rozporządzenia Parlamentu Europejskiego i Rady w sprawie prawa właściwego dla zobowiązań pozaumownych (Rzym II).

Artykuł ten rzeczywiście mógłby doprowadzić do pewnych niezgodności z dyrektywą 95/46/WE. Po pierwsze, nie było zupełnie jasne, czy ten artykuł ma obejmować naruszenia zasad prawnych w zakresie przetwarzania danych osobowych, przewidzianych w dyrektywie i powiązanych z nią instrumentach, a jeśli tak, w jakim stopniu miał je obejmować. W zakresie, w jakim ten nowy art. 7a miałby zastosowanie do naruszenia zasad prawnych w ramach zakresu zastosowania dyrektywy, odnotowano, że zawarte w nim podejście różniło się od art. 4 dyrektywy, jeżeli chodzi o prawo właściwe.

Po drugie, pojawiły się liczne inne, bardziej szczegółowe wątpliwości dotyczące jedynej części art. 7a, w której w sposób bezpośredni wymieniono pojęcie „danych osobowych". Nie było jasne, czy ustęp objąłby przetwarzanie danych w ogóle, czy tylko przetwarzanie ich przez nadawcę. Ponadto w tekście ust. 3 pojawiły się pewne nieścisłości terminologiczne w porównaniu do tekstu dyrektywy.

EIOD zasugerował przyjęcie bardziej ostrożnego podejścia na kolejnych etapach prawodawczych, aby uzyskać jasny obraz skutków, jakie proponowany tekst może przynieść w istniejącym prawodawstwie w zakresie ochrony danych, oraz aby uniknąć potencjalnych problemów, które zostały pokrótce opisane w piśmie.

Rozporządzenie zostało przyjęte 11 lipca 2007 r. ([51]). Artykuł 7a skreślono. W art. 30 ust. 2 zawarto klauzulę dotyczącą przeglądu, przewidującą, że nie później niż 31 grudnia 2008 r. Komisja powinna przedstawić opracowanie na temat sytuacji w dziedzinie prawa właściwego dla zobowiązań pozaumownych w świetle przypadków naruszenia prywatności i innych dóbr osobistych.

3.5. Interwencje przed Trybunałem

Kolejnym instrumentem, z jakiego korzysta EIOD w celu wywiązania się ze swojej roli doradczej wobec instytucji UE, są interwencje w sprawach wniesionych przed Trybunał Sprawiedliwości Wspólnot Europej-

([50]) Pismo z dnia 31 października 2007 r. w sprawie wniosku dotyczącego dyrektywy zmieniającej dyrektywę Rady 91/477/EWG w sprawie kontroli nabywania i posiadania broni.

([51]) Dz.U. L z 31.7.2007, s. 40.

skich na mocy art. 47 ust. 1 lit. i) rozporządzenia (WE) nr 45/2001. Instrument ten obejmuje interwencje przed Sądem Pierwszej Instancji i Sądem ds. Służby Publicznej (chociaż z tego ostatniego uprawnienia EIOD jeszcze nie skorzystał). Zakres tego instrumentu został określony przez Trybunał Sprawiedliwości w jego postanowieniach z dnia 17 marca 2005 r. w sprawach PNR.

W postanowieniu z dnia 12 września 2007 r. w sprawie C-73/07 *(Satakunnan Markkinapörssi i Satamedia)* prezes Trybunału Sprawiedliwości sprecyzował, że kompetencje EIOD nie obejmują postępowań dotyczących wydania orzeczenia w trybie prejudycjalnym. EIOD wniósł o dopuszczenie go do tej sprawy w charakterze interwenienta w związku ze znaczeniem „przetwarzania danych osobowych wyłącznie w celach dziennikarskich" określonego w dyrektywie 95/46/WE.

Dnia 8 listopada 2007 r. Sąd Pierwszej Instancji wydał wyrok w sprawie T-194/04 *(Bavarian Lager przeciwko Komisji)* – jednej z trzech spraw dotyczących związku między publicznym dostępem do dokumentów a ochroną danych, w których EIOD interweniował w 2006 r. Wyrok ten stanowi istotny krok w debacie na temat równowagi między tymi dwoma elementami.

Sąd Pierwszej Instancji stwierdził nieważność decyzji Komisji oddalającej wniosek o udzielenie pełnego dostępu do protokołu ze spotkania zorganizowanego przez Komisję, w tym do nazwisk uczestników tego spotkania. Sąd Pierwszej Instancji uznał, że ujawnienie nazwisk przedstawicieli podmiotu zbiorowego nie zagroziłoby ochronie ich prywatności i integralności.

EIOD interweniował w tej sprawie, popierając wniosek strony skarżącej o udzielenie dostępu i broniąc stanowiska, które zasadniczo potwierdził Sąd Pierwszej Instancji. W styczniu 2008 r. Komisja wniosła odwołanie do Trybunału Sprawiedliwości.

Inna sprawa, dotycząca podstawy prawnej dyrektywy 2006/24/WE w sprawie zatrzymywania danych (sprawa C-301/06 *Irlandia przeciwko Radzie i Parlamentowi*), w której EIOD wniósł o interwencję w 2006 r., nadal oczekuje na rozstrzygnięcie przez Trybunał Sprawiedliwości. W 2007 r. EIOD przedstawił uwagi pisemne.

Ponadto w grudniu 2007 r. EIOD wniósł do Sądu Pierwszej Instancji o dopuszczenie go w charakterze interwenienta do sprawy T-374/07 (*Pachtitis przeciwko Komisji i EPSO*). Sprawa dotyczy dostępu osoby do zadanych jej pytań i udzielonych przez nią odpowiedzi w ramach konkursu otwartego, który miał na celu stworzenie listy rezerwowej na potrzeby zatrudnienia w instytucjach europejskich.

3.6. Inne rodzaje działalności

Umowa z USA w sprawie PNR

EIOD był mocno zaangażowany w proces prowadzący do zawarcia umowy między UE a Stanami Zjednoczonymi w sprawie PNR, jak również w różne działania następcze po zawarciu nowej umowy w lipcu 2007 r.

Po pierwsze, EIOD zgłosił uwagi do mandatu negocjacyjnego, przy pełnym poszanowaniu potrzeby poufności. Po drugie, aktywnie uczestniczył w działaniach Grupy Roboczej Art. 29, między innymi podczas przygotowywania dokumentu strategicznego dotyczącego danych o pasażerach oraz podczas organizacji w Parlamencie Europejskim warsztatu, którego celem było lepsze uświadomienie różnych aspektów umowy. Swoje poglądy w sprawie proponowanej umowy przedstawiał również przy kilku innych okazjach, np. zdając sprawozdanie (pisemne i ustne) przed Komisją ds. Unii Europejskiej w Izbie Lordów.

Dane o pasażerach: wykorzystywane nie tylko z myślą o przelotach, lecz także o poszukiwaniu przestępców

Po zawarciu umowy EIOD, wraz z innymi członkami Grupy Roboczej Art. 29, wziął udział w analizie nowej umowy. W opinii przyjętej przez grupę roboczą 17 sierpnia 2007 r. wyrażono obawy w związku z faktem, że w porównaniu do poprzedniej umowy nowa umowa przewiduje słabsze zabezpieczenia.

Za szczególnie niepokojące uznano ilość i jakość przekazywanych danych, zwiększoną liczbę odbiorców, brak jasności co do celów, w jakich dane mogą być wykorzystywane, oraz warunki przeglądu systemu. Ponieważ opinia grupy roboczej w pełni odzwierciedliła poglądy EIOD, zrezygnował on z wydania własnej opinii.

Korzystając z aktywnego wkładu EIOD, grupa robocza również pracuje nad warunkami informowania pasażerów w momencie kupowania przez nich biletu lotniczego. W opinii przyjętej 15 lutego 2007 r. ([52]) przedstawiono zalecenia dla przedsiębiorstw lotniczych dotyczące sposobu przekazywania informacji telefonicznie, osobiście i przez Internet. Sporządzono wzory powiadomień, aby ułatwić przekazywanie tych informacji i zapewnić ich jednolitą treść w całej UE.

Przepisy wykonawcze SIS II

Instrumenty prawne nowego systemu informacyjnego Schengen (SIS II) nadają Komisji uprawnienia do ustanawiania środków wykonawczych, w tym do przygotowania podręcznika Sirene na potrzeby SIS II.

W podręczniku tym zawarto niektóre z zasad niezbędnych do właściwego funkcjonowania SIS II, których nie można było wyczerpująco opisać w instrumentach prawnych z uwagi na ich techniczny charakter, poziom szczegółowości i potrzebę regularnej aktualizacji. Zasady te są uzupełnieniem ram prawnych. Ponieważ środki te mogą mieć wpływ na prawa podstawowe, przeprowadzono nieformalne konsultacje z EIOD.

W swoich uwagach przesłanych Komisji 7 września 2007 r. EIOD poruszył różne kwestie dotyczące m.in.:

- przekazywania „dalszych informacji": należało wyjaśnić, jak rozumiane są „dalsze informacje", oraz potrzebę takiego przekazywania informacji w kontekście podręcznika Sirene;
- środków bezpieczeństwa: EIOD uwzględnił wysoki poziom bezpieczeństwa instrumentów prawnych, jakiego wymaga art. 10 ust. 1, oraz przedstawił kilka sugestii mających na celu podniesienie wymogów bezpieczeństwa, w szczególności bezpieczeństwa informatycznego;
- innych tematów, w tym: archiwizowania, automatycznego usuwania danych, zmiany celu wpisu, wniosków o dostęp do danych lub o ich korektę, wzajemnych powiązań między wpisami, procedur przewidzianych w art. 25 konwencji z Schengen oraz statystyki.

Początkowo planowano, że po nieformalnych uwagach zostanie wydana opinia EIOD. Nieformalne uwagi omówiono jednak z Komitetem ds. SIS-VIS 12 września 2007 r. Zostały one uwzględnione w zadowalającym zakresie. Uwagi, których nie uwzględniono, należy ponownie omówić z myślą o ocenie możliwości włączenia ich do zmienionej wersji przepisów wykonawczych.

Ku wykorzystaniu statystyki

Dnia 5 września 2007 r. EIOD przyjął opinię w sprawie wniosku dotyczącego statystyk Wspólnoty w zakresie zdrowia publicznego oraz bezpieczeństwa i higieny pracy (zob. pkt 3.3.2). W swoich wnioskach EIOD zaznaczył, że należy przeprowadzić wspólny przegląd procesów uruchomionych w Eurostacie służących do obsługi indywidualnych danych do celów statystycznych; przegląd ten może spowodować potrzebę przeprowadzenia kontroli wstępnej.

Wśród danych statystycznych mogą znaleźć się informacje prywatne

([52]) Opinia grupy roboczej 2/2007 na temat informowania pasażerów o przekazywaniu organom USA danych dotyczących przelotu pasażera (PNR) (WP 132).

Zdaniem EIOD, na ten wspólny przegląd powinny się składać: analiza minimalnego zestawu danych wymaganych do każdej operacji przetwarzania danych oraz analiza operacji przetwarzania danych wykonywanych przez Eurostat. Od tego czasu wielokrotnie kontaktowano się z właściwymi wydziałami Eurostatu w celu przeprowadzenia tego wspólnego przeglądu. Jako dokument podstawowy posłuży opinia 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych.

Jednocześnie prowadzone są z EIOD konsultacje w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie statystyki europejskiej. Konsultacje te mają być prowadzone równolegle ze wspólnym przeglądem, tak by EIOD mógł wyciągnąć ogólne wnioski na temat wykorzystywania statystyki.

System współpracy w zakresie ochrony konsumentów oraz system wymiany informacj w ramach rynku wewnętrznego

EIOD włożył wiele wysiłku w prace nad aspektami związanymi z ochroną danych w ramach dwóch systemów informatycznych na dużą skalę służących wymianie informacji między państwami członkowskimi: systemu współpracy w zakresie ochrony konsumentów (CPCS) oraz systemu wymiany informacji w ramach rynku wewnętrznego (IMI).

CPCS jest elektroniczną bazą danych zarządzaną przez Komisję Europejską w celu wymiany informacji między organami ds. ochrony konsumentów w państwach członkowskich a Komisją na mocy przepisów rozporządzenia (WE) nr 2006/2004 w sprawie współpracy w dziedzinie ochrony konsumentów ([53]).

IMI jest innym systemem informatycznym na dużą skalę zarządzanym przez Komisję Europejską w celu ułatwienia wymiany informacji między właściwymi organami w państwach członkowskich w dziedzinie prawodawstwa dotyczącego rynku wewnętrznego. Na razie wymiana informacji w ramach IMI odbywa się jedynie na mocy dyrektywy 2005/36/WE (dyrektywa o kwalifikacjach zawodowych) ([54]) i dyrektywy 2006/123/WE (dyrektywa usługowa) ([55]).

EIOD uczestniczył najpierw w pracach podgrupy *ad hoc* Grupy Roboczej Art. 29, które to prace zaowocowały dwiema opiniami grupy roboczej w sprawie CPCS i IMI ([56]). EIOD pełnił funkcję sprawozdawcy w przypadku opinii w sprawie CPCS. Następnie jesienią 2007 r. EIOD brał aktywny udział w pracach przygotowawczych nad:

- decyzją Komisji zmieniającą przepisy wykonawcze CPCS;
- nową decyzją Komisji w sprawie aspektów IMI dotyczących ochrony danych.

EIOD poparł utworzenie elektronicznych systemów wymiany informacji. Takie ujednolicone systemy mogą nie tylko usprawnić współpracę, ale także pomóc w zapewnieniu przestrzegania obowiązujących przepisów o ochronie danych. Rezultaty te można osiągnąć dzięki przyjęciu jasnych zasad dotyczących rodzaju informacji, które można wymieniać, podmiotów, które mogą brać udział w wymianie, i warunków takiej wymiany.

Ustanowienie scentralizowanego systemu elektronicznego stwarza jednak również pewne ryzyko. Ryzyko to obejmuje w szczególności fakt, że może być wymienianych więcej danych i w większym zakresie, niż jest to ściśle niezbędne do celów wydajnej współpracy, oraz że te dane, w tym dane potencjalnie nieaktualne i nierzetelne, mogą pozostać w systemie elektronicznym dłużej niż jest to konieczne. Kwestią newralgiczną jest także bezpieczeństwo bazy danych dostępnej w 27 państwach członkowskich, gdyż system jest bezpieczny jedynie na tyle, na ile pozwala mu na to najsłabsze ogniwo sieci. Dlatego EIOD zalecił, by problemy dotyczące ochrony danych rozwiązywać w sposób kompleksowy, zarówno na poziomie operacyjnym, jak i za pomocą prawnie wiążących decyzji Komisji w sprawie każdego z systemów.

([53]) Rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady z dnia 27 października 2004 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (rozporządzenie w sprawie współpracy w dziedzinie ochrony konsumentów), Dz.U. L 364 z 9.12.2004, s. 1.

([54]) Dyrektywa 2005/36/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie uznawania kwalifikacji zawodowych, tekst skonsolidowany opublikowany w Dz.U. L 271 z 16.10.2007, s. 18.

([55]) Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym, Dz.U. L 376 z 27.12.2006, s. 36.

([56]) WP 139 i WP 140 z dnia 20 września 2007 r. opublikowane na stronie internetowej grupy roboczej.

Grupa ds. RFID

W maju 2007 r. Komisja Europejska zaprosiła EIOD w charakterze obserwatora do udziału w grupie ekspertów i zainteresowanych podmiotów ds. RFID, która miała działać przez dwa lata. Zadaniem grupy jest wspomaganie Komisji w:

- przygotowaniu zalecenia, co stanowiło główną działalność grupy w 2007 r.;
- opracowaniu wytycznych w sprawie funkcjonowania aplikacji RFID;
- ocenie potrzeby dalszych działań prawodawczych;
- analizie charakteru i skutków trwających działań zmierzających do stworzenia „internetu fizycznych przedmiotów";
- realizacji inicjatywy na rzecz organizowania kampanii informacyjnych.

EIOD aktywnie uczestniczył we wszystkich pięciu spotkaniach, które zorganizowano w 2007 r., i przedstawił analizę na poparcie dyskusji prowadzonych w grupie. EIOD będzie nadal wnosił wkład w prace grupy w 2008 r., szczególnie w związku z inicjatywą „internet fizycznych przedmiotów" i aspektów RFID związanych z zarządzaniem.

Grupa ekspertów ds. zatrzymywania danych

EIOD uczestniczył w różnych spotkaniach grupy ekspertów ds. zatrzymywania danych. W 14. motywie dyrektywy 2006/24 w sprawie zatrzymywania danych uznano, że „technologie mające znaczenie dla łączności elektronicznej ulegają szybkiemu rozwojowi i dlatego uzasadnione wymogi właściwych organów także mogą ulec zmianie. W celu uzyskania opinii i zachęcenia do dzielenia się doświadczeniami co do najlepszych praktyk w tym zakresie Komisja zamierza stworzyć zespół składający się z przedstawicieli organów ścigania państw członkowskich, przedstawicieli branży łączności elektronicznej, przedstawicieli Parlamentu Europejskiego oraz organów ochrony danych, w tym *Europejskiego Inspektora ds. Ochrony Danych*.

Grupa zostanie formalnie utworzona w 2008 r., ale w 2007 r. zwołano już jej trzy posiedzenia.

3.7. Nowe wydarzenia

Pięć perspektyw przyszłych zmian (interakcje z technologią, wpływ traktatu lizbońskiego, egzekwowanie prawa, globalne zagadnienia dotyczące prywatności i jurysdykcji oraz wdrożenie dyrektywy) określonych w opinii EIOD na temat komunikatu w sprawie wdrażania dyrektywy o ochronie danych, posłuży jako plan przyszłych działań EIOD.

3.7.1. Interakcje z technologią

W sprawozdaniu rocznym z 2005 r. EIOD wyróżnił trzy tendencje w rozwoju technologii, od których coraz bardziej będzie uzależniony rozwój społeczeństwa informacyjnego:

1) codzienne otoczenie złożone z wszechobecnych punktów dostępu do sieci;
2) niemal nieograniczona przepustowość;
3) nieograniczona pojemność przechowywania danych.

Od czasu tego stwierdzenia te nowe tendencje technologiczne zaczęły przynosić pewne konkretne zmiany, które należy uważnie śledzić, gdyż oczekuje się, że wywrą one istotny wpływ na ramy UE w zakresie ochrony danych. Niektóre z tych tendencji opisano poniżej.

Tendencje

W 1984 r. William Gibson ([57]) opisał „cyberprzestrzeń" jako nowe i docelowo równoległe środowisko społeczeństwa informacyjnego. Ponad 20 lat później społeczeństwa informacyjnego nie można już uważać za równoległą rzeczywistość, ale za coraz wyraźniejszą część codziennego życia każdej osoby, opartą na technologiach cyfrowych.

Zasady ochrony danych mają zastosowanie także w digitalnej przestrzeni społecznej

([57]) *Neuromancer,* William Gibson, Ace edition, lipiec 1984.

Jak stwierdzono w artykule opublikowanym niedawno w „Firstmonday" ([58]), internetowym czasopiśmie naukowym redagowanym i recenzowanym przez niezależnych ekspertów, użytkownik (osoba) postrzegany jest jako główny „producent" nowych aplikacji zapełniających tzw. *Internet 2.0,* a aplikacje te są z kolei zasilane jego danymi osobowymi wraz z powiązaniami społecznymi i gospodarczymi, które użytkownik wytwarza z innymi osobami.

Rozwój aplikacji społecznościowych

Życie społeczne obywateli przenosi się w coraz większym stopniu na platformę cyfrową w wyniku stosowania aplikacji przetwarzających dane, ukierunkowanych na użytkowników, które w większości są danymi osobowymi. Powodzenie tych aplikacji, z których wywodzą się społeczności sieciowe, opiera się na liczbie zarejestrowanych użytkowników, zasobach rzetelnych danych definiujących przechowywane profile i oczywiście na zdolności tworzenia silniejszych powiązań między osobami a treścią.

EIOD uważa ten nowy model aplikacji za innowację technologiczną, która prawdopodobnie wywrze istotny wpływ na ochronę danych. Okaże się, czy istniejące europejskie ramy prawne w zakresie ochrony danych zapewnią wystarczającą ochronę. Szczególną uwagę należy poświęcić pojęciu „administratora" (jak należy je rozumieć, gdy użytkownicy końcowi są głównymi podmiotami przetwarzającymi dane), zastosowaniu rozporządzenia oraz coraz bardziej względnemu pojęciu lokalizacji procesu. EIOD z zadowoleniem przyjmuje wydany w 2007 r. pierwszy dokument Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) przedstawiający jej stanowisko w sprawie pewnych zagadnień związanych z bezpieczeństwem i proponujący zalecenia w zakresie aplikacji społecznościowych ([59]).

Aplikacje społecznościowe i społeczności sieciowe mają również podstawy techniczne we wcześniejszym środowisku gospodarczym, które napędzane było rozwojem zdalnych aplikacji i zdalnych pamięci masowych, wspomaganych ogromnymi centrami danych i zespołami serwerów tworzących wspólnie tzw. chmurę ([60]).

Centra danych, wirtualizacja i zdalne przechowywanie danych

Centra danych, których rozwój jest możliwy dzięki trzem opisanym wyżej głównym tendencjom technologicznym, mogą oznaczać koniec komputera osobistego, na którym do tej pory były przetwarzane dane, a szczególnie dane osobowe. Zdalne przechowywanie danych i aplikacje sieciowe już się pojawiają, ale związane z nimi ramy ochrony danych i warunki ich właściwego stosowania nadal wymagają analizy. Tak jak w wypadku społeczności sieciowych – pojęcie lokalizacji procesu i administratora w wypadku rozproszonych zasobów obliczeniowych staje się coraz trudniejsze do określenia.

Kiedy przetwarzanie danych osobowych, przechowywanych w sieciach *peer-to-peer,* rozproszone będzie w chmurze obliczeniowej, skuteczne egzekwowanie europejskich ram w zakresie ochrony danych przy zastosowaniu tradycyjnego podejścia może być coraz trudniejsze.

Jak podkreślono w opinii na temat wdrażania dyrektywy o ochronie danych ([61]), EIOD uważa, że w świetle tych zmian technologicznych oraz w celu podtrzymywania innowacji i wspierania nowych interakcji społecznych i modeli biznesowych zmiany do dyrektywy wydają się nieuniknione, chociaż jej podstawowe zasady powinny pozostać niezmienione. Konieczne mogą być inne rozwiązania administracyjne, które z jednej strony będą skuteczne i właściwe z punktu widzenia społeczeństwa sieciowego, a z drugiej strony ograniczą do minimum koszty administracyjne.

Badania i rozwój

W związku z tym, że na wymogi związane z ochroną prywatności i danych należy zwracać uwagę i stosować je na możliwie wczesnym etapie w cyklu życia nowych technologii, europejskie działania w zakresie badań i rozwoju (B + R) dają, zdaniem EIOD, bardzo dobrą sposobność do realizacji tych celów, a zasada „wbudowanej" prywatności powinna stanowić nieodłączny element tych inicjatyw w zakresie badań i rozwoju.

([58]) http://www.firstmonday.org/ISSUES/issue12_3/pascu/

([59]) Kwestie bezpieczeństwa i zalecenia w zakresie społeczności sieciowych (Security issues and recommendations for online social networks), dokument nr 1 przedstawiający stanowisko ENISA, październik 2007, (http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf).

([60]) http://en.wikipedia.org/wiki/Cloud_computing

([61]) Omówiono ją w rozdziale 3.3 sprawozdania rocznego.

Dlatego też w 2007 r. EIOD przeprowadził kilka działań z myślą o wprowadzeniu tej zasady w życie.

Przegląd wniosków dotyczących 7. PR

W lipcu 2007 r., na wniosek Komisji, EIOD dokonał przeglądu niektórych wniosków w ramach siódmego programu ramowego w zakresie badań i rozwoju technologicznego (7. PR), będących odpowiedzią na pierwsze zaproszenie do składania ofert związanych z technologiami informacyjno-komunikacyjnymi (ICT/TIK). W odniesieniu do wniosków, które uzyskały już wymaganą liczbę punktów, udzielono wskazówek na temat aspektów związanych z ochroną danych.

Dokument strategiczny dotyczący B + R

Na początku 2008 r. EIOD przyjął dokument strategiczny, w którym opisano ewentualną rolę, jaką jego instytucja mogłaby odegrać w projektach związanych z badaniami i rozwojem w ramach 7. PR. W dokumencie tym przedstawiono kryteria selekcji projektów do działań EIOD oraz sposób, w jaki EIOD może wnosić wkład w te projekty. W związku z tym, że EIOD posiada status niezależnego organu, nie można zakładać jego udziału w projekcie w charakterze partnera konsorcjum.

3.7.2. Nowe wydarzenia w polityce i prawodawstwie

Wpływ traktatu lizbońskiego

Ramy prawne UE ulegną zmianie wraz z wejściem w życie traktatu lizbońskiego. Sytuacja ta będzie miała także konsekwencje dla działania EIOD jako organu doradczego. Nowy traktat określi nowy kontekst tych działań, co będzie miało szczególny wpływ na wnioski prawodawcze dotyczące wymiany danych osobowych oraz ochrony tych danych w celu egzekwowania prawa.

W 2008 r. EIOD będzie musiał zająć się następującymi zagadnieniami:

- jaki powinien być sposób działania w okresie przejściowym: nie należy przyjmować istotnych aktów przed wejściem w życie nowego traktatu (głosowanie większością kwalifikowaną, współdecyzja i dostępność postępowań o naruszenie przepisów);
- wpływ nowego traktatu na obszary, w których podmioty prywatne zaangażowane są w działania w zakresie egzekwowania prawa;
- czy konieczne jest zmodyfikowanie dyrektywy 95/46/WE i rozporządzenia (WE) nr 45/2001.

Egzekwowanie prawa

EIOD spodziewa się, że kontynuowane będą działania prawodawcze związane ze zwiększoną potrzebą przechowywania i wymiany danych osobowych do celów egzekwowania prawa. W ramach swojego podejścia do tych działań prawodawczych EIOD – oprócz zajmowania się istniejącym prawodawstwem, które częstokroć nie zostało nawet w pełni wprowadzone w życie – będzie nadal analizował uzasadnienie takich działań.

Możliwe, że potrzebne będą alternatywne podejścia obejmujące inne sposoby reagowania na zagrożenia dla społeczeństwa. Pełne wprowadzenie w życie istniejącego prawodawstwa powinno mieć zawsze istotne znaczenie. We właściwy sposób należy uwzględnić ryzyko związane z nowymi aktami prawnymi przyczyniającymi się do powstania „społeczeństwa kontrolowanego".

Inną kwestią, którą powinien się zająć EIOD, są ramy ochrony danych, które mimo, a może także z powodu przyjęcia decyzji ramowej Rady, co nastąpi prawdopodobnie na początku 2008 r., można określić jako eklektyczne. Ramy te są niewystarczające i niejasne jest, jakie przepisy mają zastosowanie w danej sytuacji. To samo odnosi się do środków odwoławczych, którymi dysponuje podmiot danych.

Globalne zagadnienia dotyczące prywatności i jurysdykcji

W tym kontekście przydatne jest uwzględnienie następujących kwestii:

- Wymiana informacji za pośrednictwem ogólnie dostępnych źródeł, takich jak Internet, staje się coraz powszechniejszym zjawiskiem. Nie jest oczywiste, w jakim stopniu prawodawstwo UE jest możliwe do zastosowania i egzekwowania w odniesieniu do Internetu, także w związku z tym, że dostawcy usług to dość często podmioty spoza UE. Przykładem są tu wyszukiwarki, takie jak Google lub Yahoo.

- Przekazywanie danych osobowych do państw trzecich w celu egzekwowania prawa, a nawet dostęp organów państw trzecich do danych znajdujących się na obszarze UE, ma coraz większe znaczenie. Wzrasta liczba państw trzecich, które zwracają się o przekazanie lub przyznanie dostępu do danych, na przykład dotyczących pasażerów.
- Nie ma powszechnej jednomyślności co do wspólnych norm w zakresie prywatności. W ostatnim czasie poczyniono pierwsze kroki w celu określenia wspólnego podejścia transatlantyckiego.

Jak stwierdzono w opinii EIOD w sprawie wdrażania dyrektywy o ochronie danych, wyzwaniem będzie opracowanie praktycznych rozwiązań, które pogodziłyby potrzebę ochrony europejskich podmiotów danych z ograniczeniami terytorialnymi Unii Europejskiej i jej państw członkowskich.

Drugim wyzwaniem będzie utrzymanie (wysokiego) poziomu ochrony na obszarze UE, także w stosunkach z państwami trzecimi: W jakim stopniu powinniśmy propagować nasze normy lub z nich rezygnować oraz w jakim zakresie powinniśmy negocjować wspólne normy?

Pełne wdrożenie

Jak wyjaśniono w opinii EIOD w sprawie wdrażania dyrektywy o ochronie danych (zob. pkt 3.3), pełne wdrożenie obejmuje szereg działań, które będą miały również istotne znaczenie w pracach prowadzonych przez EIOD w najbliższych latach. Istotnym zagadnieniem będzie w każdym razie praca nad komunikatami wyjaśniającymi. Komunikaty te mogą przyczynić się do dalszej harmonizacji prawa dotyczącego ochrony danych w państwach członkowskich, a także do ujawnienia zagadnień, które mogą powodować w przyszłości konieczność zmian wspomnianej dyrektywy.

EIOD będzie również aktywnie uczestniczyć w dyskusjach dotyczących ewentualnych przyszłych zmian dyrektywy o ochronie danych, a także, w niektórych przypadkach, będzie inicjatorem takich dyskusji.

Należy pamiętać, że przyszłe zmiany mogłyby mieć konsekwencje nie tylko dla dyrektywy 95/46/WE, lecz także dla związanych z nią instrumentów, takich jak dyrektywa 2002/58/WE i rozporządzenie (WE) nr 45/2001.

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 ([62]). Zadania grupy zostały określone w art. 30 dyrektywy i w skrócie można je przedstawić następująco:

- dostarczanie Komisji Europejskiej fachowych opinii pochodzących od państw członkowskich na temat zagadnień związanych z ochroną danych;
- promowanie jednolitego stosowania ogólnych zasad przedmiotowej dyrektywy we wszystkich państwach członkowskich przez współpracę między organami zajmującymi się nadzorem nad ochroną 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 odniesieniu do przetwarzania danych osobowych we Wspólnocie Europejskiej.

EIOD jest członkiem Grupy Roboczej Art. 29 od początku 2004 r. Artykuł 46 lit. g) rozporządzenia (WE) 45/2001 przewiduje, że EIOD bierze udział w działalności wspomnianej grupy roboczej. Zdaniem EIOD jest to bardzo ważna platforma współpracy z krajowymi organami nadzoru. Jest również oczywiste, że ta grupa robocza powinna odgrywać jedną z głównych ról, jeśli chodzi o jednolite stosowanie dyrektywy oraz interpretowanie jej ogólnych zasad.

Zgodnie z programem prac grupy roboczej na lata 2006–2007 i przy zdecydowanym wsparciu ze strony EIOD grupa skoncentrowała się na pewnych zagadnieniach strategicznych, by przyczynić się do wypracowania wspólnej interpretacji najważniejszych przepisów i do ich lepszego wdrożenia. Grupa robocza udoskonaliła również sposób informowania na zewnątrz o swoich działaniach. Doprowadziło to do opracowania różnych ważnych dokumentów, takich jak:

- dokument roboczy na temat przetwarzania danych osobowych dotyczących zdrowia zawartych w elektronicznej dokumentacji zdrowotnej, przyjęty 15 lutego 2007 r. (WP 131);
- opinia 2/2007 na temat informowania pasażerów o przekazaniu organom USA danych dotyczących przelotu pasażera (PNR), przyjęta 15 lutego 2007 r. (WP 132);
- zmieniona i uaktualniona polityka promowania przejrzystości działań grupy roboczej utworzonej na mocy art. 29 dyrektywy 95/46/WE, przyjęta 15 lutego 2007 r. (WP 135);
- opinia 4/2007 na temat pojęcia danych osobowych, przyjęta 20 czerwca 2007 r. (WP 136).

Grupa robocza wydała szereg opinii na temat wniosków prawodawczych lub podobnych dokumentów. W niektórych przypadkach wnioski te były również przedmiotem opinii EIOD na podstawie art. 28 ust. 2 rozporządzenia (WE) 45/2001. Opinia EIOD jest obowiązkowym elementem procesu prawodawczego UE, ale opinie grupy roboczej są również niezwykle przydatne, zwłaszcza ze względu na fakt, że mogą zawierać kwestie szczególnie istotne z punktu widzenia danego kraju.

([62]) 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.

EIOD z zadowoleniem przyjmuje opinie Grupy Roboczej Art. 29, które są w dużym stopniu zbieżne z jego opiniami. W jednym przypadku EIOD rozwinął w swojej opinii pewne elementy opinii wydanej przez grupę roboczą. W innym przypadku EIOD wolał współpracować przy opracowaniu jednej opinii i nie wydał własnych uwag. Przykłady dobrej synergii między grupą roboczą a EIOD w tej dziedzinie są następujące:

- opinia 3/2007 na temat 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, łącznie z przepisami dotyczącymi organizacji przyjmowania i rozpatrywania wniosków wizowych, przyjęta 1 marca 2007 r. (WP 134) ([63]);
- opinia nr 5/2007 w sprawie Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych zawartej w lipcu 2007 r., przyjęta 17 sierpnia 2007 r. (WP 138);
- wspólna opinia na temat wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących przelotu pasażera w celu egzekwowania prawa, przedstawionego przez Komisję 6 listopada 2007 r., przyjęta 5 grudnia 2007 r. (WP 145) ([64]).

EIOD ściśle współpracował ze wspomnianą grupą roboczą przy analizie dwóch dużych systemów w ramach pierwszego filaru, która to analiza wymagała koordynacji zadań związanych z nadzorem na szczeblu unijnym i krajowym:

- opinia 6/2007 na temat problematyki ochrony danych związanej z systemem współpracy w zakresie ochrony konsumentów, przyjęta 20 września 2007 r. (WP 139);
- opinia 7/2007 na temat problematyki ochrony danych związanej z systemem wymiany informacji w ramach rynku wewnętrznego, przyjęta 20 września 2007 r. (WP 140).

Zgodnie z art. 46 lit. f) ppkt (i) rozporządzenia 45/2001 EIOD musi również współpracować z krajowymi organami nadzoru w stopniu umożliwiającym im wykonanie własnych obowiązków; polega to w szczególności na wymianie wszystkich użytecznych informacji i na zwracaniu się o pomoc lub na świadczeniu pomocy przy wykonywaniu powierzonych tym organom zadań. Współpraca taka dostosowywana jest do poszczególnych przypadków. Dobrym przykładem wielostronnej współpracy nadal była sprawa SWIFT; Grupa Robocza Art. 29 regularnie monitorowała działania podejmowane w następstwie swojej opinii ([65]) przyjętej w 2006 r. i ostatecznie udało jej się odnotować istotne postępy w stosowaniu się do tej opinii (zob. także pkt 2.5) .

Bezpośrednia współpraca z organami krajowymi staje się coraz bardziej istotna w związku z istnieniem międzynarodowych systemów, takich jak Eurodac, które wymagają skoordynowanego podejścia w zakresie nadzoru (zob. pkt 4.3).

4.2. Grupa Robocza Rady ds. Ochrony Danych

W 2006 r. prezydencje austriacka i fińska zwołały szereg posiedzeń Grupy Roboczej Rady ds. Ochrony Danych. EIOD z zadowoleniem przyjął tę inicjatywę, zauważając, że stanowi ona użyteczną sposobność zapewnienia bardziej horyzontalnego podejścia do spraw pierwszego filaru, i wziął udział w kilku z tych posiedzeń.

Prezydencja niemiecka postanowiła na tej samej zasadzie kontynuować dyskusje na temat ewentualnych inicjatyw Komisji i innych stosownych tematów związanych z pierwszym filarem. W styczniu 2007 r. wystąpiła z inicjatywą polegającą na skierowaniu do państw członkowskich kwestionariusza dotyczącego ich doświadczeń związanych z dyrektywą 95/46/WE. Około połowy delegacji odpowiedziało na zadane pytania. Ich reakcje potwierdziły ogólne zadowolenie z dyrektywy, chociaż delegacje przekazały również istotne informacje zwrotne na temat potencjalnych problemów i możliwych rozwiązań. Prezydencja niemiecka nie sformułowała jednak żadnych konkretnych wniosków.

([63]) Zob. również opinia EIOD wydana 27 października 2006 r.

([64]) Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości (zob. pkt 4.4) przyjęła tę opinię w dniu 18 grudnia 2007 r. Zob. również opinia EIOD wydana 20 grudnia 2007 r.

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

W maju 2007 r. Komisja przedstawiła komunikaty w sprawie: kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności oraz identyfikacji radiowej (RFID). Dwa z tych komunikatów były przedmiotem opinii EIOD (zob. pkt 3.3). Dyskusje w ramach grupy roboczej Rady nie doprowadziły do sformułowania odmiennych wniosków.

EIOD wykorzystał pierwsze posiedzenie w ramach prezydencji niemieckiej, aby przedstawić swoje priorytety w zakresie konsultacji dotyczących nowego prawodawstwa (zob. pkt 3.2). W trakcie drugiego posiedzenia przedstawił sprawozdanie roczne za 2006 r.

Prezydencja portugalska przewidziała jedno posiedzenie grupy roboczej, lecz zostało ono odwołane. Prezydencja słoweńska również zaplanowała jedno posiedzenie – w maju 2008 r.

EIOD nadal z ogromnym zainteresowaniem śledzi wspomniane działania; w stosownych przypadkach pozostaje również do dyspozycji w kwestii doradztwa i współpracy.

4.3. Skoordynowany nadzór nad systemem Eurodac

Współpraca z krajowymi organami ds. ochrony danych, mająca na celu wypracowanie skoordynowanego podejścia do nadzoru nad systemem Eurodac, choć zainicjowana została dopiero kilka lat temu, szybko się rozwija.

W skład grupy ds. koordynowania nadzoru nad systemem Eurodac (zwanej dalej „grupą") wchodzą przedstawiciele krajowych organów ds. ochrony danych oraz EIOD; odbyły się trzy posiedzenia tej grupy: w marcu, czerwcu i grudniu 2007 r. Grupa przyjęła kilka bardzo istotnych dokumentów dotyczących skoordynowanego nadzoru, natomiast EIOD w tym samym okresie przeprowadził audyt bezpieczeństwa w jednostce centralnej Eurodac (zob. pkt 2.10).

Pierwsza skoordynowana kontrola

Na pierwszym posiedzeniu w 2005 r. wspomniana grupa postanowiła przeprowadzić na szczeblu krajowym kontrolę określonych elementów systemu Eurodac. EIOD miał opracować zestawienie wyników tej kontroli. Prowadzono ją w 2006 r. i zakończono wiosną 2007 r. Sprawozdanie opublikowano w lipcu 2007 r. ([66]).

Dokładnie przeanalizowano trzy główne zagadnienia: „wyszukiwania specjalne", „dalsze użytkowanie danych" i „jakość danych".

- Stosowanie „wyszukiwań specjalnych" zostało prawnie ograniczone do tych azylantów i nielegalnych imigrantów, którzy chcą mieć dostęp do swoich danych osobowych. Liczba wyszukiwań była bardzo zróżnicowana między poszczególnymi państwami, co wywołało obawy związane z dużymi liczbami w niektórych państwach. Grupa stwierdziła, że początkowo przy wyszukiwaniach specjalnych popełniano błędy, które już zostały naprawione. Stosowanie wyszukiwań specjalnych powinno być w przyszłości monitorowane, aby uniknąć ewentualnych błędów lub nadużyć. W sprawozdaniu podkreślono również konieczność podniesienia świadomości na temat praw podmiotów danych.
- Odciski palców znajdujące się w Eurodac można wykorzystywać wyłącznie do określenia, które państwo odpowiada za wniosek o azyl. Nie stwierdzono nadużyć, pomimo faktu, że niektóre krajowe jednostki Eurodac są obsługiwane przez służby policyjne i pomimo ogólnego rozszerzenia dostępu do baz danych dla organów ścigania. Grupa ustaliła również, że w niektórych państwach występowały trudności w określeniu, która jednostka odpowiada za przetwarzanie danych osobowych, w związku z czym sprawozdanie zaleca podjęcie kroków, które będą miały na celu rozwiązanie tej sytuacji.
- Podstawowym wymaganiem jest jakość odcisków palców. Komisja Europejska wyraziła zaniepokojenie faktem, że 6% odcisków palców odrzucono ze względu na ich niską jakość. Grupa stwierdziła, że państwa zainteresowane powinny dołożyć wszelkich starań, aby zagwarantować lepszą jakość w zakresie technologii (skanowanie na żywo) oraz szkolenia.

([66]) Zob. strona internetowa EIOD: część „Supervision", zakładka „Eurodac".

Grupa nie stwierdziła przypadków nadużywania systemu Eurodac. Niektóre aspekty jego funkcjonowania, np. informacje przekazywane osobom zainteresowanym, wymagają jednak udoskonalenia.

Sprawozdanie przekazano głównym zainteresowanym podmiotom instytucjonalnym na szczeblu UE, a także organizacjom międzynarodowym i organizacjom pozarządowym zajmującym się kwestiami azylu i imigracji. Kontrola miała widoczny wpływ na liczbę wyszukiwań specjalnych, która we wszystkich państwach członkowskich wyraźnie się zmniejszyła.

EIOD uznał to za pozytywne doświadczenie, będące dowodem na dobrą współpracę grupy i jej zdolność do wprowadzania zmian. Jest to ważne nie tylko z punktu widzenia egzekwowania praw do ochrony danych osób ubiegających się o azyl, lecz także dlatego, że ten pilotażowy projekt miał ogromne znaczenie dla innych systemów informacyjnych o dużym zasięgu, takich jak nowy system informacyjny Schengen (SIS II).

Sformalizowanie metod pracy

Początkowo grupa zajmowała się skoordynowanym nadzorem nad systemem Eurodac w sposób nieformalny, opierając się na rozporządzeniu dotyczącym Eurodac (art. 20) i doświadczeniach innych organów. Konieczne okazało się bardziej zorganizowane podejście, za czym przemawiały trzy główne powody.

- W przyszłości model skoordynowanego nadzoru w ramach systemu Eurodac zostanie prawdopodobnie wykorzystany przy innych systemach. W dokumentach prawodawczych dotyczących tych systemów mówi się o skoordynowanej kontroli; zaangażowane organy powinny określić i wypracować przepisy wewnętrzne lub metody pracy do celów tej skoordynowanej kontroli. Rozpoczęcie rozważań nad tymi przepisami zapewniłoby więcej czasu na ich stopniowe opracowanie.
- Dokonanie przeglądu systemu dublińskiego przez Komisję doprowadzi do przedstawienia wniosków prawodawczych dotyczących systemu Eurodac. Część tego nowego prawodawstwa będzie prawdopodobnie dotyczyć nadzoru nad systemem Eurodac. W tym kontekście logiczne byłoby, gdyby prawodawca europejski postępował według tego samego wzoru, który przewidziano dla innych systemów IT o dużym zasięgu. Eurodac mógłby zatem wykorzystywać skoordynowany nadzór oparty na tym samym modelu, obejmującym wymóg istnienia sformalizowanych metod pracy.
- Państwa spoza UE (np. Norwegia, Islandia i Szwajcaria) przyłączyły się już do systemu, w tym do jego nadzoru, lub uczynią to wkrótce. Państwa te nie są objęte *expressis verbis* rozporządzeniem dotyczącym Eurodac; ich organom ds. ochrony należy przedstawić jasny obraz modelu nadzoru, do którego się przyłączają.

System Eurodac został stworzony, by można było sprawdzać odciski palców osób ubiegających się o azyl i nielegalnych imigrantów

EIOD przedłożył wykaz najważniejszych punktów, które należy omówić na marcowym posiedzeniu. Po ich przedyskutowaniu, na czerwcowym posiedzeniu przeanalizowano formalną propozycję regulaminu. Uzgodniono, że przepisy wewnętrzne powinny zapewniać jednocześnie przejrzystość i elastyczność. Regulamin nie powinien być też zbyt przeładowany. W grudniu 2007 r. regulamin ten został przyjęty.

Przyszłe działania

W 2007 r. miało miejsce kilka ważnych wydarzeń. W czerwcu Komisja opublikowała sprawozdanie z oceny systemu dublińskiego, które zawiera analizę działania systemu Eurodac i propozycje nowych perspektyw. Jednocześnie coraz bardziej naciskano na przyznanie w pewnym zakresie dostępu do systemu Eurodac organom ścigania. Kontekstem dla obu tych wydarzeń było trwające opracowywanie systemów IT o dużym zasięgu.

Grupa wskazała w tym kontekście na swoje priorytety – na grudniowym posiedzeniu przyjęto program prac. Skoordynowanemu nadzorowi poddane zostaną następujące zagadnienia: przekazywanie informacji podmiotom danych, odciski palców dzieci oraz korzystanie z DubliNet. Pod koniec 2008 r. powinna również zostać przeanalizowana kwestia wcześniejszego usuwania danych.

4.4. Trzeci filar

Artykuł 46 lit. f) ppkt (ii) rozporządzenia (WE) 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 organów nadzoru. W praktyce współpraca odbywa się z udziałem stosownych wspólnych organów nadzoru, wspieranych przez wspólny sekretariat ds. ochrony danych przy Radzie, a mówiąc ogólniej, z udziałem krajowych organów ds. ochrony danych.

Rosnąca liczba inicjatyw na poziomie europejskim, które mają na celu zwalczanie przestępczości zorganizowanej i terroryzmu, w tym różnych wniosków dotyczących wymiany danych osobowych, uwidoczniła w ostatnich latach potrzebę ściślejszej współpracy między krajowymi organami ds. ochrony danych a EIOD.

W 2007 r. koncentrowano się na dwóch głównych kwestiach. Pierwszą z nich było omówienie wniosku Komisji dotyczącego decyzji ramowej w sprawie ochrony danych w trzecim filarze. Pierwotny wniosek został przedyskutowany i zmieniony; EIOD dokładnie śledził rozwój wydarzeń – 27 kwietnia wydał swoją trzecią opinię, a 16 października wystosował pismo do prezydencji portugalskiej (zob. pkt 3.3 i 3.4).

Na konferencji europejskich organów ds. ochrony danych zorganizowanej w Larnace (Cypr) w dniach 10–11 maja 2007 r. przyjęto oświadczenie, które było całkowicie spójne z opinią EIOD. Europejskie krajowe organy ds. ochrony danych potwierdziły, że zapewnienie zharmonizowanego i wysokiego poziomu ochrony danych, obejmującego działania policyjne i sądowe, ma istotne znaczenie w procesie tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Ponadto wyrażono ubolewanie w związku z tym, że przebieg negocjacji wskazuje na zwrot ku wąskiemu zakresowi stosowania i niedostatecznemu poziomowi ochrony danych ([67]).

Drugą kwestią była wymiana informacji dotyczących egzekwowania prawa zgodnie z zasadą dostępności, a w szczególności inicjatywa piętnastu państw członkowskich mająca na celu sprawienie, by konwencja z Prüm – ustanawiająca transgraniczną wymianę danych biometrycznych do celów walki z terroryzmem i przestępczością transgraniczną – miała zastosowanie w całej UE. EIOD wydał dwie opinie: 4 kwietnia 2007 r. – w sprawie samej inicjatywy dotyczącej konwencji z Prüm i 19 grudnia 2007 r. – w sprawie jej przepisów wykonawczych (zob. pkt 3.3).

W tym kontekście EIOD wniósł wkład do wspólnego stanowiska europejskich organów ds. ochrony danych na temat wykorzystywania pojęcia dostępności w egzekwowaniu prawa, przyjętego w Larnace na konferencji europejskich organów ds. ochrony danych ([68]). To oświadczenie i załączona do niego lista kontrolna dostarczają instytucjom UE oraz parlamentom krajowym wskazówki, w jaki sposób zagwarantować, by instrumenty dotyczące zasady dostępności poprawiły skuteczność egzekwowania prawa, a jednocześnie, jak dbać o podstawowe prawo do ochrony danych osobowych.

Na konferencji w Larnace postanowiono również przyznać szerszy mandat Grupie Roboczej ds. Policji, która na potrzeby konferencji monitoruje zagadnienia w trzecim filarze. Rosnąca potrzeba stałego monitorowania inicjatyw w trzecim filarze oraz szybkiego i skutecznego reagowania na nie wymaga bardziej stabilnego i zorganizowanego forum. Szerszy mandat Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości (nowa nazwa grupy) będzie obejmował monitorowanie rozwoju wydarzeń w zakresie egzekwowania prawa w odniesieniu do przetwarzania danych osobowych,

([67]) Oświadczenie dotyczące projektu decyzji ramowej w sprawie ochrony danych w trzecim filarze, przyjęte 11 maja 2007 r., dostępne na stronie internetowej EIOD w części „Cooperation" w zakładce „European Conference".

([68]) Oświadczenie w sprawie zasady dostępności oraz wspólne stanowisko i lista kontrolna, przyjęte 11 maja 2007 r., dostępne na stronie internetowej EIOD w części „Cooperation" w zakładce „European Conference".

przygotowywanie wszelkich niezbędnych działań, które w tej dziedzinie powinna podjąć konferencja, a także działanie w imieniu konferencji, w sytuacji gdy pilnie potrzebna jest szybka reakcja. W związku z tym konferencja powołała Francesca Pizzettiego, przewodniczącego włoskiego organu ds. ochrony danych, na stanowisko przewodniczącego grupy roboczej, a Barta De Schuttera, członka belgijskiego organu ds. ochrony danych, na stanowisko zastępcy przewodniczącego; kadencja w obu przypadkach potrwa dwa lata.

EIOD był aktywnym uczestnikiem trzech posiedzeń Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości zorganizowanych w 2007 r. Po osiągnięciu porozumienia co do regulaminu wewnętrznego i metod pracy grupa robocza zajęła się innymi istotnymi kwestiami, m.in.:

- pismem do prezydencji portugalskiej na temat debaty w Radzie nad decyzją ramową w sprawie ochrony danych w trzecim filarze;
- pierwszą dyskusją na temat przepisów wykonawczych na potrzeby inicjatywy dotyczącej konwencji z Prüm;
- opinią na temat propozycji UE dotyczącej PNR, przyjętą wspólnie z Grupą Roboczą Art. 29;
- potrzebą wspólnej polityki nadzoru nad działaniami w zakresie egzekwowania prawa.

Ponadto EIOD oraz przewodniczący Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości wzięli udział w posiedzeniu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego poświęconym sytuacji w dziedzinie ochrony danych w trzecim filarze.

4.5. Konferencja europejska

Organy ds. ochrony danych z państw członkowskich UE oraz Rada 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. EIOD i jego zastępca uczestniczyli w konferencji w Larnace (Cypr), która odbyła się w dniach 10–11 maja 2007 r. i której gospodarzem był cypryjski komisarz ds. ochrony danych osobowych.

EIOD wziął udział w sesji poświeconej „Ochronie danych w instytucjach UE". Wśród innych tematów, które omawiano podczas konferencji, były: „elektroniczna dokumentacja zdrowotna", „ochrona danych – dalsze działania", „ochrona danych w trzecim filarze", „media a ochrona danych osobowych", „dzieci a dane osobowe" oraz inne sprawy bieżące. Na konferencji przyjęto także kilka istotnych dokumentów (zob. pkt 4.4).

Kolejną konferencję europejską zaplanowano w Rzymie w dniach 17–18 kwietnia 2008 r. w celu podsumowania istotnych zagadnień wymagających uwagi.

Przedstawiciele personelu uczestniczyli w warsztatach poświęconych rozpatrywaniu spraw; zorganizowano je w Helsinkach i Lizbonie w kwietniu i listopadzie 2007 r. Ten interesujący mechanizm współpracy na poziomie personelu, służący wymianie najlepszych wzorców wśród europejskich organów ds. ochrony danych, działa już dziewiąty rok. Kolejne warsztaty poświęcone rozpatrywaniu spraw zaplanowano na marzec 2008 r. w Lublanie.

4.6. Konferencja międzynarodowa

Przedstawiciele organizacji ds. ochrony danych oraz komisarze ds. ochrony prywatności z Europy i innych części świata, w tym z Kanady, Ameryki Łacińskiej, Australii, Nowej Zelandii, Hongkongu, Japonii i innych jurysdykcji w regionie Azji i Pacyfiku od wielu lat spotykają się jesienią na corocznej konferencji. 29. Międzynarodowa Konferencja Komisarzy ds. Ochrony Danych i Prywatności odbyła się w Montrealu w dniach 25–28 września 2007 r.; jej gospodarzem był kanadyjski komisarz ds. ochrony prywatności. W konferencji wzięli udział liczni delegaci z około 60 państw z całego świata.

Temat konferencji („Perspektywy prywatności: *terra incognita*") koncentrował się na wielu trudnych zagadnieniach, którymi zajmują się komisarze ds. ochrony danych i prywatności. Do głównych wyzwań (nazywanych „smokami") należą następujące zagadnienia: „bezpieczeństwo publiczne", „globalizacja", „prawo a technologia", „wszechobecna komputeryzacja", „następne pokolenie" oraz „ciało jako źródło danych". Na niektórych warsztatach analizowano możliwe odpowiedzi, określane jako „pogromcy smoków", a wśród nich: „oceny oddziaływania na sferę prywatności", „audyty" i „kształcenie dzieci dotyczące prywatności".

W konferencji tej uczestniczył EIOD i jego zastępca. EIOD przewodniczył sesji zamkniętej z udziałem komisarzy, poświęconej inicjatywie londyńskiej (zob. pkt 4.7); wziął również udział w warsztatach poświęconych globalizacji.

Na konferencji przyjęto trzy rezolucje ([69]):
- na temat pilnej potrzeby ustanowienia światowych norm ochrony danych pasażerów, stosowanych przez rządy do celów związanych z egzekwowaniem prawa i bezpieczeństwem granic;
- na temat wypracowania międzynarodowych norm (rezolucja wzywająca do ściślejszego zaangażowania mechanizmów ISO);
- na temat współpracy międzynarodowej (m.in. transgranicznego egzekwowania prawa i inicjatyw dotyczących zwiększania świadomości w zakresie ochrony danych)

Kolejna międzynarodowa konferencja jest zaplanowana na 15–17 października 2008 r. w Strasburgu; gospodarzami będą: francuski organ ds. ochrony danych (CNIL) oraz federalny komisarz ds. ochrony danych i wolności informacji z Niemiec.

4.7. Inicjatywa londyńska

Na 28. międzynarodowej konferencji w Londynie w listopadzie 2006 r. przedstawiono oświadczenie zatytułowane „Przekazywanie informacji na temat ochrony danych i zwiększanie efektywności tego procesu", które spotkało się z ogólnym poparciem organów ds. ochrony danych na całym świecie. Była to wspólna inicjatywa prezesa francuskiego organu ds. ochrony danych, brytyjskiego komisarza ds. informacji oraz EIOD (zwana od tamtej pory „inicjatywą londyńską"). EIOD jako jeden z twórców inicjatywy będzie aktywnie uczestniczył w monitorowaniu stosownych działań wraz z krajowymi organami ds. ochrony danych ([70]).

W kontekście inicjatywy londyńskiej w lutym 2007 r. prezes CNIL zorganizował w Paryżu warsztaty na temat zagadnień związanych z przekazywaniem informacji. Ich rezultatem było utworzenie sieci kontaktowej urzędników ds. informacji, umożliwiającej im wymianę doświadczeń i najlepszych wzorców w dziedzinie, którą się zajmują (zob. także pkt 5.1).

([69]) Dostępne na stronie internetowej EIOD: część „Cooperation", zakładka „International Conference".

([70]) Zob. sprawozdanie roczne za rok 2006, pkt 4.5 i 5.1.

W kwietniu 2007 r. EIOD zorganizował w Brukseli warsztaty na temat zagadnień dotyczących egzekwowania prawa. Podczas tych warsztatów zajmowano się trzema głównymi kwestiami, mianowicie:
- działaniami organów ds. ochrony danych w zakresie kontroli i audytu,
- wspomaganiem egzekwowania prawa z zastosowaniem interwencji i kar,
- możliwościami w zakresie transgranicznego egzekwowania prawa.

Przy tej ostatniej kwestii wykorzystano pożyteczne prace przeprowadzone przez Organizację Współpracy Gospodarczej i Rozwoju (OECD). Uwidocznił się coraz większy udział organów ds. ochrony danych w egzekwowaniu prawa. Wspomniane warsztaty pozwoliły zwrócić uwagę na cenne doświadczenia i najlepsze wzorce w tej dziedzinie.

Na międzynarodowej konferencji w Montrealu (zob. pkt 4.6) EIOD przewodniczył sesji zamkniętej z udziałem komisarzy, poświęconej inicjatywie londyńskiej. Omówiono możliwości podjęcia dalszych działań, zarówno w UE, jak i w regionie Azji i Pacyfiku. Świadczy to o tym, że inicjatywa londyńska ma mieć rzeczywiście światowy wymiar.

W grudniu 2007 r. brytyjski komisarza ds. informacji zorganizował w Londynie warsztaty koncentrujące się na skutecznej strategii organów ds. ochrony danych. Warsztaty poświęcone były kwestiom istotnym z punktu widzenia planowania strategicznego oraz takiemu sposobowi określania priorytetów, który zapewni skuteczność działań („działać wybiórczo, ale skuteczniej").

EIOD wyraża zadowolenie z faktu, że wspomniane warsztaty przyczyniają się do bardziej skutecznej ochrony danych oraz do znalezienia praktycznych sposobów osiągnięcia tego strategicznego celu.

4.8. Organizacje międzynarodowe

Organizacje międzynarodowe w wielu przypadkach są zwolnione ze stosowania prawa krajowego. W rezultacie często brakuje ram prawnych ochrony danych, nawet co do takich spraw, które wiążą się z gromadzeniem wysoce wrażliwych danych lub ich wymianą między organizacjami. Sprawę tę poruszono podczas międzynarodowej konferencji w Sydney w 2003 r., gdzie wydano rezolucję wzywającą, by „organy mię-

dzynarodowe i ponadnarodowe oficjalnie zobowiązały się do […] stosowania głównych międzynarodowych instrumentów dotyczących ochrony danych i prywatności".

We wrześniu 2005 r. EIOD zorganizował wspólnie z Radą Europy i OECD warsztaty, których tematem była ochrona danych jako element dobrego zarządzania organizacjami międzynarodowymi. Miały one na celu zwiększenie świadomości w zakresie uniwersalnych zasad ochrony danych i ich konsekwencji dla organizacji międzynarodowych. Przedstawiciele około 20 organizacji wzięli udział w dyskusjach na temat ochrony danych osobowych personelu i innych odnośnych osób. Zajmowano się również kwestią przetwarzania wrażliwych danych dotyczących zdrowia, statusu uchodźcy i wyroków karnych.

EIOD udzielił wsparcia drugiej edycji warsztatów zorganizowanej w Monachium w marcu 2007 r. przez Europejski Urząd Patentowy. Przedstawiciele różnych organizacji międzynarodowych omówili istotne dla wszystkich uczestników zagadnienia, takie jak rola urzędników ds. ochrony danych, sposoby tworzenia systemu ochrony danych oraz współpraca międzynarodowa z podmiotami stosującymi odmienne standardy ochrony danych.

Rozważana jest możliwość zorganizowania trzeciej edycji warsztatów w 2008 r. lub 2009 r.

5. Komunikacja

5.1. Wprowadzenie

Działalność w zakresie przekazywania informacji nadal odgrywa kluczową rolę w strategii i bieżącej pracy omawianej instytucji. Wprawdzie działalność ta nie należy do głównych zadań EIOD, które omówiono w poprzednich rozdziałach, nie da się jednak przecenić jej wielkiego znaczenia dla praktycznych skutków realizacji tych zadań. Sprawdza się to na wielu poziomach. Elementarna **świadomość w zakresie ochrony danych** jest warunkiem koniecznym do tego, by ochrona ta zawsze była należyta i skuteczna. Podmioty danych muszą mieć świadomość swoich określonych praw, zanim będą mogły z nich skutecznie korzystać. Odpowiedzialni administratorzy danych muszą znać swoje obowiązki, aby móc zapewnić przestrzeganie zasad ochrony danych. Zainteresowane podmioty instytucjonalne muszą być świadome konsekwencji, jakie ich polityka może mieć dla ochrony danych osobowych, oraz dziedzin, w których ochrona danych może przyczynić się do większej legitymizacji i lepszych rezultatów. Przekazywanie informacji to również ważne narzędzie służące przejrzystości polityk i działań EIOD.

EIOD był jednym z głównych twórców **inicjatywy londyńskiej**, mającej na celu usprawnienie informowania o ochronie danych i samej ochrony danych (zob. także pkt 4.7). W lutym 2007 r. w ramach monitorowania tej inicjatywy EIOD aktywnie uczestniczył w warsztatach poświęconych przekazywaniu informacji zorganizowanych przez francuski organ ds. ochrony danych (CNIL). Jednym z ich istotnych rezultatów było utworzenie **sieci urzędników ds. informacji** (obejmującej EIOD). Organy ds. ochrony danych będą mogły wykorzystywać tę sieć do wymiany najlepszych wzorców i do realizowania określonych projektów, takich jak podejmowanie wspólnych działań przy okazji istotnych wydarzeń.

Innym zasadniczym elementem świadomości w zakresie ochrony danych jest **współpraca między urzędnikami ds. ochrony danych** w instytucjach i organach UE. Ścisła współpraca między tymi urzędnikami jest twórczą metodą udostępniania dobrych wzorców i skutecznej wspólnej pracy na rzecz zwiększania świadomości w zakresie problematyki ochrony danych wśród zainteresowanych stron z UE i wśród personelu UE. EIOD chciałby kontynuować tę współpracę przez stymulowanie wspólnych działań i inicjatyw, na przykład w kontekście wydarzeń takich jak Dzień Ochrony Danych. Wspólna praca prowadzona w tak spójny sposób umożliwia pełne wykorzystanie potencjału działań informacyjnych.

W niniejszym rozdziale wymieniono działania w zakresie przekazywania informacji, przeprowadzone przez EIOD w 2007 r., które obejmowały pracę służby prasowej, wykorzystywanie i rozwijanie narzędzi do udostępniania informacji w Internecie (takich jak strona internetowa i biuletyn elektroniczny), udział w warsztatach i konferencjach, udzielanie wywiadów, wizyty, konferencje prasowe, a także kontakty z mediami (np. polegające na publikowaniu odpowiednich materiałów informacyjnych i na regularnych kontaktach z dziennikarzami).

5.2. Aspekty działań informacyjnych

Polityka informacyjna EIOD musi być kształtowana z uwzględnieniem aspektów, które mają znaczenie ze względu na krótki czas działania tej instytucji, jej rozmiar i zakres kompetencji. Opiera się ona zatem na podejściu dostosowanym do potrzeb i wykorzystuje właściwe narzędzia, aby dotrzeć do odpowiednich odbiorców, a jednocześnie jest w stanie dostosować się do rozmaitych ograniczeń i wymogów.

Odbiorcy

W odróżnieniu od większości pozostałych instytucji i organów UE, których polityki i działania informacyjne muszą funkcjonować na poziomie ogólnym i skierowane są do wszystkich obywateli UE, bezpośredni zakres działań EIOD jest wyraźnie węższy. Zasadniczo skupia się on na instytucjach i organach UE, podmiotach danych w ogóle, a w szczególności na personelu UE, zainteresowanych podmiotach politycznych z UE, a także „partnerach zajmującymi się ochroną danych". Dlatego polityka informacyjna EIOD nie musi być częścią strategii „komunikacji masowej". Uświadamianie obywateli UE w państwach członkowskich w zakresie problematyki ochrony danych opiera się na bardziej pośrednim podejściu – bazującym głównie na pośrednictwie organów ds. ochrony danych na poziomie krajowym – oraz na wykorzystywaniu ośrodków informacyjnych i punktów kontaktowych.

EIOD przyciąga jednak uwagę ogółu społeczeństwa, w szczególności przez wykorzystanie różnych narzędzi informacyjnych (strona internetowa, biuletyn elektroniczny i inne materiały informacyjne), regularne kontakty z zainteresowanymi stronami (np. wizyty studentów u EIOD) oraz udział w wydarzeniach publicznych, posiedzeniach i konferencjach.

Zastosowanie odpowiedniego języka

Polityka informacyjna EIOD musi również uwzględniać złożoność obszaru działalności tej instytucji.

Problematyka ochrony danych może być w istocie postrzegana jako zbyt techniczna i niejasna dla laika, a język stosowany do informowania powinien zostać odpowiednio dostosowany, w szczególności jeżeli chodzi o narzędzia informacyjne skierowane do wszystkich grup odbiorców, takie jak strona internetowa czy broszury informacyjne. Przy tego rodzaju materiałach informacyjnych, a także przy redagowaniu odpowiedzi na kierowane przez obywateli prośby o informacje konieczne jest stosowanie jasnego i zrozumiałego stylu oraz unikanie żargonu, gdy nie jest on niezbędny.

W przypadku bardziej wyspecjalizowanych odbiorców (media, specjaliści w zakresie ochrony danych, zainteresowane podmioty z UE itd.) stosowanie terminów technicznych i prawnych jest bardziej celowe. W tym sensie może być konieczne przekazywania tych samych wiadomości przy użyciu dostosowanej formy i stylu, odpowiadających odbiorcom docelowym (ogół społeczeństwa a odbiorcy bardziej wyspecjalizowani).

Wpływ

Aby zapewnić jak największą skuteczność, styl informacyjny stosowany przez EIOD opiera się na zasadzie: „nadmiar informacji osłabia przekaz", która sugeruje, by unikać zalewu informacjami. Wykorzystanie tradycyjnych narzędzi informowania (komunikatów prasowych, biuletynów) jest celowo ograniczane do kwestii o większym znaczeniu – do sytuacji, gdy uznaje się, że konieczne i właściwe jest zareagowanie i poinformowanie jak najszerszego kręgu odbiorców.

Eksponowanie roli EIOD

W pierwszych latach funkcjonowania EIOD jego działalność w zakresie przekazywania informacji była wyraźnie ukierunkowana na większe wyeksponowanie tej niedawno utworzonej instytucji na politycznej mapie UE. W stosunkowo krótkim czasie dużo zrobiono, by osiągnąć ten cel. Obecnie, trzy lata po rozpoczęciu prac w tej dziedzinie, widać pozytywne skutki tej działalności informacyjnej.

Jednym z przykładów na to jest fakt, że EIOD znalazł się w gronie 50 nominowanych w 2007 r. przez „European Voice" do nagrody **Europejczyka Roku**; celem tej nagrody jest wyróżnienie najważniejszych osobistości europejskich za ich wkład w realizację programu UE w danym roku. Peter Hustinx zdobył uznanie za to, że „przyjął bardziej aktywną rolę i nie wahał się zabierać głosu, nawet w odniesieniu do drażliwych kwestii polityki bezpieczeństwa" ([71]). Uznanie to świadczy o tym, że wzrosła wiedza na temat działań EIOD i jego stanowiska w newralgicznych kwestiach z zakresu ochrony danych, które należą do najważniejszych punktów programu politycznego UE.

Ponadto odnotowany w 2007 r. wzrost liczby wniosków o udzielenie informacji i porad otrzymywanych codzienne przez służbę prasową EIOD (zob. pkt 5.5) stanowi dodatkowe potwierdzenie opinii, że EIOD stał się punktem odniesienia w kwestiach dotyczących ochrony danych.

([71]) Zob. s. 45 magazynu: Presenting the EV50 2007: http://www.ev50.org/prs/EV50_Magazine_2007-pages28-54.pdf.

5.3. Wystąpienia

W ciągu całego roku EIOD nadal poświęcał wiele czasu i wysiłku na to, by objaśnić swoje zadania oraz propagować wiedzę o ochronie danych w ogóle, a także o szeregu konkretnych zagadnień, występując publicznie i podejmując inne podobne formy aktywności w różnorodnych instytucjach i w różnych państwach członkowskich.

EIOD był często obecny na posiedzeniach Komisji Parlamentu Europejskiego ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) lub uczestniczył w podobnych wydarzeniach. W dniu 27 lutego przedstawił swoją opinię w sprawie wniosku dotyczącego decyzji Rady ustanawiającej Europejski Urząd Policji (Europol). W dniu 26 marca przemawiał na publicznym seminarium na temat PNR, SWIFT, „zasad bezpiecznej przystani" oraz transatlantyckiej ochrony danych. W dniu 27 marca wziął udział w seminarium dotyczącym wspólnych instrukcji konsularnych i wykorzystywania biometrii. W dniu 10 kwietnia zabrał głos podczas wysłuchania publicznego na temat przyszłości Europolu. W dniu 11 kwietnia przedstawił swoją opinię na temat inicjatywy w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną, opartej na konwencji z Prüm. W dniu 7 maja zabrał głos podczas wysłuchania publicznego na temat „decyzji w sprawie konwencji z Prüm". W dniu 8 maja przedstawił swoją trzecią opinię na temat wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych w trzecim filarze. W dniu 14 maja złożył sprawozdanie roczne za 2006 r. W dniu 21 listopada przedstawił uwagi na temat ogólnego podejścia Rady do ochrony danych w trzecim filarze. W dniu 11 września na wspólnym wysłuchaniu Komisji ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) i Komisji Prawnej (JURI) zastępca EIOD przedstawił opinię EIOD na temat zobowiązań alimentacyjnych, a w dniu 8 października zabrał głos na publicznym seminarium komisji LIBE na temat wielopoziomowej ochrony praw podstawowych.

W dniu 16 stycznia EIOD przedstawił Grupie Roboczej Rady ds. Ochrony Danych swoje priorytety w zakresie konsultacji dotyczących nowego prawodawstwa. W dniu 4 maja przebywał w Berlinie, gdzie wziął udział w dyskusjach z prezydencją niemiecką na temat ochrony danych w pierwszym i trzecim filarze. W dniu 7 maja dyskusje te kontynuowano w Brukseli,

Peter Hustinx podczas prezentacji przygotowanej dla Europejskiego Stowarzyszenia Marketingu i Zarządzania Finansami

koncentrując się na ochronie danych w trzecim filarze. W dniu 24 maja EIOD przedstawił swoje sprawozdanie roczne za 2006 r. Grupie Roboczej Rady ds. Ochrony Danych. W dniu 4 września na seminarium zorganizowanym w Lizbonie przez Strategiczny Komitet ds. Imigracji, Granic i Azylu (SCIDA) wygłosił przemówienie na temat „Kwestii etycznych związanych w wykorzystywaniem biometrii". W dniu 13 marca zastępca EIOD przedstawił opinię EIOD w sprawie Europolu Grupie Roboczej Rady ds. Europolu.

Na liście kontaktów znalazły się również inne instytucje i organy UE. W dniu 22 marca EIOD i jego zastępca przemawiali na posiedzeniu z udziałem sekretarza generalnego i dyrektorów generalnych Komisji Europejskiej poświęconym przestrzeganiu przepisów rozporządzenia (WE) nr 45/2001. W dniu 26 kwietnia EIOD zabrał głos podczas posiedzenia plenarnego wspólnego organu nadzorczego Eurojustu. W dniu 11 czerwca przemawiał na posiedzeniu szefów agencji, które dotyczyło przestrzegania przepisów rozporządzenia (WE) nr 45/2001. W dniu 12 lipca EIOD i zastępca EIOD przedstawili w Eurojuscie informacje na temat kwestii związanych z trzecim filarem. W dniu 7 grudnia EIOD spotkał się z personelem Biura Europejskiego Rzecznika Praw Obywatelskich w Strasburgu. W dniu 19 kwietnia na posiedzeniu kolegium szefów administracji zastępca EIOD dokonał prezentacji na temat zatrzymywania danych medycznych, a w dniu 24 kwietnia przedstawił zadania i uprawnienia EIOD na posiedzeniu zgromadzenia komitetów personelu agencji UE, które odbyło się w Torrejon de Ardoz (Hiszpania).

W ciągu tego roku EIOD odwiedził także szereg państw członkowskich. W dniu 8 lutego przemawiał w Ministerstwie Sprawiedliwości Niderlandów w Hadze. W dniu 2 kwietnia w Atenach zabrał głos na sympozjum poświęconym niezależnym organom. W dniu 10 maja w Larnace (Cypr) przemawiał na wiosennej konferencji europejskich komisarzy ds. ochrony danych. W dniu 15 maja w Brukseli przedstawił prezentację podczas seminarium na temat zaawansowanych systemów ID. W dniu 24 maja wygłosił przemówienie dotyczące strategicznych kwestii z zakresu ochrony danych na konferencji „European Data Protection Intensive" w Amsterdamie. W dniu 7 czerwca w Brukseli zabrał głos na konferencji na temat przestrzegania prawa farmaceutycznego. W dniu 21 czerwca przedstawił prezentację na temat roli EIOD na forum Rady Adwokackiej w Atenach. W dniu 26 czerwca w Berlinie przemawiał na konferencji poświęconej identyfikacji radiowej.

W dniach 2–3 lipca EIOD wygłosił przemówienia na zorganizowanej w Cambridge (Zjednoczone Królestwo) konferencji pod hasłem „Prawo do prywatności a biznes". W dniu 6 lipca przebywał z wizytą w Instytucie Spraw Europejskich w Dublinie. W dniu 13 lipca wziął udział w seminarium na temat ochrony danych w Sofii. W dniu 24 sierpnia w Cambridge (USA) wygłosił przemówienie na seminarium dotyczącym prywatności. W dniu 6 września przedstawił w Londynie prezentację dla Forum Ochrony Danych w Zjednoczonym Królestwie. W dniu 14 września przemawiał na seminarium na temat współpracy sądowej zorganizowanym w Strasburgu przez Radę Europy. W dniu 19 września w Paryżu wygłosił przemówienie na konferencji poświęconej kartom płatniczym. W dniu 20 września zabrał głos na seminarium EurActiv w Brukseli. W dniu 27 września wygłosił przemówienie na Międzynarodowej Konferencji Komisarzy ds. Ochrony Danych i Prywatności w Montrealu.

W dniu 2 października przemawiał na seminarium zorganizowanym przez europejskie forum biometrii (European Biometrics Forum) w Brukseli. W dniu 10 października w Brukseli zabrał głos podczas panelu dyskusyjnego zorganizowanego przez Centrum Europejskich Studiów Politycznych (Centre for European Policy Studies – CEPS) i firmę Google, dotyczącego prywatności w Internecie. W dniu 11 października wziął udział w zorganizowanej w Londynie konferencji na temat przestrzegania ochrony danych. W dniu 13 października wygłosił przemówienie na temat roli organów ds. ochrony danych na zorganizowanej w Brukseli międzynarodowej konferencji pod hasłem „Re-inventing data protection" (Nowe spojrzenie na ochronę danych). W dniu 22 października przemawiał na konferencji pod hasłem „Prawo do prywatności w społeczeństwie kontrolowanym", którą zorganizowano w Warszawie. W dniu 26 października zabrał głos w sprawie SIS II na konferencji szwajcarskich organów ds. ochrony danych, zorganizowanej w Solothurn. W dniu 13 listopada wziął udział w konferencji litewskich urzędników ds. ochrony danych, która odbyła się w Wilnie. W dniu 15 listopada przemawiał na zorganizowanej w Lizbonie konferencji poświęconej identyfikacji radiowej. W dniu 10 grudnia zabrał głos na seminarium na temat bezpieczeństwa danych zorganizowanym w Brukseli przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji.

Zastępca EIOD przedstawił podobne prezentacje. W dniu 30 stycznia na seminarium zorganizowanym w Barcelonie z okazji Dnia Ochrony Danych dokonał prezentacji nowych wniosków prawodawczych w UE. W dniu 16 lutego w Brukseli przemawiał na zorganizowanym przez CEPS seminarium na temat mobilności, kontroli i nowych technologii. W dniu 22 marca zabrał głos na forum jednej z komisji Izby Lordów na temat PNR i konwencji z Prüm. W dniu 1 czerwca wziął udział w warsztatach poświęconych prywatności i zwalczaniu terroryzmu, które zorganizowane zostały w Strasburgu przez Komisarza Praw Człowieka Rady Europy. W dniu 6 lipca przemawiał na dorocznej konferencji CEPS na temat kontroli demokratycznej i odpowiedzialności sądowej prawników w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W dniach 12–14 września przedstawił kilka prezentacji podczas zorganizowanych przez Radę Europy seminariów dotyczących ochrony danych i współpracy sądowej, a w dniu 12 września zabrał głos na regionalnej europejskiej konferencji UNESCO–Rada Europy poświęconej etyce i prawom człowieka w społeczeństwie informacyjnym. W dniu 5 października w Madrycie przedstawił prezentację na temat projektu decyzji ramowej w sprawie ochrony danych w trzecim filarze. W dniu 10 października przemawiał na 9. posiedzeniu plenarnym sieci lizbońskiej (zrzeszającej prawne instytucje szkoleniowe) Rady Europy. W dniu 23 października w Bilbao wygłosił przemówienie zatytułowane: „Publiczny dostęp do dokumentów a ochrona danych".

5.4. Służba prasowa

W 2007 r. w służbie prasowej odnotowano pewien brak ciągłości w związku z mobilnością personelu, mimo że podjęto działania wewnętrzne, aby utrzymać tempo prowadzonych prac informacyjnych. W grudniu 2007 r. zatrudniono nowego rzecznika prasowego, aby zapewnić stabilność oraz rozwój praktyki zawodowej w zakresie działań związanych z prasą i działalności informacyjnej.

Służba prasowa odpowiada za zewnętrzną komunikację z mediami, polegającą na regularnych kontaktach z dziennikarzami. Zajmuje się również wnioskami o udzielenie informacji i porad, redagowaniem komunikatów prasowych i biuletynów, a także organizowaniem konferencji prasowych i wywiadów udzielanych przez EIOD i jego zastępcę. Ponadto rzecznik prasowy kieruje elastycznym zespołem ds. informacji, który bierze udział w działaniach i wydarzeniach o charakterze promocyjnym (w szczególności Dzień Ochrony Danych i dni otwartych drzwi w instytucjach europejskich; zob. pkt 5.8) oraz w przygotowywaniu materiałów informacyjnych skierowanych do społeczeństwa i dziennikarzy.

W 2007 r. służba prasowa wydała 14 komunikatów prasowych, czyli średnio w całym roku co miesiąc ukazywał się jeden komunikat. Większość z tych komunikatów dotyczyła nowych opinii w sprawie aktów prawnych mających istotne znaczenie z punktu widzenia ogółu społeczeństwa. Dotyczyły one m.in. następujących zagadnień: postulowanej decyzji ramowej w sprawie ochrony danych w trzecim filarze, kontroli i audytu Eurodac, wdrażania dyrektywy 95/46/WE o ochronie danych, postulowanego rozporządzenia dotyczącego transportu drogowego, identyfikacji radiowej (RFID), przepisów wykonawczych do konwencji z Prüm oraz propozycji UE w sprawie danych dotyczących przelotu pasażera (PNR).

Zespół ds. informacji podczas przygotowywania materiałów informacyjnych

Peter Hustinx i Joaquín Bayo Delgado przedstawiają na konferencji prasowej roczne sprawozdanie za rok 2006

Komunikaty prasowe są publikowane na stronie internetowej EIOD oraz rozsyłane do członków regularnie aktualizowanej sieci kontaktowej dziennikarzy i zainteresowanych podmiotów. Informacje dostarczane w postaci komunikatów prasowych są zazwyczaj podstawą istotnych relacji w mediach – ukazują się w prasie ogólnej i specjalistycznej, oprócz tego publikowane są na instytucjonalnych i pozainstytucjonalnych stronach internetowych, w tym m.in. na stronach instytucji i organów UE, organizacji pozarządowych, instytucji naukowych i firm informatycznych.

Na początku maja 2007 r. zorganizowano konferencję prasową, na której przedstawiono sprawozdanie roczne za 2006 r. Na tej konferencji podkreślono, że w ciągu trzech lat działalności zadania EIOD związane z nadzorem i działaniami konsultacyjnymi uległy rozszerzeniu oraz że od administracji UE oczekuje się obecnie dowodów na to, iż poczyniła ona „istotne postępy w wypełnianiu zobowiązań w zakresie ochrony danych".

5.5. Wnioski o udzielenie informacji i porad

W stosunku do 2006 r. liczba wniosków o udzielenie informacji i porad w 2007 r. utrzymywała się na stałym poziomie (około 160 wniosków w 2007 r.

w porównaniu do 170 w 2006 r.). Wnioski o udzielenie informacji i porad pochodziły od różnych osób i podmiotów, m.in. od zainteresowanych stron, które działają w środowisku unijnym lub których praca wiąże się z ochroną danych (firmy prawnicze, firmy konsultingowe, stowarzyszenia, wyższe uczelnie itd.), oraz od obywateli zwracających się o dodatkowe informacje dotyczące problematyki ochrony danych lub o naszą pomoc w rozwiązaniu wątpliwości lub problemów napotykanych w praktyce.

Znaczną większość tych wniosków sklasyfikowano jako **wnioski o informacje** – jest to szeroka kategoria, która obejmuje ogólne pytania dotyczące polityk i prawodawstwa UE, ale także bardziej szczegółowe pytania związane z ochroną danych w państwach członkowskich oraz w administracji UE. W 2007 r. otrzymano na przykład wnioski o informacje dotyczące: kwestii bezpieczeństwa związanych z danymi osobowymi, technologii biometrycznych, prywatności w Internecie, przekazywania danych osobowych do państw trzecich, dostępu do danych osobowych będących w dyspozycji EPSO, a także wdrażania dyrektywy 95/46/WE w państwach członkowskich.

Wnioski, które wykraczają poza aspekt informacyjny i wymagają w związku z tym bardziej szczegółowej analizy, klasyfikuje się jako **wnioski o poradę**. W 2007 r. stanowiły one zdecydowaną mniejszość (mniej niż 5% wniosków); zazwyczaj zajmują się nimi urzędnicy odpowiedzialni za konkretną sprawę. O porady zwracali się głównie urzędnicy zajmujący się, bezpośrednio lub pośrednio, problematyką ochrony danych w instytucjach i agencjach UE. Nie obejmuje to oczywiście poważniejszych konsultacji na temat środków administracyjnych (zob. pkt 2.7).

Wnioski o poradę otrzymane w 2007 r. dotyczyły publicznego dostępu do list dopuszczonych kandydatów w procedurach Parlamentu Europejskiego, warunków wyznaczania urzędników ds. ochrony danych, a także zasad ochrony danych, które mają być przestrzegane przy publikowaniu na stronie internetowej zdjęć osób uczestniczących w danym wydarzeniu.

Podobnie jak w latach poprzednich większość otrzymanych wniosków sporządzona została w języku angielskim, w mniejszym stopniu – w języku francuskim. Dzięki temu służba prawna szybko udzielała odpowiedzi, bez problemu mieszcząc się w limicie 15 dni roboczych. Część otrzymanych wniosków została jednak sporządzona w innych językach urzędowych UE, co sprawiło, że czasem potrzebna była pomoc służby tłumaczeniowej Rady. W takich wypadkach zarówno wniosek, jak i odpowiedź musiały zostać przetłumaczone, tak by autor wniosku mógł uzyskać odpowiednie informacje w języku ojczystym.

5.6. Internetowe narzędzia informacyjne

Zmiany na stronie internetowej

Strona internetowa EIOD pozostaje najważniejszym narzędziem informacyjnym. Jest ona również środkiem, który umożliwia odwiedzającym wgląd do wszelkich różnorodnych dokumentów sporządzonych w ramach działań EIOD (opinii, uwag, priorytetów pracy, publikacji, przemówień, komunikatów prasowych, biuletynów, informacji na temat wydarzeń itd.).

W lutym 2007 r. uruchomiono nową wersję strony internetowej EIOD. Wykorzystuje ona system zarządzania treścią serwisów internetowych (WCMS), który ułatwia zarządzanie dużą liczbą dokumentów.

Strona powitalna, dostępna we wszystkich językach Wspólnoty, zawiera ogólne informacje na temat EIOD i jego głównych zadań. Pozostałe strony są obecnie dostępne w wersji angielskiej i francuskiej. Jednak wiele dokumentów udostępnionych na stronie występuje we wszystkich językach Wspólnoty.

Strona główna nowego portalu Europejskiego Inspektora Ochrony Danych

Stronę internetową podzielono na 4 części.

- Pierwsza część („The EDPS") zawiera ogólne informacje na temat EIOD, jego zastępcy oraz ich misji, szczegółowego prawodawstwa UE dotyczącego ochrony danych, a także publikacji EIOD – m.in. sprawozdanie roczne, nowości i dane kontaktowe.
- Podział na pozostałe części odzwierciedla podział głównych zadań EIOD. Część „Supervision" zawiera informacje i dokumenty na temat monitorowania operacji przetwarzania danych prowadzonych przez administracje UE. Zawiera ona między innymi dużą liczbę opinii EIOD wydanych w związku z powiadomieniami wystosowywanymi przez instytucje i dotyczącymi operacji przetwarzania stwarzających szczególne zagrożenia. Część „Consultation" poświęcona jest doradczej roli EIOD. Opinie na temat proponowanego prawodawstwa publikowane są w Dzienniku Urzędowym i dostępne we wszystkich językach Wspólnoty w zakładce „Opinions". W części „Cooperation" przedstawiono prace podejmowane w ścisłej współpracy z krajowymi organami ds. ochrony danych, w większości na poziomie europejskim lub międzynarodowym.

Dodatkowe funkcje na stronie internetowej, takie jak rejestr powiadomień utworzony w 2007 r., udostępnione zostaną w 2008 r. Planuje się również inne narzędzia informacyjne – takie ja FAQ i glosariusz – dzięki którym treść strony zostanie dopracowana i będzie lepiej spełniać oczekiwania odwiedzających.

Służba prasowa EIOD nadal uczestniczyła w pracach Międzyinstytucjonalnego Komitetu ds. Redagowania Treści Internetowych (Interinstitutional Internet Editorial Committee – CEiii), by śledzić na bieżąco najnowsze osiągnięcia w dziedzinie technologii tworzenia stron internetowych.

Biuletyn

Biuletyn EIOD dostarcza informacje na temat działań podejmowanych w ostatnim czasie przez tę instytucję, takich jak wydawanie opinii dotyczących wniosków prawodawczych UE oraz opinii na temat kontroli wstępnych, a także stosowne informacje źródłowe i dotyczące kontekstu tych działań. Biuletyny dostępne są na stronie internetowej EIOD, na której można również zamówić automatycznie ich subskrypcję ([72]).

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

W 2007 r. opublikowano pięć wydań biuletynu EIOD; ukazywały się one średnio co dwa miesiące. Biuletyn jest dostępny się w języku angielskim i francuskim.

Liczba subskrybentów wzrosła z 460 osób pod koniec 2006 r. do 635 osób pod koniec 2007 r. Należą do nich między innymi posłowie do Parlamentu Europejskiego, pracownicy UE oraz krajowych organów ds. ochrony danych, a także dziennikarze, przedstawiciele środowiska akademickiego, firmy telekomunikacyjne i prawnicze. Utrzymujący się wyraźny wzrost liczby subskrybentów odnotowywany od ukazania się pierwszego biuletynu sprawił, że konieczne stało się rozważenie ulepszenia tej publikacji przez nadanie jej wyglądu, który byłby bardziej przyjazny dla odbiorcy. Dlatego rozważa się wprowadzenie takich zmian w 2008 r.

Biuletyn pozostaje efektywnym narzędziem umożliwiającym zwrócenie uwagi na nowości na stronie internetowej, a także zwiększenie wiedzy na temat działań podejmowanych w ostatnim czasie przez EIOD. Dzięki temu strona internetowa jest bardziej eksponowana i zachęca do kolejnych wizyt. Biuletyn jest również pożytecznym mechanizmem pozwalającym na tworzenie społeczności sieciowej zainteresowanej działalnością w zakresie ochrony danych na poziomie UE.

5.7. Kontakty z mediami i wizyty studyjne

EIOD udzielił blisko 20 wywiadów dziennikarzom reprezentującym prasę, rozgłośnie radiowe i telewizyjne oraz media elektroniczne z różnych państw członkowskich lub państw trzecich, w tym dziennikowi „Financial Times" i agencji Associated Press, a także stacjom radiowym lub telewizyjnym z Austrii, Danii, Niderlandów, Niemiec, Polski i ze Zjednoczonego Królestwa. Ponadto informacje na temat działalności EIOD często ukazywały się w czasopismach „European Voice" i „EU Reporter " oraz w wewnętrznych publikacjach różnych instytucji.

W ramach działań, których celem jest większe uwidocznienie EIOD, a także współdziałanie z kręgami akademickimi, EIOD gościł grupy studentów specjalizujących się w problematyce ochrony danych lub w kwestiach związanych z bezpieczeństwem systemów informatycznych. Na przykład w maju 2007 r. EIOD

przyjął grupę niemieckich studentów, z którymi omówił zagadnienia związane z ochroną danych w „społeczeństwie kontrolowanym". EIOD i jego zastępca wzięli również udział w Europejskich Dniach Młodych Dziennikarzy (European Youth Media Days) zorganizowanych w czerwcu 2007 r.

5.8. Działania promocyjne

Udział EIOD w działaniach dotyczących UE stanowi doskonałą okazję do zwiększania wiedzy na temat praw przysługujących podmiotom danych oraz na temat obowiązków instytucji i organów UE w zakresie ochrony danych.

Dzień Ochrony Danych

W 2007 r. Rada Europy zwróciła się do EIOD, instytucji UE oraz krajowych organów ds. ochrony danych o informacje na temat imprez, które zamierzają zorganizować w ramach pierwszego Europejskiego Dnia Ochrony Danych.

EIOD uruchomił stoiska informacyjne w Parlamencie Europejskim (25 stycznia 2007 r.) oraz w Komisji Europejskiej (26 stycznia 2007 r.), aby zwiększyć świadomość w zakresie problematyki ochrony danych wśród pracowników UE oraz ich wiedzę na temat działań EIOD.

EIOD wykorzystał tę okazję, by przekazać informacje na temat najważniejszych w owym czasie kwestii związanych z ochroną danych, takich jak dane dotyczące przelotu pasażera (dane PNR), SWIFT, system informacyjny Schengen, wizowy system informacyjny (VIS), zatrzymywanie danych telekomunikacyjnych oraz monitoring z użyciem kamer. Szczególną uwagę poświęcono prawom podmiotów danych.

Zaprojektowano plakat przedstawiający wymienione wyżej kwestie związane z ochroną danych. Osoby odwiedzające stanowisko EIOD zapraszano również do udziału w quizie na temat ochrony danych w instytucjach i organach UE. Rozlosowano nagrody (w tym przypadku pamięć USB z logo EIOD).

Obchody pierwszego Dnia Ochrony Danych w dniu 28 stycznia 2007 r., który niestety wypadał w niedzielę, zorganizowano z inicjatywy Rady Europy wspieranej przez Komisję Europejską. Jest to data upamiętniająca

Stoisko Europejskiego Inspektora Ochrony Danych w Komisji Europejskiej podczas Dnia Ochrony Danych (25 stycznia 2007 r.)

Pracownicy urzędu Inspektora przy stoisku w Parlamencie Europejskim podczas unijnego Dnia Otwartych Drzwi (5 maja 2007 r.)

otwarcie do podpisu Konwencji Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 1981 r. Konwencja ta była pierwszym prawnie wiążącym instrumentem międzynarodowym dotyczącym ochrony danych.

Dzień Otwartych Drzwi w instytucjach UE

W dniu 5 maja 2007 r. w Brukseli EIOD uczestniczył w Dniu Otwartych Drzwi w instytucjach UE zorganizowanym przez instytucje i organy UE, aby uczcić Dzień Europy (9 maja).

EIOD przygotował stoisko w siedzibie Parlamentu Europejskiego, a jego personel odpowiadał na pytania odwiedzających.

Odwiedzającym rozdawano różnorodne materiały informacyjne przedstawiające działalność EIOD, a także upominki promocyjne (długopisy, naklejki, kubki, pamięć USB z logo EIOD). Mieli oni również możliwość sprawdzenia swojej wiedzy na temat ochrony danych w krótkim quizie oraz wzięcia udziału w losowaniu nagród.

6. Administracja, budżet i personel

6.1. Wprowadzenie: rozwój nowej instytucji

Rozwój EIOD jako nowej instytucji ([73]) był kontynuowany, aby utrwalić osiągnięcia początkowego okresu jego działalności. W 2007 r. EIOD uzyskał **dodatkowe zasoby** zarówno budżetowe (wzrost z 4 138 378 euro do 4 955 726 euro), jak i osobowe (wzrost z 24 osób w 2006 r. do 29 w 2007 r.).

Otoczenie administracyjne jest stopniowo rozszerzane zgodnie z priorytetami ustalanymi na dany rok z uwzględnieniem potrzeb i rozmiarów instytucji. EIOD przyjął nowe przepisy wewnętrzne ([74]) niezbędne do prawidłowego funkcjonowania tej instytucji. Komitet pracowniczy ściśle angażuje się w proces przyjmowania przez EIOD ogólnych przepisów wykonawczych dotyczących regulaminu pracowniczego oraz innych przepisów wewnętrznych. W 2007 r. audytor wewnętrzny ogłosił zakończenie pierwszego audytu wewnętrznego.

Współpraca z innymi instytucjami – Parlamentem Europejskim, Radą i Komisją Europejską – uległa dalszej poprawie, co pozwoliło uzyskać znaczne korzyści skali. Rozwiązano częściowo problem wolnego tempa realizacji pewnych zadań związany z zasadą wzajemnej pomocy (głównie w zakresie dostępu do oprogramowania administracyjnego i finansowego). EIOD przejął pewne zadania, które pierwotnie wykonywane były przez inne instytucje.

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

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

Dział ds. Personelu, Budżetu i Administracji

6.2. Budżet

Budżet przyjęty przez władzę budżetową na 2007 r. wynosił 4 955 726 euro. Stanowi to wzrost o 19,8 % w porównaniu z budżetem na 2006 r.

W 2007 r. EIOD przygotował aktualizację swojej terminologii budżetowej do zastosowania przy ustalaniu budżetu na 2008 r. Opiera się ona na trzyletnim doświadczeniu EIOD, uwzględnia szczególne potrzeby tej instytucji oraz zapewnia przejrzystość wymaganą przez władzę budżetową.

W odniesieniu do wykonania swojego budżetu EIOD stosuje przepisy wewnętrzne Komisji w stopniu, w jakim przepisy te mają zastosowanie do struktury i skali EIOD, i w przypadku braku przepisów szczegółowych.

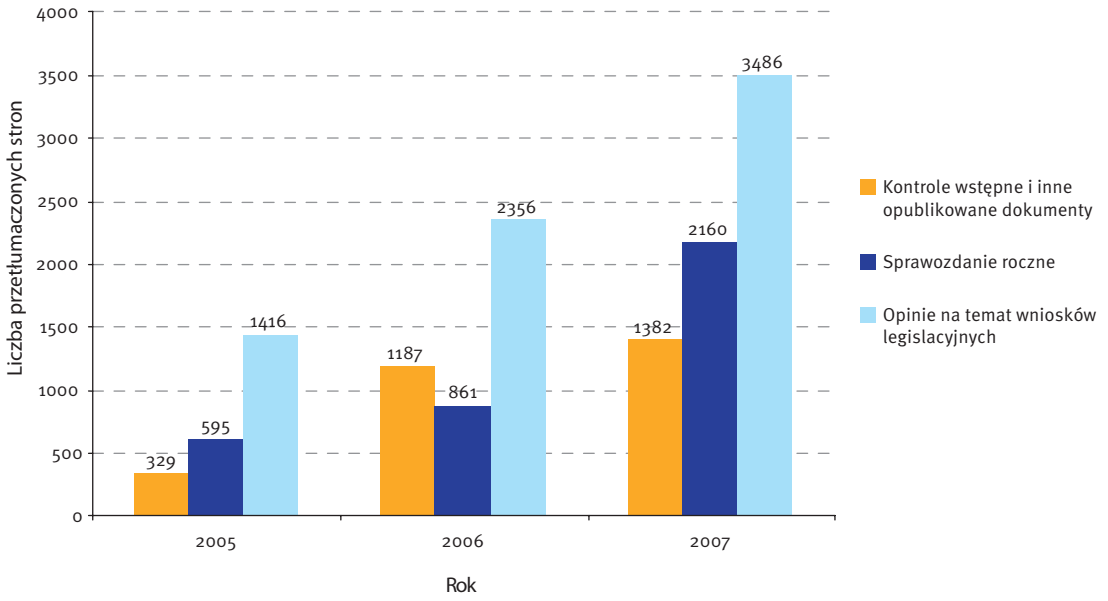


Tabela 1. Zmiana ilości tłumaczeń

Komisja nadal udzielała EIOD wsparcia, zwłaszcza w zakresie rachunkowości; księgowy Komisji został bowiem mianowany także księgowym EIOD. Jeśli chodzi o oprogramowanie finansowe, EIOD uzyskał bezpośredni dostęp do programu (ABAC Workflow) umożliwiającego przetwarzanie transakcji finansowych z jego siedziby.

W sprawozdaniu za rok budżetowy 2006 Trybunał Obrachunkowy stwierdził, że nie ma żadnych uwag po przeprowadzeniu kontroli.

Znaczna część budżetu przeznaczona jest na tłumaczenia, co ma istotny wpływ na prace administracyjne. Wydawane przez EIOD opinie na temat wniosków prawodawczych tłumaczone są na 22 języki urzędowe UE; tymczasowo nie dotyczy to języka irlandzkiego. Decyzje te publikowane są w Dzienniku Urzędowym Unii Europejskiej. W 2007 r. EIOD wydał 12 takich opinii. Od 2005 r. liczba opinii, podobnie jak liczba języków urzędowych, stale wzrasta. W rezultacie liczba stron do przetłumaczenia jest ponaddwukrotnie wyższa.

Opinie na temat kontroli wstępnych i inne publikowane dokumenty tłumaczone są zwykle tylko na języki robocze instytucji UE. W 2007 r. EIOD sporządził 151 oficjalnych dokumentów, które wymagały przetłumaczenia. Od 2005 r. liczba takich dokumentów wzrosła ponadtrzykrotnie.

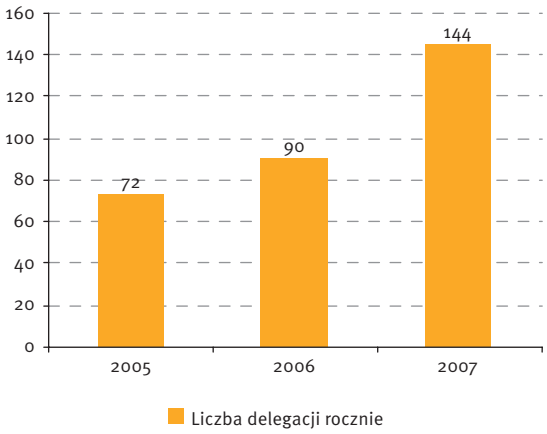


Tabela 2. Zmiana liczby delegacji

Liczba delegacji z udziałem członków i personelu EIOD wzrosła dwukrotnie od 2005 r. Jest to logiczną konsekwencją intensywniejszych działań tej instytucji. Zespół administracyjny zarządza stroną finansową delegacji; pomocy udziela mu Urząd Administrowania i Rozliczania Należności Indywidualnych (PMO).

6.3. Zasoby ludzkie

Jeśli chodzi o zadania w zakresie zarządzania personelem EIOD (składającym się z dwóch mianowanych członków i 29 członków personelu), instytucja ta korzysta ze skutecznej pomocy służb Komisji.

6.3.1. Rekrutacja

EIOD jako instytucja, która powstała niedawno, jest ciągle w fazie tworzenia i tak będzie jeszcze przez kilka najbliższych lat. Coraz większe uwidocznienie działalności EIOD oznacza dla niego większe obciążenie pracą, a także poszerzenie zakresu zadań. Na kwestię znacznego wzrostu obciążenia pracą w 2007 r. zwrócono uwagę w poprzednich rozdziałach. W tym kontekście bardzo istotne znaczenie mają oczywiście zasoby ludzkie.

EIOD postanowił jednak ograniczyć rozszerzanie zakresu zadań i zwiększanie liczebności personelu, stosując wzrost kontrolowany, tak by nowi pracownicy zostali w pełni wdrożeni do pracy i odpowiednio wyszkoleni oraz by mogli się odpowiednio zintegrować z zespołem. Dlatego też w 2007 r. EIOD postulował utworzenie tylko pięciu stanowisk (cztery stanowiska administratorów i jedno stanowisko asystenta). Wniosek dotyczący zwiększenia liczby personelu z 24 w 2006 r. do 29 w 2007 r. został zatwierdzony przez władze budżetowe. Na początku 2007 r. opublikowano ogłoszenia o naborze i w ciągu roku wszystkie stanowiska zostały obsadzone.

Cenna była pomoc Komisji w tym względzie, zwłaszcza udzielona przez Urząd Administrowania i Wypłacania Należności Indywidualnych (PMO) oraz służbę medyczną.

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

6.3.2. Program stażowy

Realizacja programu stażowego rozpoczęła się w 2005 r. Głównym celem tego programu jest stworzenie osobom, które właśnie skończyły studia, możliwości wykorzystania wiedzy teoretycznej w praktyce, a jednocześnie zdobycia doświadczenia w zakresie bieżącej działalności EIOD. Dzięki temu EIOD ma okazję stać się bardziej rozpoznawalny wśród młodych obywateli UE, w szczególności wśród tych studentów i młodych absolwentów, którzy specjalizują się w problematyce ochrony danych.

Główny program obejmuje dwie pięciomiesięczne sesje rocznie (od marca do lipca oraz od października do lutego); w każdej sesji uczestniczy średnio dwoje stażystów. Sesje te przynoszą nader pozytywne rezultaty.

Oprócz głównego programu stażowego stworzono specjalne warunki umożliwiające przyjmowanie studentów i doktorantów na krótkoterminowe staże bezpłatne. Ta druga część programu oferuje młodym studentom możliwość prowadzenia badań związanych z tematyką ich prac naukowych. Program ten jest realizowany zgodnie z procesem bolońskim i wiąże się z obowiązkiem odbycia przez studentów stażu w ramach studiów. Pod koniec 2007 r. do odbycia dwumiesięcznego bezpłatnego stażu zaproszono jednego doktoranta. Uczestnictwo we wspomnianym wyżej bezpłatnym stażu jest ograniczone do wyjątkowych przypadków i uzależnione od spełnienia rygorystycznych kryteriów.

Wszyscy stażyści, odbywający staże płatne i bezpłatne, uczestniczyli zarówno w pracach teoretycznych, jak i praktycznych, zdobywając doświadczenie u samych źródeł.

Na podstawie porozumienia o gwarantowanym poziomie usług podpisanego w 2005 r. EIOD korzysta z pomocy administracyjnej Biura ds. Staży Dyrekcji Generalnej ds. Edukacji i Kultury w Komisji, które udziela mu stale cennego wsparcia dzięki bogatemu doświadczeniu swoich pracowników.

6.3.3. Programy dla oddelegowanych ekspertów krajowych

Realizacja programu dla oddelegowanych ekspertów krajowych rozpoczęła się w styczniu 2006 r., po ustanowieniu jesienią 2005 r. ([75]) jego podstaw prawnych i organizacyjnych.

Oddelegowanie ekspertów krajowych daje EIOD możliwość korzystania z wiedzy fachowej i doświadczenia pracowników organów ds. ochrony danych utworzonych w państwach członkowskich. Program ten umożliwia także ekspertom krajowym zapoznanie się z problematyką ochrony danych w UE (w zakresie nadzoru, konsultacji i współpracy). Program przynosi korzyści obu stronom, gdyż dzięki niemu EIOD staje się bardziej widoczny na poziomie krajowym jako podmiot w dziedzinie ochrony danych.

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

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

W 2007 r. oddelegowano dwóch ekspertów krajowych: jeden pochodził z organu ds. ochrony danych w Zjednoczonym Królestwie – z Biura Komisarza ds. Informacji, a drugi z węgierskiego organu ds. ochrony danych – z Biura Komisarza ds. Ochrony Danych i Wolności Informacji.

6.3.4. Struktura organizacyjna

Od 2004 r. struktura organizacyjna EIOD nie uległa zmianie: jedna sekcja – licząca obecnie 8 osób – jest odpowiedzialna za administrację, personel i budżet; pozostałych 21 członków personelu zajmuje się operacyjną stroną zadań związanych z ochroną danych. Pracują oni pod bezpośrednim zwierzchnictwem EIOD lub jego zastępcy w dwóch głównych dziedzinach: zajmują się nadzorem i konsultacjami.

Zachowana jest jednak pewna elastyczność w przydzielaniu zadań pracownikom, ponieważ działalność EIOD wciąż ewoluuje.

6.3.5. Szkolenia

Zasadniczo celem szkolenia personelu w EIOD jest rozszerzanie i doskonalenie kompetencji członków personelu, tak by każdy z nich mógł optymalnie przyczyniać się do realizacji zamierzeń instytucji. W 2007 r. EIOD przyjął **politykę w zakresie szkoleń wewnętrznych** uwzględniającą szczególny charakter działań tej instytucji, a także jej strategiczne cele. W ogólnych wytycznych załączonych do odpowiedniej decyzji zawarte są priorytety w zakresie dziedzin kształcenia na lata 2007–2008. Celem EIOD jest utworzenie centrum doskonałości w dziedzinie ochrony danych oraz podniesienie poziomu wiedzy i umiejętności pracowników, tak aby wartości, którym hołduje ta instytucja, były w pełni rozumiane i przestrzegane przez jej personel.

Dla nowych pracowników organizuje się „dzień zapoznawczy". Odbywa się on zgodnie ze standardowym programem, który obejmuje ogólne zapoznanie nowych pracowników z instytucją oraz otoczeniem administracyjnym.

Personel EIOD może uczestniczyć w szkoleniach organizowanych przez inne instytucje i organy międzyinstytucjonalne, głównie Komisję i Europejską Szkołę Administracji (ESA).

Udział EIOD w międzyinstytucjonalnych grupach roboczych (w grupie roboczej ds. ESA i międzyinstytucjonalnym komitecie ds. szkoleń językowych) ma na celu zapewnienie wspólnego podejścia w dziedzinie, w której potrzeby we wszystkich instytucjach są zasadniczo podobne, dzięki czemu możliwe jest uzyskanie korzyści skali.

W 2007 r. EIOD wraz z innymi instytucjami podpisał nowy protokół w sprawie harmonizacji kosztów międzyinstytucjonalnych kursów językowych.

6.4. Pomoc administracyjna i współpraca międzyinstytucjonalna

Współpraca międzyinstytucjonalna, która opiera się na porozumieniu o współpracy międzyinstytucjonalnej podpisanym w czerwcu 2004 r. i przedłużonym w 2006 r. na okres trzech lat, nadal ma istotne znaczenie dla EIOD i jego działań ze względu na zwiększenie wydajności i uzyskanie korzyści skali. Pozwala również uniknąć mnożenia infrastruktur administracyjnych oraz ograniczyć jałowe wydatki administracyjne, a jednocześnie zapewnia administrację publiczną na wysokim poziomie.

Na tej podstawie w 2007 r. kontynuowano współpracę międzyinstytucjonalną z różnymi dyrekcjami generalnymi Komisji (DG ds. Personelu i Administracji, DG ds. Budżetu, służbą audytu wewnętrznego, DG ds. Sprawiedliwości, Wolności i Bezpieczeństwa, DG ds. Edukacji i Kultury), Urzędem Administrowania i Rozliczania Należności Indywidualnych (PMO), różnymi służbami Parlamentu Europejskiego (służbami ds. technologii informacyjnych – w szczególności w powiązaniu z pracami nad nową wersją strony internetowej EIOD; również w związku z wyposażaniem pomieszczeń, zabezpieczaniem budynków, sprzętem drukującym, pocztą, sprzętem telefonicznym, zaopatrzeniem itd.) oraz z Radą (przy pracach translatorskich).

Porozumienia o gwarantowanym poziomie usług podpisane w 2005 r. z różnymi instytucjami i ich wydziałami są regularnie aktualizowane. Przygotowywane są umowy obejmujące nowe dziedziny.

Aby ułatwić współpracę pomiędzy wydziałami Komisji a EIOD oraz usprawnić wymianę informacji pomiędzy służbami, w 2006 r. zwrócono się o umożliwienie bezpośredniego dostępu z siedziby EIOD do niektórych aplikacji Komisji służących do zarządzania finansami. Umożliwiono już taki bezpośredni dostęp do systemu ABAC i trwają prace nad dostępem do aplikacji SAP. Jeśli chodzi o aplikacje stosowane do zarządzania zasobami ludzkimi, nadal możliwy jest tylko częściowy dostęp do systemu Syslog ([76]). Oczekuje się, że w 2008 r. zapewniony będzie pełny dostęp.

We współpracy z odpowiednimi służbami Parlamentu Europejskiego opracowano nową wersję strony internetowej EIOD. Jednak finalizację tego projektu spowolniły problemy związane z oprogramowaniem wybranym do jego realizacji. EIOD ma nadzieje, że w ciągu 2008 r. projekt zostanie zakończony.

W 2007 r. kontynuowano udział w międzyinstytucjonalnych przetargach dotyczących pracowników tymczasowych, ubezpieczeń i dostawy umeblowania, co pozwoliło EIOD zwiększyć wydajność w wielu dziedzinach administracji i poczynić postępy na drodze do większej niezależności. Jeśli chodzi o dostawę materiałów biurowych, EIOD uczestniczył w zorganizowanym przez Parlament Europejski przetargu, w którego wyniku latem 2008 r. udzielone zostaną nowe zamówienia.

EIOD nadal uczestniczył w pracach różnych komitetów międzyinstytucjonalnych. Jednak ze względu na niewielki rozmiar tej instytucji, udział taki musiał się ograniczyć do prac tylko 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 wzorców.

6.5. Infrastruktura

Zgodnie z porozumieniem o współpracy administracyjnej siedziba EIOD znajduje się na terenie Parlamentu Europejskiego, który wspiera EIOD w zakresie infrastruktury informatycznej i telefonicznej.

Z pomocą służb Parlamentu Europejskiego dokonano inwentaryzacji mebli i sprzętu informatycznego.

6.6. Otoczenie administracyjne

6.6.1. System kontroli wewnętrznej i audyt

Proces identyfikowania ryzyka związanego z rozwijaniem działalności przez EIOD znajduje się niewątpliwie we wczesnej fazie. EIOD przyjął szczegółowe procedury kontroli wewnętrznej, które uznano za najbardziej odpowiadające potrzebom tej instytucji ze względu na jej rozmiar i prowadzone przez nią działania. Ma to na celu zapewnienie kierownictwu i personelowi wystarczającej pewności odnośnie do realizacji celów EIOD oraz zarządzanie ryzykiem, które wiąże się z jego działalnością.

Ogólnie rzecz biorąc, funkcjonujące systemy kontroli wewnętrznej zapewniają, zdaniem EIOD, wystarczającą pewność co do legalności i prawidłowości operacji, za które instytucja ta odpowiada. EIOD dopilnuje, by delegowany intendent kontynuował działania na rzecz zagwarantowania wystarczającej pewności, że oświadczenia załączone do sprawozdań rocznych mają faktycznie poparcie w odpowiednich systemach kontroli wewnętrznej.

Pierwsza ocena przeprowadzona przez służby EIOD wykazała, że system kontroli wewnętrznej funkcjonuje prawidłowo i sprawnie.

Sprawozdanie z pierwszego audytu sporządzone przez służbę audytu wewnętrznego (IAS) otrzymano we wrześniu 2007 r. Potwierdziło ono zdolność systemu kontroli wewnętrznej EIOD do zagwarantowania wystarczającej pewności odnośnie do realizacji celów tej instytucji. W procesie oceny wskazano jednak pewne aspekty, w których wymagana jest poprawa. W niektórych z tych przypadków podjęto natychmiastowe działania, a inne działania będą podejmowane stopniowo w przyszłości w miarę ewoluowania zadań powierzonych EIOD.

Wykonanie zaleceń IAS zaakceptowanych przez EIOD znalazło się wśród priorytetów tej instytucji na 2008 r.

([76]) Syslog jest systemem informatycznym służącym do zarządzania szkoleniami. SI12 i ABAC to systemy rachunkowości.

Będzie ono przebiegać zgodnie z planem działania, który zostanie sporządzony na początku 2008 r.

EIOD zamierza poczynić postępy w tej dziedzinie, tak by utrzymać ryzyko dla swojej instytucji na minimalnym poziomie.

6.6.2. Komitet Pracowniczy

Zgodnie z art. 9 regulaminu pracowniczego urzędników Wspólnot Europejskich w dniu 8 lutego 2006 r. EIOD przyjął decyzję w sprawie utworzenia Komitetu Pracowniczego. Konsultacje prowadzone z tym komitetem obejmują szereg ogólnych przepisów wykonawczych dotyczących regulaminu pracowniczego oraz innych przepisów wewnętrznych przyjmowanych przez EIOD.

Zebranie Komitetu Pracowniczego

6.6.3. Przepisy wewnętrzne

Kontynuowano proces przyjmowania nowych przepisów wewnętrznych niezbędnych do prawidłowego funkcjonowania przedmiotowej instytucji, a także nowych ogólnych przepisów wykonawczych dotyczących 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, jednak zostały dostosowane w sposób uwzględniający charakter EIOD. Nowo zatrudnieni pracownicy otrzymują na powitanie przewodnik administracyjny zawierający wszystkie przepisy wewnętrzne EIOD oraz informacje o szczególnych cechach tej instytucji. Dokument ten jest regularnie aktualizowany.

EIOD nadal rozwijał zaplecze socjalne (głównie z myślą o dzieciach – na przykład żłobki, dostęp do Szkoły Europejskiej itd.).

W 2007 r. przyjęto ważne decyzje wewnętrzne:

- Po dokładnym przeanalizowaniu systemów oceny stosowanych w pozostałych instytucjach europejskich oraz w wyniku owocnego dialogu z Komitetem Pracowniczym EIOD przyjął decyzję nr 30 z 30 marca 2007 r. ustanawiającą zasady **oceny** swego personelu – zgodnie z regulaminem pracowniczym urzędników Wspólnot Europejskich ([77]). Opracowano przewodnik dotyczący oceny personelu, określający kryteria oceny oraz procedury sporządzania raportów. Nowością jest przeprowadzana w połowie okresu rozmowa, dzięki której oceniany urzędnik uzyskuje informacje dotyczące pierwszych sześciu miesięcy, co umożliwia mu poprawienie wyników na długo przed oceną oficjalną. Pierwszą ocenę po przyjęciu tych przepisów przeprowadzono w 2007 r.;
- Gdy gotowy był już system oceny, kolejnym logicznym krokiem w procesie prowadzącym do utworzenia i rozwinięcia otoczenia administracyjnego i określenia ścieżek kariery zawodowej było wdrożenie systemu **awansów**; EIOD przyjął przepisy regulujące system awansów, które zawarto w decyzji nr 38 z 26 listopada 2007 r. Po przyjęciu tej decyzji po raz pierwszy przystąpiono do przyznania awansów;
- EIOD jest stosunkowo młodą instytucją, lecz szybko ewoluuje. W związku z tym przepisy i procedury, które są odpowiednie w pierwszych latach działalności, mogą okazać się mniej skuteczne w przyszłości – przy większej i bardziej złożonej strukturze. Dlatego też przepisy te (dotyczące oceny i awansów) zostaną ocenione dwa lata po ich przyjęciu; mogą zatem zostać odpowiednio zmienione.

Dodatkowo przyjęto pakiet trzech decyzji dotyczących **uprawnień emerytalnych** pracowników. EIOD rozpoczął negocjacje z Urzędem Administrowania i Rozliczania Należności Indywidualnych (PMO) w sprawie przekazania mu bieżących działań w tej wysoce technicznej dziedzinie.

([77]) Art. 43: „Kwalifikacje, wydajność oraz zachowanie w ramach służby każdego urzędnika są przedmiotem okresowej oceny […]".

6.6.4. Urzędnik ds. ochrony danych

Zgodnie z art. 24 ust. 1 rozporządzenia (WE) nr 45/2001 EIOD powołał urzędnika ds. ochrony danych (DPO), aby zapewnić stosowanie przepisów tego rozporządzenia na poziomie wewnętrznym. W 2007 r. sporządzono spis operacji, które wiążą się z przetwarzaniem danych osobowych. Spis ten ma na celu ukierunkowanie procedury powiadamiania. EIOD ze względu na swoją szczególną sytuację opracowuje uproszczoną procedurę powiadamiania mającą zastosowanie w przypadku spraw podlegających kontroli wstępnej.

6.6.5. Zarządzanie dokumentami

EIOD wspierany przez służby Parlamentu Europejskiego rozpoczął prace nad wdrażaniem nowego systemu zarządzania pocztą elektroniczną (GEDA). Ma to być pierwszy krok na drodze do stworzenia systemu zarządzania przepływem spraw, który lepiej wesprze działania EIOD.

6.7. Stosunki zewnętrzne

Jako organ europejski z siedzibą w Brukseli i uznany przez władze Belgii EIOD i jego personel korzystają z przywilejów i immunitetów ustanowionych w Protokole w sprawie przywilejów i immunitetów Wspólnot Europejskich.

6.8. Cele na 2008 r.

Cele ustalone na 2007 r. zostały w pełni osiągnięte. W 2008 r. EIOD będzie kontynuował rozpoczętą wcześniej konsolidację oraz pogłębiał niektóre aspekty swojej działalności.

Zaktualizowana terminologia **budżetowa** zacznie obowiązywać w 2008 r. EIOD planuje przyjęcie nowych wewnętrznych zasad finansowych dostosowanych do wielkości tej instytucji. Przewiduje się optymalizację kilku procedur wewnętrznych, aby dostosować instytucję do stale rosnącej liczby spraw finansowych. Jeśli chodzi o oprogramowanie finansowe, EIOD będzie kontynuował działania w celu nabycia narzędzi umożliwiających mu dostęp do danych finansowych ze swojej siedziby.

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 służb Parlamentu rozwinięte i udoskonalone zostanie zarządzanie pocztą oraz rejestrem. Jeśli chodzi o oprogramowanie do zarządzania zasobami ludzkimi (głównie delegacjami: MIPs oraz urlopami i szkoleniami: Syslog), EIOD podejmie wszelkie niezbędne działania w celu nabycia programów umożliwiających mu dostęp do danych ze swojej siedziby.

Wprowadzanie ulepszeń określonych podczas pierwszej oceny systemu kontroli wewnętrznej, a także zaleceń otrzymanych pod koniec 2007 r. od służby audytu wewnętrznego (IAS) będzie traktowane priorytetowo. Urzędnik ds. ochrony danych będzie nadal czuwał nad stosowaniem przepisów rozporządzenia (WE) nr 45/2001 na poziomie wewnętrznym.

Mając na uwadze stopień poufności wymagany w niektórych dziedzinach działalności, EIOD zamierza opracować kompleksową politykę **w zakresie bezpieczeństwa**, odpowiadającą funkcjom pełnionym przez tę instytucję.

Przyszli pracownicy będą potrzebować dodatkowej **powierzchni biurowej**. W 2008 r. EIOD rozpocznie negocjacje ze służbami Parlamentu Europejskiego na temat przydzielenia wystarczającej powierzchni odpowiadającej jego przyszłym potrzebom.

EIOD zamierza rozwijać działania w sferze socjalnej i zakończyć tworzenie nowej strony internetowej.

Załącznik A

Ramy prawne

Artykuł 286 Traktatu WE, przyjęty w 1997 r. jako część traktatu z Amsterdamu, stanowi, że akty wspólnotowe dotyczące ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych oraz swobodnego przepływu tych danych powinny mieć również zastosowanie do instytucji i organów wspólnotowych oraz że należy ustanowić niezależny organ kontrolny.

Aktami wspólnotowymi, o których mowa w tym artykule, 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 r. 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 nr 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 nr 108, precyzowała i rozwijała je jednak pod różnymi względami. Jej celem było zapewnienie wysokiego poziomu ochrony danych osobowych i ich swobodnego przepływu w UE. We wniosku w sprawie tej dyrektywy złożonym na początku lat 90. przez Komisję stwierdzono, że instytucje i organy Wspólnoty powinny być objęte podobnymi zabezpieczeniami prawnymi, 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; rozporządzenie to weszło w życie w 2001 r. ([78]). Rozporządzenie to przewidywało również ustanowienie niezależnego organu kontrolnego, zwanego „europejskim inspektorem ochrony danych", któremu, zgodnie z Traktatem, postawiono konkretne zadania i nadano konkretne uprawnienia.

Traktat konstytucyjny podpisany w październiku 2004 r. kładzie duży nacisk na ochronę praw podstawowych. Poszanowanie życia prywatnego i rodzinnego oraz ochrona danych osobowych traktowane są jako odrębne prawa podstawowe w art. II-67 i II-68 konstytucji. O ochronie danych wspomniano również w art. I-51 konstytucji w tytule VI poświęconym „życiu demokratycznemu" Unii. Wynika z tego jasno, że ochrona danych uważana jest za jeden z podstawowych elementów „dobrych rządów". Niezależny nadzór jest zasadniczą częścią tej ochrony.

Rozporządzenie 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 przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu". Oznacza to, że z zadań i uprawnień EIOD w zakresie nadzoru wyłączone są jedynie te czynności, które znajdują się całkowicie poza obszarami wchodzącymi w skład pierwszego filaru.

Definicje zawarte w tym rozporządzeniu i jego zasadnicza treść są spójne z podejściem przyjętym w dyrektywie 95/46/WE. Można stwierdzić, że rozporządzenie

([78]) Dz.U. L 8 z 12.1.2001, s. 1.

(WE) nr 45/2001 stanowi wdrożenie tej dyrektywy na poziomie europejskim. Wynika stąd, że rozporządzenie to dotyczy ogólnych zasad, takich 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 wypadkach szczególne okoliczności na poziomie UE – a także nadzór, stosowanie prawa i środki odwoławcze. Oddzielny rozdział dotyczy ochrony danych osobowych i prywatności w kontekście wewnętrznych sieci telekomunikacyjnych. Rozdział ten faktycznie wdraża na poziomie europejskim dyrektywę 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. Zadaniem tych urzędników jest zapewnienie (w sposób niezależny) 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 doradzać lub interweniować na wczesnym etapie, jak również pomagać w wypracowywaniu sprawdzonych rozwiązań. Ponieważ formalnym obowiązkiem urzędnika ds. ochrony danych jest współpraca z EIOD, współdziałanie w ramach tej sieci współpracy i jej rozwój są bardzo istotne i wartościowe (zob. pkt 2.2).

Zadania i uprawnienia EIOD

Zadania i uprawnienia EIOD zostały dokładnie 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 i badanie skarg, prowadzenie innych dochodzeń, informowanie administratorów danych 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 pomieszczeń, 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 doradzaniu Komisji i innym instytucjom Wspólnoty w zakresie nowego prawodawstwa – uwydatnione w art. 28 ust. 2 przez nałożenie na Komisję formalnego obowiązku konsultowania się z EIOD w przypadku przyjmowania wniosku prawodawczego odnoszącego się do ochrony danych osobowych – dotyczy także z projektów dyrektyw i innych środków, które mają mieć zastosowanie na poziomie krajowym lub mają być wdrażane do 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 rozwoju sytuacji w stosownych dziedzinach w aspektach mogących mieć wpływ na ochronę danych osobowych. Te czynności **konsultacyjne** EIOD omówiono obszerniej w rozdziale 3 niniejszego sprawozdania.

Obowiązek współpracy z krajowymi organami nadzoru oraz organami nadzoru działającymi w trzecim filarze 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 działającymi w trzecim filarze 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 skorzystaniu 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

CCL	wspólny wykaz przechowywanych dossier
CdT	Centrum Tłumaczeń dla Organów Unii Europejskiej
CFCA	Wspólnotowa Agencja Kontroli Rybołówstwa
CIS	System Informacji Celnej
CoA	Trybunał Obrachunkowy
KR	Komitet Regionów
CPCS	system współpracy w zakresie ochrony konsumentów
CPVO	Wspólnotowy Urząd Ochrony Odmian Roślin
DG JLS	Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa
DPC	koordynator ds. ochrony danych
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 Szans
DG INFSO	Dyrekcja Generalna ds. Społeczeństwa Informacyjnego i Mediów
DPA	Organy odpowiedzialne za ochronę danych
DPC	koordynator ds. ochrony danych (wyłącznie w Komisji Europejskiej)
DPO	urzędnik ds. ochrony danych
ESA	Europejska Szkoła Administracji
EC	Wspólnoty Europejskie
EBC	Europejski Bank Centralny
ETS	Europejski Trybunał Sprawiedliwości
EKES	Europejski Komitet Ekonomiczno-Społeczny
EFSA	Europejski Urząd ds. Bezpieczeństwa Żywności
EBI	Europejski Bank Inwestycyjny
EMPL	Komisja Zatrudnienia i Spraw Socjalnych działająca w Parlamencie Europejskim
ENISA	Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji
EKPC	Europejska konwencja praw człowieka
EMEA	Europejska Agencja Leków
EMCDDA	Europejskie Centrum Monitorowania Narkotyków i Narkomanii
EMSA	Europejska Agencja ds. Bezpieczeństwa na Morzu
EO	Europejski Rzecznik Praw Obywatelskich
EP	Parlament Europejski
EPSO	Europejski Urząd Doboru Kadr
EFK	Europejska Fundacja Kształcenia
EU	Unia Europejska
EUMC	Europejskie Centrum Monitorowania Rasizmu i Ksenofobii
Eurofound	Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy
EWS	system wczesnego ostrzegania
FIDE	identyfikująca baza danych rejestru celnego
7. PR	Siódmy program ramowy w zakresie badań i rozwoju technologicznego
IAS	służba audytu wewnętrznego
IGC	konferencja międzyrządowa
IMI	system wymiany informacji w ramach rynku wewnętrznego

WCB	Wspólne Centrum Badawcze
LIBE	Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych działająca w Parlamencie Europejskim
MoU	protokół ustaleń
OECD	Organizacja Współpracy Gospodarczej i Rozwoju
OHC	Centrum Zdrowia w Miejscu Pracy
OHIM	Urząd Harmonizacji Rynku Wewnętrznego
OLAF	Europejski Urząd ds. Zwalczania Nadużyć Finansowych
PMO	Urząd Administrowania i Wypłacania Należności Indywidualnych działający w Komisji Europejskiej
PNR	dane dotyczące przelotu pasażera
B+R	badania i rozwój
RFID	identyfikacja radiowa
SIS	system informacyjny Schengen
SWIFT	Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych
trzeci filar	współpraca policyjna i sądowa w sprawach karnych
VIS	wizowy system informacyjny
WP 29	Grupa Robocza Art. 29
WPPJ	Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości

Załącznik D

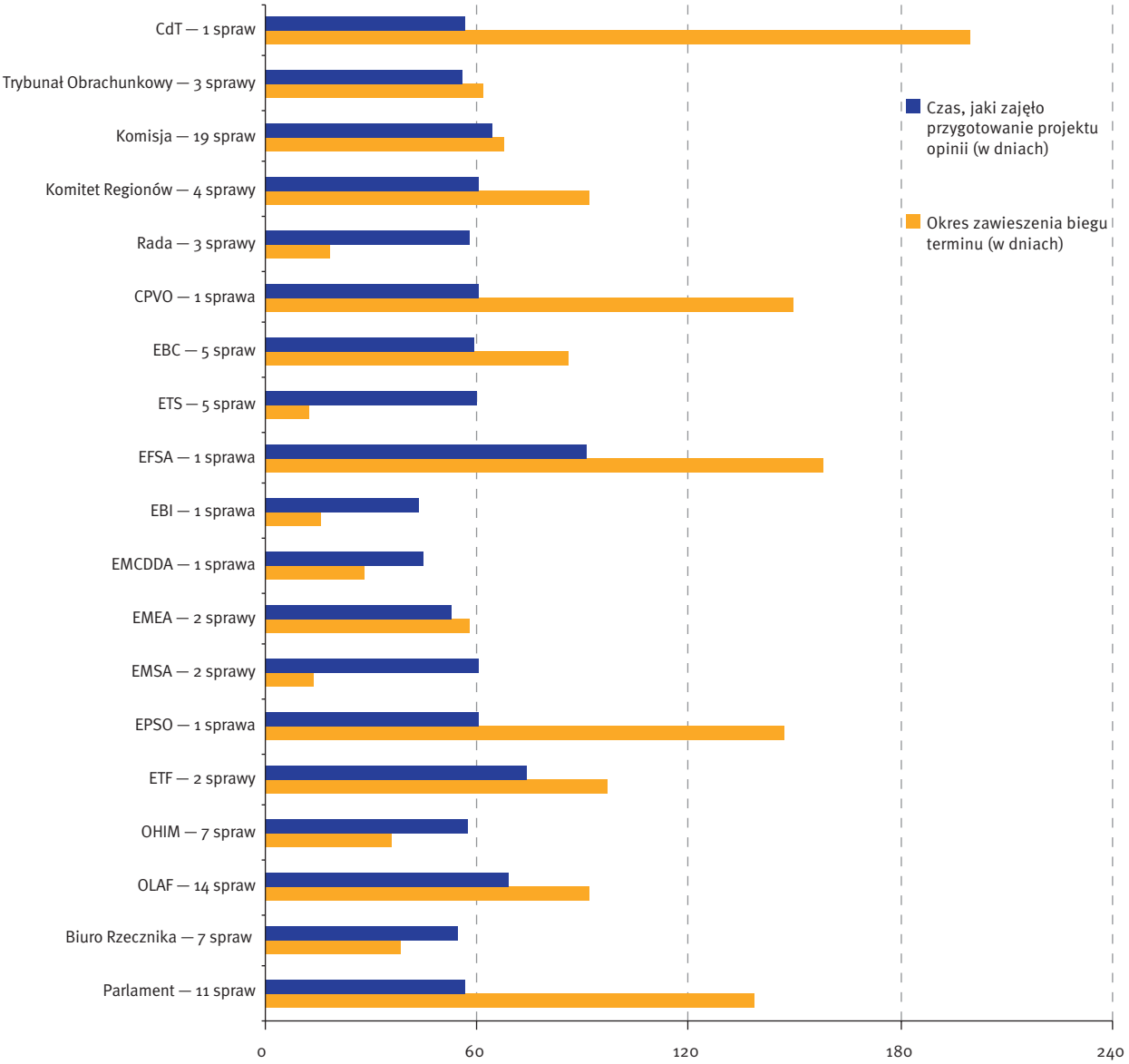
Lista urzędników ds. ochrony danych (DPO)

Organizacja	Imię i 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	Jan KILB	data-protection@eca.europa.eu
Europejski Komitet Ekonomiczno-Społeczny	Sofia FAKIRI	data.protection@eesc.europa.eu
Komitet Regionów	Petra CANDELLIER	data.protection@cor.europa.eu
Europejski Bank Inwestycyjny	Jean-Philippe MINNAERT	dataprotectionofficer@eib.org
Europejski Rzecznik Praw Obywatelskich	Loïc JULIEN	dpo-euro-ombudsman@ombudsman.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 (OLAF)	Laraine LAUDATI	laraine.laudati@ec.europa.eu
Centrum Tłumaczeń dla Organów Unii Europejskiej	Benoît VITALE	data-protection@cdt.europa.eu
Urząd Harmonizacji Rynku Wewnętrznego (OHIM)	Luc DEJAIFFE	dataprotectionofficer@oami.europa.eu
Agencja Praw Podstawowych	Nikolaos FIKATAS	nikolaos.fikatas@fra.europa.eu
Europejska Agencja Leków	Vincenzo SALVATORE	data.protection@emea.europa.eu
Wspólnotowy Urząd Ochrony Odmian Roślin	Véronique DOREAU	doreau@cpvo.europa.eu
Europejska Fundacja Kształcenia	*jeszcze niemianowany*	
Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA)	Andreas MITRAKAS	dataprotection@enisa.europa.eu
Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy	Markus GRIMMEISEN	mgr@eurofound.europa.eu
Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA)	Cécile MARTEL	cecile.martel@emcdda.europa.eu
Europejski Urząd ds. Bezpieczeństwa Żywności	Claus REUNIS	dataprotectionofficer@efsa.europa.eu
Europejska Agencja ds. Bezpieczeństwa na Morzu	Małgorzata NESTEROWICZ	malgorzata.nesterowicz@emsa.europa.eu
Europejska Agencja Odbudowy	Martin DISCHENDORFER	martin.dischendorfer@ear.europa.eu

Organizacja	Imię i nazwisko	E-Mail
Europejskie Centrum Rozwoju Kształcenia Zawodowego (CEDEFOP)	Spyros ANTONIOU	spyros.antoniou@cedefop.europa.eu
Agencja Wykonawcza ds. Edukacji, Kultury i Sektora Audiowizualnego (EACEA)	Hubert MONET	hubert.monet@ec.europa.eu
Agencja Wykonawcza ds. Konkurencyjności i Innowacyjności (EACI)	Olivier CORNU	olivier.cornu@ext.ec.europa.eu
Europejska Agencja ds. Bezpieczeństwa i Ochrony Zdrowia w Miejscu Pracy (OSHA)	Terry TAYLOR	taylor@osha.europa.eu
Wspólnotowa Agencja Kontroli Rybołówstwa (CFCA)	Rieke ARNDT	rieke.arndt@ext.ec.europa.eu
Organ Nadzoru Europejskiego GNSS	Dimitri NICOLAÏDES	dimitri.nicolaides@gsa.europa.eu
Europejska Agencja Kolejowa (ERA)	Zografia PYLORIDOU	zographia.pyloridou@era.europa.eu
Agencja Wykonawcza ds. Zdrowia i Konsumentów	Eva LÄTTI	eva.latti@ec.europa.eu
Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC)	Elisabeth ROBINO	elisabeth.robino@ecdc.europa.eu
Europejska Agencja Ochrony Środowiska	Gordon McINNES	gordon.mcinnes@eea.europa.eu
Europejski Fundusz Inwestycyjny	Jobst NEUSS	j.neuss@eif.org
Europejska Agencja ds. Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych (Frontex)	Sakari VUORENSOLA	sakari.vuorensola@frontex.europa.eu
Europejska Agencja Bezpieczeństwa Lotniczego (EASA)	Arthur BECKAND	arthur.beckand@easa.europa.eu

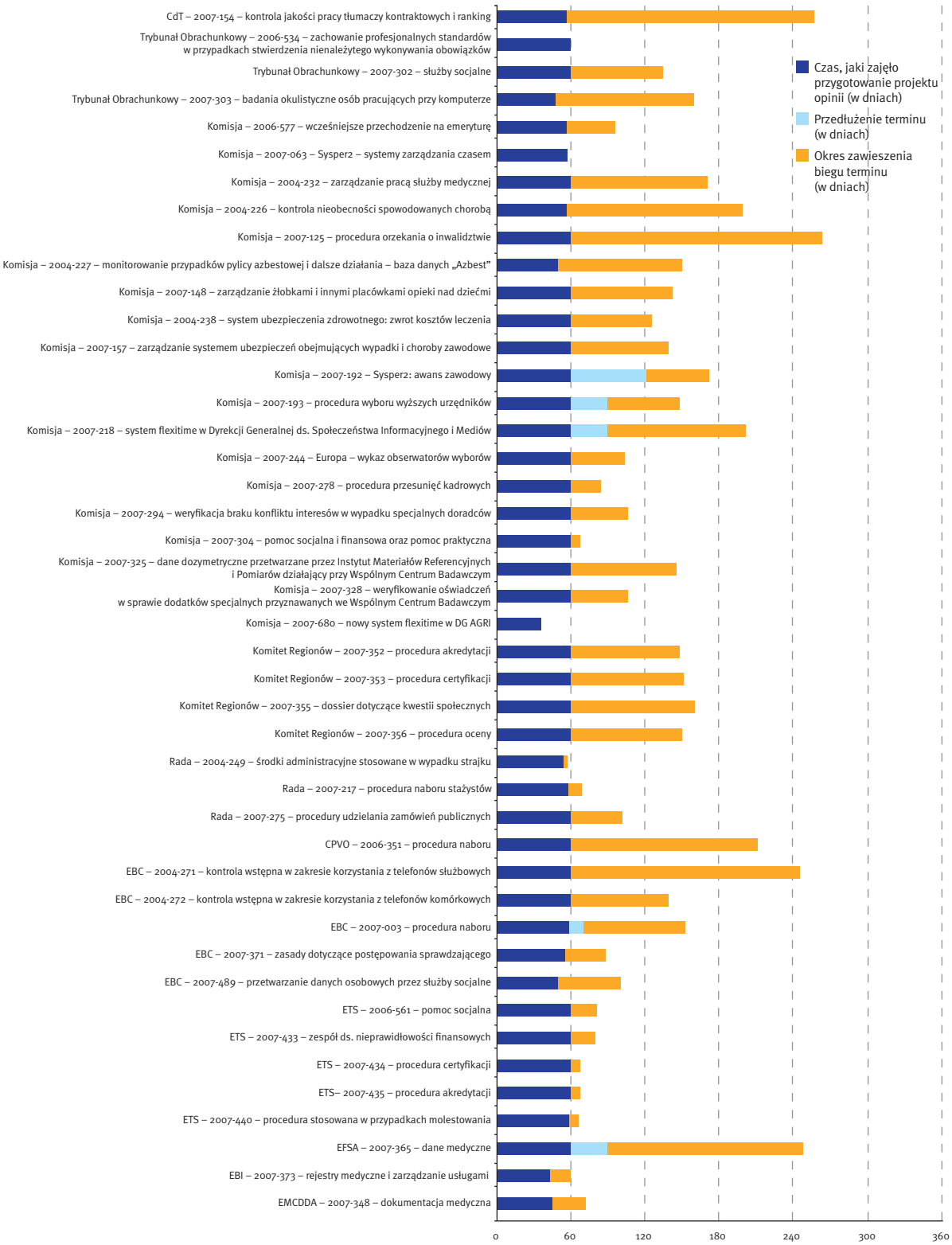
Załącznik E

Czas trwania kontroli wstępnej w poszczególnych sprawach i instytucjach

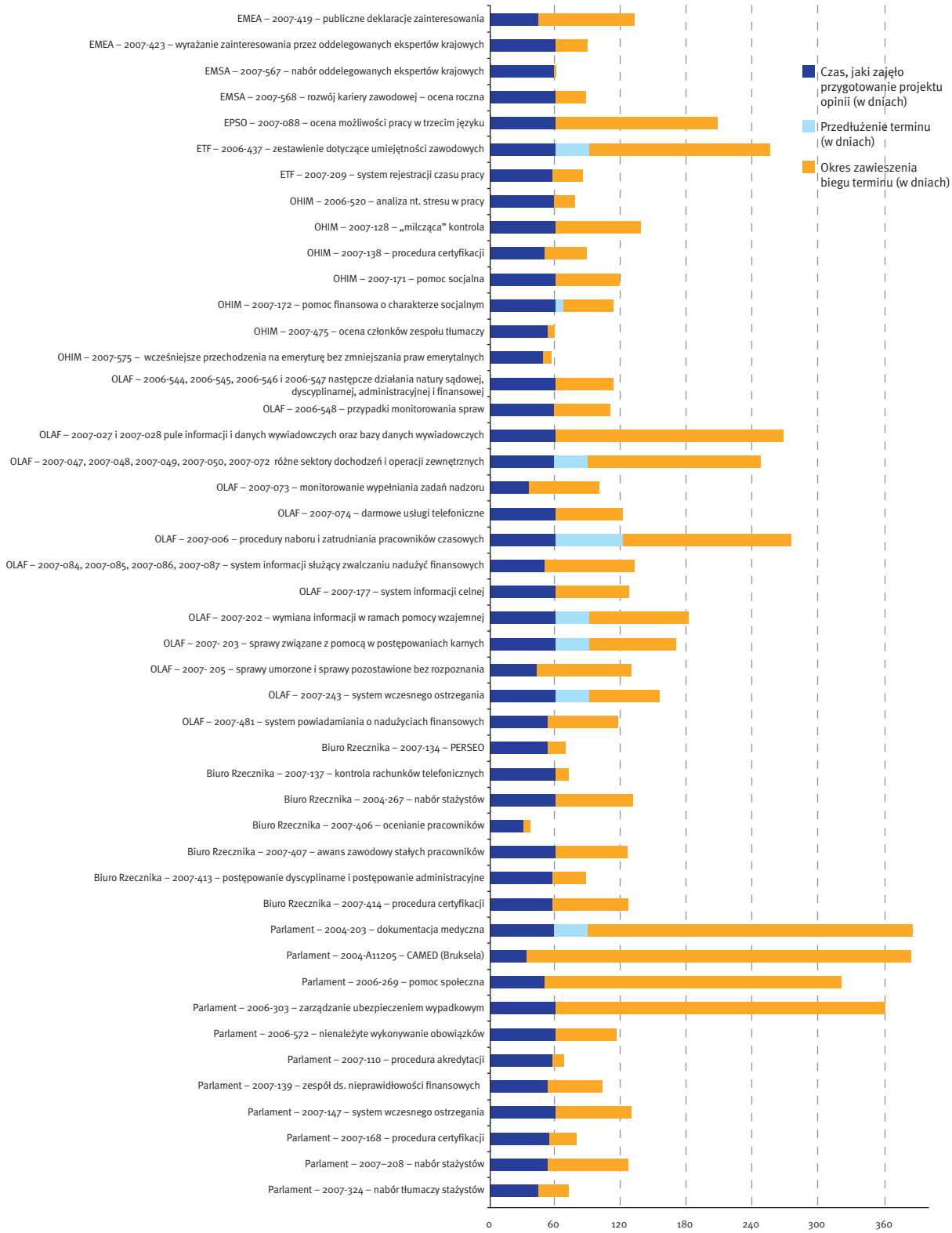


Uwaga: Czas przygotowania projektu opinii (w dniach) nie obejmuje sierpnia w sprawach dotyczących kontroli *ex post* otrzymanych przed 1.9.2007. Okres zawieszenia biegu terminu (w dniach) obejmuje także oczekiwanie na uwagi do projektu (zwykle 7–10 dni).

Opinie wydane w 2007 r. (I)



Opinie wydane w 2007 r. (II)



Uwaga: Czas przygotowania projektu opinii (w dniach) nie obejmuje sierpnia w sprawach dotyczących kontroli *ex post* otrzymanych przed 1.9.2007. Okres zawieszenia biegu terminu (w dniach) obejmuje także oczekiwanie na uwagi do projektu (zwykle 7–10 dni).

Załącznik F

Wykaz opinii wydanych w wyniku kontroli wstępnej

Nowy system *flexitime* w DG AGRI – Komisja

Odpowiedź z dnia 19 grudnia 2007 r. na powiadomienie dotyczące przeprowadzenia kontroli wstępnej w zakresie nowego systemu *flexitime* w DG AGRI (sprawa 2007-680)

System powiadamiania o nadużyciach finansowych – OLAF

Opinia z dnia 4 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej rejestrów medycznych (sprawa 2007-481)

Rozwój kariery zawodowej – Europejska Agencja ds. Bezpieczeństwa na Morzu

Opinia z dnia 17 grudnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Rozwój kariery zawodowej – ocena roczna" (sprawa 2007-568)

Doradca społeczny – Europejski Bank Centralny

Opinia z dnia 6 grudnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie danych przetwarzanych przez doradcę społecznego (sprawa 2007-489)

Dossier dotyczące kwestii społecznych – EKES i KR

Opinia z dnia 6 grudnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Kwestie społeczne" (sprawa 2007-355)

Procedura oceny – Komitet Regionów

Opinia z dnia 4 grudnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura oceny urzędników i innych pracowników" (sprawa 2007-356)

Procedura akredytacji – Komitet Regionów

Opinia z dnia 29 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura certyfikacji" (sprawa 2007-352)

Procedura orzekania o inwalidztwie – Komisja

Opinia z dnia 29 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura orzekania o inwalidztwie – służba medyczna Bruksela–Luksemburg" (sprawa 2007-125)

Strajk i podobne działania – Rada

Opinia z dnia 29 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Środki administracyjne stosowane w przypadku strajku i podobnych działań: potrącenie z wynagrodzenia i zapewnienie obecności niezbędnych pracowników" (sprawa 2004-249)

Dane dozymetryczne przetwarzane przez Instytut Materiałów Referencyjnych i Pomiarów działający przy Wspólnym Centrum Badawczym – Komisja

Opinia z dnia 29 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Dane dozymetryczne przetwarzane przez działający przy Wspólnym Centrum Badawczym Instytut Materiałów Referencyjnych i Pomiarów (Geel)" (sprawa 2007-325)

Certyfikacja – Komitet Regionów

Opinia z dnia 29 maja 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura certyfikacji" (sprawa 2007-353)

Badania okulistyczne – Trybunał Obrachunkowy

Opinia z dnia 29 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Regularne badania okulistyczne osób pracujących przy komputerze" (sprawa 2007-303)

Wcześniejsze przechodzenie na emeryturę – OHIM

Opinia z dnia 22 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenie kontroli wstępnej w zakresie procedury wcześniejszego przechodzenia na emeryturę bez zmniejszania praw emerytalnych (sprawa 2007-575)

Bazy danych zawierających informacje wywiadowcze – OLAF

Opinia z dnia 21 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie gromadzenia informacji i danych wywiadowczych oraz w zakresie baz danych zawierających informacje wywiadowcze (połączone sprawy 2007-27 i 2007-28)

Nabór oddelegowanych ekspertów krajowych – EMSA

Opinia z dnia 20 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury naboru oddelegowanych ekspertów krajowych (sprawa 2007-567)

Nabór pracowników czasowych – OLAF

Opinia z dnia 14 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie selekcji prowadzonej przez OLAF i naboru pracowników czasowych (sprawa 2007-6)

Ocena członków zespołu tłumaczy – OHIM

Opinia z dnia 12 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny członków zespołu tłumaczy (sprawa 2007-475)

Przetwarzanie danych osobowych przez służby socjalne – Trybunał Obrachunkowy

Opinia z dnia 8 listopada 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przetwarzania danych osobowych przez służby socjalne (sprawa 2007-302)

Eksperci krajowi – EMEA

Opinia z dnia 26 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wyrażania zainteresowania przez oddelegowanych ekspertów krajowych (sprawa 2007-423)

Certyfikacja – Europejski Rzecznik Praw Obywatelskich

Opinia z dnia 24 maja 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura certyfikacji" (sprawa 2007-414)

Awans zawodowy – Europejski Rzecznik Praw Obywatelskich

Opinia z dnia 22 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Awans zawodowy stałych pracowników" (sprawa 2007-407)

System *flexitime* w DG INFSO – Komisja

Opinia z dnia 19 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wdrożenia systemu *flexitime* w Dyrekcji Generalnej ds. Społeczeństwa Informacyjnego i Mediów (sprawa 2007-218)

Wymiana informacji w ramach pomocy wzajemnej – OLAF

Opinia z dnia 19 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wymiany informacji w ramach pomocy wzajemnej (sprawa 2007-202)

Postępowanie dyscyplinarne i postępowanie administracyjne – Europejski Rzecznik Praw Obywatelskich

Opinia z dnia 17 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Postępowanie dyscyplinarne i postępowanie administracyjne " (sprawa 2007-413)

Nieprawidłowości finansowe – Trybunał Sprawiedliwości

Opinia z dnia 17 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Wyspecjalizowany zespół ds. nieprawidłowości finansowych" (sprawa 2007-433)

Pomoc przy prowadzeniu dochodzeń w postępowaniu karnym – OLAF

Opinia z dnia 12 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie pomocy przy prowadzeniu dochodzeń w postępowaniu karnym (sprawa 2007-203)

Nieobecność spowodowana chorobą – Komisja

Opinia z dnia 11 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Kontrola nieobecności spowodowanych chorobą: Bruksela–Luksemburg" (sprawa 2004-226)

Sysper2: awans zawodowy – Komisja

Opinia z dnia 9 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Sysper2: awans zawodowy" (sprawa 2007-192)

System wczesnego ostrzegania – OLAF

Opinia z dnia 4 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej systemu wczesnego ostrzegania (sprawa 2007-243)

Dodatki specjalne przyznawane we Wspólnym Centrum Badawczym – Komisja

Opinia z dnia 4 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Weryfikowanie oświadczeń w sprawie dodatków specjalnych przyznawanych we Wspólnym Centrum Badawczym" (sprawa 2007-328)

Przypadki molestowania – Trybunał Sprawiedliwości

Opinia z dnia 4 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura stosowana w przypadkach molestowania" (sprawa 2007-440)

Dochodzenia zewnętrzne – OLAF

Opinia z dnia 4 października 2007 r. w sprawie pięciu powiadomień dotyczących przeprowadzenia kontroli wstępnej w zakresie dochodzeń zewnętrznych (sprawy 2007-47, 2007-48, 2007-49, 2007-50, 2007-72)

Procedura certyfikacji – Trybunał Sprawiedliwości

Opinia z dnia 3 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura certyfikacji" (sprawa 2007-434)

Sprawy umorzone – OLAF

Opinia z dnia 3 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie spraw umorzonych i spraw pozostawionych bez rozpoznania (sprawa 2007-205)

Procedura akredytacji – Trybunał Sprawiedliwości

Opinia z dnia 3 października 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura akredytacji" (sprawa 2007-435)

Procedura wyboru wyższych urzędników – Komisja

Opinia z dnia 17 września 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury wyboru wyższych urzędników (sprawa 2007-193)

Badania lekarskie – EMCDDA

Opinia z dnia 13 września 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie badań lekarskich poprzedzających zatrudnienie i rocznych badań lekarskich pracowników (sprawa 2007-348)

Konflikt interesów w przypadku specjalnych doradców – Komisja

Opinia z dnia 11 września 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zweryfikowania braku konfliktu interesów w przypadku specjalnych doradców i opublikowania oświadczeń w tej sprawie na stronie internetowej „Europa" (sprawa 2007-294)

Służba medyczna – Komisja

Opinia z dnia 10 września 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Zarządzanie pracą służby medycznej Bruksela – Luksemburg, przede wszystkim za pomocą programu informatycznego SERMED" (sprawa 2004-232)

Postępowanie sprawdzające – Europejski Bank Centralny

Opinia z dnia 7 września 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie stosowania zasad postępowania sprawdzającego (sprawa 2007-371)

Procedura przesunięć kadrowych – Komisja

Opinia z dnia 5 maja 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej nagrywania rozmów telefonicznych w salach, w których przeprowadzane są rozmowy handlowe (sprawa 2007-278)

Ocena stopnia znajomości trzeciego języka – EPSO

Opinia z dnia 4 września 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Ocena umiejętności posługiwania się trzecim językiem przy wykonywaniu obowiązków zawodowych (zastosowanie art. 45 ust. 2 regulaminu pracowniczego)" (sprawa 2007-88)

Rejestry medyczne i zarządzanie czasem pracy – Europejski Bank Inwestycyjny

Opinia z dnia 3 sierpnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Zmiany sposobu przetwarzania danych dotyczących zarządzania czasem pracy i dokumentacji medycznej" (sprawa 2007-373)

Ocenianie pracowników – Europejski Rzecznik Praw Obywatelskich

Opinia z dnia 3 sierpnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceniania pracowników (sprawa 2007-406)

Nabór tłumaczy stażystów – Parlament

Opinia z dnia 31 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej operacji przetwarzania danych do celów rekrutacji (sprawa 2007-324)

Nabór stażystów – Parlament

Opinia z dnia 31 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru stażystów (sprawa 2007-208)

Baza danych „Azbest" – Komisja

Opinia z dnia 27 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Monitorowanie przypadków pylicy azbestowej i dalsze działania – baza danych „Azbest" (służba medyczna i działania na płaszczyźnie psychologicznej i społecznej, Bruksela)" (sprawa 2004-227)

Żłobki – Komisja

Opinia z dnia 27 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Zarządzanie żłobkami i innymi placówkami opieki nad dziećmi w Brukseli" (sprawa 2007-148)

Ubezpieczenie obejmujące wypadki i choroby zawodowe – Komisja

Opinia z dnia 27 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania systemem ubezpieczeń obejmującym wypadki i choroby zawodowe (sprawa 2007-157)

Pomoc socjalna (Ispra) – Komisja

Opinia z dnia 24 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie pomocy socjalnej i finansowej oraz pomocy praktycznej (sprawa 2007-304)

System informacji celnej – OLAF

Opinia z dnia 24 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu informacji celnej (sprawa 2007-177)

Pomoc socjalna – OHIM

Opinia z dnia 23 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie udzielania pomocy socjalnej (sprawa 2007-171)

Wykaz obserwatorów wyborów – Komisja

Opinia z dnia 23 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wykazu obserwatorów wyborów umieszczonego na stronie internetowej „Europa" (sprawa 2007-244)

Procedury udzielania zamówień publicznych – Rada

Opinia z dnia 19 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedur udzielania zamówień publicznych (sprawa 2007-275)

Prowadzenie działań dochodzeniowych – OLAF

Opinia z dnia 19 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie regularnego monitorowania prowadzonych działań dochodzeniowych (sprawa 2007-73)

„Milcząca" kontrola – OHIM

Opinia z dnia 18 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „milczącej" kontroli (sprawa 2007-128)

System wczesnego ostrzegania – Parlament

Opinia z dnia 16 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu wczesnego ostrzegania (sprawa 2007-147)

Przypadki monitorowania spraw – OLAF

Opinia z dnia 11 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przypadków monitorowania spraw (sprawa 2006-548)

System ubezpieczenia zdrowotnego

Opinia z dnia 10 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania systemem ubezpieczenia zdrowotnego (sprawa 2004-238)

Pomoc finansowa o charakterze socjalnym – OHIM

Opinia z dnia 3 lipca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej dotyczącej pomocy socjalnej i finansowej (sprawa 2007-172)

System AFIS – OLAF

Opinia z dnia 29 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie stosowania w systemie AFIS ukierunkowanych modułów sektorowych (sprawy 2007-84, 2007-85, 2007-86, 2007-87)

System rejestracji czasu pracy – ETF

Opinia z dnia 21 czerwca 2007 r. w sprawie powiadomienia dotyczącego systemu rejestracji czasu pracy stosowanego w Europejskiej Fundacji Kształcenia (sprawa 2007-209)

Dokumentacja medyczna (Bruksela) – Parlament

Opinia z dnia 14 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Camed – Bruksela" (sprawa 2004-205)

Dokumentacja medyczna (Luksemburg) – Parlament

Opinia z dnia 14 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Dokumentacja medyczna – Luksemburg" (sprawa 2004-203)

Zestawienie dotyczące umiejętności zawodowych – Europejska Fundacja Kształcenia

Opinia z dnia 13 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zestawienia dotyczącego umiejętności zawodowych pracowników Europejskiej Fundacji Kształcenia (sprawa 2006-437)

Procedura naboru stażystów – Rada

Opinia z dnia 12 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury naboru stażystów w Sekretariacie Generalnym Rady Unii Europejskiej (sprawa 2007-217)

Zespół ds. nieprawidłowości finansowych

Opinia z dnia 12 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zespołu ds. nieprawidłowości finansowych (sprawa 2007-139)

Bezpłatne połączenia telefoniczne – OLAF

Opinia z dnia 6 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie bezpłatnych połączeń telefonicznych (sprawa 2007-74)

Procedura certyfikacji – Parlament

Opinia z dnia 6 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Procedura akredytacji" (sprawa 2007-168)

Procedura certyfikacji – OHIM

Opinia z dnia 6 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury certyfikacji (sprawa 2007-138)

Procedura naboru – Europejski Bank Centralny

Opinia z dnia 4 czerwca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury naboru (sprawa 2007-3)

Kontrola rachunków telefonicznych – Europejski Rzecznik Praw Obywatelskich

Opinia z dnia 14 maja 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie kontroli rachunków telefonicznych (sprawa 2007-137)

„Perseo" – Europejski Rzecznik Praw Obywatelskich

Opinia z dnia 7 maja 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie programu komputerowego Perseo (sprawa 2007-134)

Stres w pracy – OHIM

Opinia z dnia 2 maja 2007 r. w sprawie analizy poświęconej tematyce stresu w miejscu pracy (sprawa 2006-520)

Pomoc społeczna – Parlament

Opinia z dnia 30 kwietnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Pomoc społeczna i wsparcie w przypadku uzależnienia" (sprawa 2006-269)

Ubezpieczenie wypadkowe – Parlament

Opinia z dnia 30 kwietnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania ubezpieczeniem wypadkowym (sprawa 2006-303)

Procedura akredytacji – Parlament

Opinia z dnia 26 kwietnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury akredytacji (sprawa 2007-110)

Procedura zaradzania przypadkom nienależytego wykonywania obowiązków – Parlament

Opinia z dnia 10 kwietnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury zaradzania przypadkom nienależytego wykonywania obowiązków (sprawa 2006-572)

Zarządzanie czasem pracy – Komisja

Opinia z dnia 29 marca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Sysper2: moduł zarządzania czasem pracy" (sprawa 2007-63)

Monitorowanie przetwarzania danych – OLAF

Opinia z dnia 26 marca 2007 r. w sprawie monitorowania przetwarzania danych (działania dyscyplinarne, administracyjne, sądowe, finansowe) (sprawy 2006-544, 2006-545, 2006-546, 2006-547)

Badania lekarskie – Europejski Urząd ds. Bezpieczeństwa Żywności

Opinia z dnia 23 marca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie badań lekarskich kandydatów na pracowników i rocznych badań lekarskich pracowników EFSA (sprawa 2006-365)

Wcześniejsze przechodzenie na emeryturę – Komisja

Opinia z dnia 20 marca 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Stosowana co roku procedura dotycząca wcześniejszego przechodzenia na emeryturę bez zmniejszania praw emerytalnych" (sprawa 2006-577)

Korzystanie z telefonów komórkowych – Europejski Bank Centralny

Opinia z dnia 26 lutego 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie korzystania z telefonów komórkowych (sprawa 2004-272)

Pomoc socjalna – Trybunał Sprawiedliwości

Opinia z dnia 21 lutego 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie pomocy socjalnej (sprawa 2006-561)

Korzystanie z telefonów służbowych – Europejski Bank Centralny

Opinia z dnia 13 lutego 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenie kontroli wstępnej w zakresie korzystania z telefonów służbowych (sprawa 2004-271)

Procedura naboru – Wspólnotowy Urząd Ochrony Odmian Roślin

Opinia z dnia 2 lutego 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury naboru (sprawa 2006-351)

Nienależyte wykonywanie obowiązków – Trybunał Obrachunkowy

Opinia z dnia 18 stycznia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Zachowanie profesjonalnych standardów w przypadkach stwierdzenia nienależytego wykonywania obowiązków" (sprawa 2006-534)

Załącznik G

Wykaz opinii w sprawie wniosków prawodawczych

Europejskie dane PNR

Opinia z dnia 20 grudnia 2007 r. w sprawie projektu wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa.

Identyfikacja radiowa (RFID)

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie identyfikacji radiowej (RFID) w Europie: w stronę ram polityki COM(2007) 96.

Przepisy wykonawcze inicjatywy dotyczącej konwencji z Prüm

Opinia z dnia 19 grudnia 2007 r. na temat inicjatywy Republiki Federalnej Niemiec w sprawie przyjęcia decyzji Rady dotyczącej wdrożenia decyzji 2007/.../WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej.

Przewoźnik drogowy

Opinia z dnia 12 września 2007 r. w sprawie wniosku dotyczącego rozporządzenia w sprawie wspólnych zasad dotyczących warunków wykonywania zawodu przewoźnika drogowego, Dz.U. C 14 z 19.1.2008, s. 1.

Statystyki Wspólnoty dotyczące danych w zakresie zdrowia

Opinia z dnia 5 września 2007 r. na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz bezpieczeństwa i higieny pracy (COM(2007) 46 wersja ostateczna), Dz.U. C 295 z 7.12.2007, s. 1.

Wdrażanie dyrektywy o ochronie danych

Opinia z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, Dz.U. C 255 z 27.10.2007, s. 1.

Ochrona danych w trzecim filarze

Trzecia opinia z dnia 27 kwietnia 2007 r. w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. C 139 z 23.6.2007, s. 1.

Finansowanie wspólnej polityki rolnej

Opinia z dnia 10 kwietnia 2007 r. w sprawie wniosku dotyczącego rozporządzenia Rady zmieniającego rozporządzenie (WE) nr 1290/2005 w sprawie finansowania wspólnej polityki rolnej (COM(2007) 122 wersja ostateczna), Dz.U. C 134 z 16.6.207, s. 1.

Współpraca transgraniczna (konwencja z Prüm)

Opinia z dnia 4 kwietnia 2007 r. na temat inicjatywy 15 państw członkowskich w celu przyjęcia decyzji Rady w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną, Dz.U. C 169 z 21.7.2007, s. 2.

Koordynacja systemów zabezpieczenia społecznego

Opinia z dnia 6 marca 2007 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie wykonywania rozporządzenia (WE) nr 883/2004 w sprawie koordynacji systemów zabezpieczenia społecznego (COM(2006) 16 wersja ostateczna), Dz.U. C 91 z 26.4.2007, s. 15.

Prawidłowe stosowanie przepisów prawa celnego i rolnego

Opinia z dnia 22 lutego 2007 r. w sprawie wniosku dotyczącego rozporządzenia zmieniającego rozporządzenie Rady (WE) nr 515/97 w sprawie wzajemnej pomocy między organami administracyjnymi państw członkowskich i współpracy między państwami członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego (COM(2006) 866 wersja ostateczna), Dz.U. C 94 z 28.4.2007, s. 3.

Europejski Urząd Policji

Opinia z dnia 16 lutego 2007 r. w sprawie wniosku dotyczącego decyzji Rady ustanawiającej Europejski Urząd Policji (Europol) (COM(2006) 817 wersja ostateczna), Dz.U. C 255 z 27.10.2007, s. 13.

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

María Verónica PÉREZ ASINARI
Administrator – urzędnik ds. prawnych

Jaroslaw LOTARSKI
Administrator – urzędnik ds. prawnych

Tereza STRUNCOVA
Administrator – urzędnik ds. prawnych

György HALMOS (*)
Ekspert krajowy – urzędnik ds. prawnych (od września 2007)

Delphine HAROU (*)
Asystent ds. nadzoru

Xanthi KAPSOSIDERI
Asystent ds. nadzoru

Sylvie LONGRÉE
Asystent ds. nadzoru

Kim Thien LÊ
Asystent ds. sekretariatu

Thomas GREMEL
Asystent ds. nadzoru

Stephen McCARTNEY
Ekspert krajowy – urzędnik ds. prawnych (luty 2007 – listopad 2007)

Endre SZABÓ
Ekspert krajowy – urzędnik ds. prawnych (do lipca 2007)

- **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

Anne-Christine LACOSTE
Administrator – urzędnik ds. prawnych

Nathalie VANDELLE (*)
Administrator – urzędnik ds. kontaktów z prasą

Per SJÖNELL (*)
Administrator – urzędnik ds. kontaktów z prasą (do sierpnia 2007)

Martine BLONDEAU (*)
Asystent ds. dokumentacji

Andrea BEACH
Asystent ds. sekretariatu

Matteo BONFANTI
Stażysta (październik 2007 – styczeń 2008)

Marie MCGINLEY
Stażysta (marzec–lipiec 2007)

(*) Zespół ds. informacji.

Europejski inspektor ochrony danych i jego zastępca wraz z zespołem

Sekcja Personel – Budżet – Administracja

Monique LEENS-FERRANDO
Kierownik sekcji

- **Zasoby ludzkie – Administracja**

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

Anne LEVÊCQUE
Asystent ds. zasobów ludzkich

Vittorio MASTROJENI
Asystent ds. zasobów ludzkich

Anne-Françoise REYNDERS
Asystent ds. zasobów ludzkich

- **Budżet i finanse**

Tonny MATHIEU
Administrator ds. finansów

Valérie LEAU
Asystent ds. księgowości

Raja ROY
Asystent ds. finansów i księgowości

Załącznik I

Wykaz porozumień administracyjnych i decyzji

Porozumienie administracyjne podpisane przez sekretarza generalnego Parlamentu Europejskiego, sekretarza generalnego Rady i sekretarza generalnego Komisji oraz przez Europejskiego Inspektora Ochrony Danych (24 czerwca 2004 r.). W dniu 11 grudnia 2006 r. podpisano przedłużenie obowiązywania tego porozumienia.

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

- Porozumienia o gwarantowanym poziomie usług zawarte z Komisją (Biuro ds. Szkoleń DG ds. Edukacji i Kultury; DG ds. Personelu i Administracji; DG ds. Zatrudnienia, Spraw Społecznych i Równości Szans)
- Porozumienie o gwarantowanym poziomie usług zawarte z Radą
- Porozumienie o gwarantowanym poziomie usług zawarte z Europejską Szkołą Administracji (ESA)
- Porozumienie administracyjne zawarte między EIOD a Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA)
- Porozumienie w sprawie harmonizacji kosztów międzyinstytucjonalnych kursów językowych
- Dwustronne porozumienie między Parlamentem Europejskim i EIOD w sprawie wdrożenia porozumienia administracyjnego z dnia 24 czerwca 2004 r., przedłużonego w dniu 11 grudnia 2006 r.

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 określenia długości stażu pracy w momencie mianowania lub podjęcia pracy

Decyzja EIOD z dnia 15 czerwca 2005 r. w sprawie przyjęcia elastycznego czasu pracy z możliwością odebrania 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 długości kadencji

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

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

Decyzja EIOD z dnia 7 listopada 2005 r. ustanawiająca procedury kontroli wewnętrznej stosowane w odniesieniu do EIOD

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

Decyzja z dnia 16 stycznia 2006 r. zmieniająca decyzję EIOD z dnia 22 czerwca 2005 r. w sprawie przyjęcia wspólnych zasad ubezpieczenia urzędników Wspólnot Europejskich od ryzyka wypadku i choroby zawodowej

Decyzja 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 jako 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

Decyzja EIOD z dnia 30 stycznia 2007 r. w sprawie mianowania urzędnika ds. ochrony danych w ramach EIOD

Decyzja EIOD z dnia 30 marca 2007 r. w sprawie przyjęcia ogólnych przepisów wykonawczych dotyczących systemu oceniania pracowników

Decyzja EIOD z dnia 18 lipca 2007 r. w sprawie przyjęcia polityki w zakresie szkoleń wewnętrznych

Decyzja EIOD z dnia 1 października 2007 r. w sprawie mianowania księgowego w ramach EIOD

Decyzja EIOD z dnia 1 października 2007 r. w sprawie wdrożenia art. 4 załącznika VIII regulaminu pracowniczego w zakresie dotyczącym uprawnień emerytalnych

Decyzja EIOD z dnia 1 października 2007 r. w sprawie wdrożenia art. 11 i 12 załącznika VIII regulaminu pracowniczego w zakresie dotyczącym przenoszenia uprawnień emerytalnych

Decyzja EIOD z dnia 1 października 2007 r. w sprawie wdrożenia art. 22 ust. 4 załącznika XIII regulaminu pracowniczego w zakresie dotyczącym uprawnień emerytalnych

Decyzja EIOD z dnia 12 września 2007 r. w sprawie zasad i warunków prowadzenia dochodzeń wewnętrznych w sprawie zapobiegania nadużyciom finansowym, korupcji oraz każdej innej nielegalnej działalności naruszającej interesy Wspólnot

Decyzja EIOD z dnia 9 listopada 2007 r. w sprawie mianowania audytora wewnętrznego w ramach EIOD

Decyzja EIOD z dnia 26 listopada 2007 r. w sprawie przyjęcia ogólnych przepisów wykonawczych dotyczących awansu zawodowego

Europejski Inspektor Ochrony Danych

Sprawozdanie roczne 2007

Luksemburg: Urząd Oficjalnych Publikacji Wspólnot Europejskich

2008 – 116 str. – 21 x 29,7 cm

ISBN 978-92-95030-50-3

Jak otrzymać publikacje UE

Płatne publikacje Urzędu Publikacji są dostępne w EU Bookshop http://bookshop.europa.eu. Ze strony tej można złożyć zamówienie na publikacje w dowolnym biurze sprzedaży.

Pełną listę sprzedawców naszych publikacji na całym świecie można uzyskać, wysyłając faks pod numer (352) 2929 42758.

EUROPEJSKI INSPEKTOR
OCHRONY DANYCH

QT-AA-08-001-PL-N

Europejski strażnik ochrony danych osobowych

www.edps.europa.eu

Urząd Publikacji
Publications.europa.eu