ISSN 1830-9518

Sprawozdanie roczne

2010

Sprawozdanie roczne

2010

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 portalu Europa (http://europa.eu).

Dane katalogowe znajdują się na końcu niniejszej publikacji.

Luksemburg: Urząd Publikacji Unii Europejskiej, 2010

ISBN 978-92-95073-20-3
doi:10.2804/2085

Printed in Luxembourg

WYDRUKOWANO NA PAPIERZE BIELONYM BEZ CHLORU PIERWIASTKOWEGO (ECF)

Spis treści

3 KONSULTACJE

4 WSPÓŁPRACA

5 KOMUNIKACJA

6 ADMINISTRACJA, BUDŻET I PERSONEL

7 INSPEKTOR OCHRONY DANYCH (IOD) EIOD

PRZEWODNIK UŻYTKOWNIKA

Bezpośrednio po niniejszym przewodniku zamieszczono deklarację misji oraz przedmowę autorstwa Europejskiego Inspektora Ochrony Danych (EIOD) Petera Hustinxa i jego zastępcy, Giovanniego Buttarellego.

Rozdział 1 – Najważniejsze wydarzenia 2010 r. – przedstawia główne działania EIOD w 2010 r. oraz wyniki osiągnięte w poszczególnych dziedzinach.

Rozdział 2 – Nadzór i egzekwowanie prawa – opisuje działania wdrażane w celu monitorowania i zapewnienia wykonania przez instytucje i organy UE obowiązków związanych z ochroną danych. W rozdziale tym przedstawiono analizę najważniejszych kwestii związanych z kontrolami wstępnymi, dalszymi działaniami dotyczącymi skarg, monitorowaniem przestrzegania przepisów oraz doradztwem w zakresie środków administracyjnych w 2010 r. Zaprezentowano także wytyczne tematyczne przyjęte przez EIOD w dziedzinie dochodzeń administracyjnych i postępowań dyscyplinarnych oraz dalsze prace w zakresie wytycznych dotyczących nadzoru wideo. Rozdział ten przedstawia również nową politykę EIDO w zakresie przestrzegania i egzekwowania prawa.

Rozdział 3 – Konsultacje – obejmuje działania EIDO dotyczące jego funkcji doradczej, koncentrując się na jego opiniach i uwagach na temat wniosków ustawodawczych i dokumentów pokrewnych, jak również na ich skutkach dla coraz większej liczby dziedzin. Rozdział ten zawiera również omówienie zaangażowania EIDO w sprawy przed Trybunałem Sprawiedliwości. Zawiera on analizę spraw ogólnych: wybranych nowych zagadnień technologicznych oraz nowych działań w zakresie polityki i prawodawstwa.

Rozdział 4 – Współpraca – opisuje działania podejmowane w ramach najważniejszych forów, takich jak Grupa Robocza Art. 29 ds. Ochrony Danych, oraz podczas europejskich i międzynarodowych konferencji dotyczących ochrony danych. Opisuje on również skoordynowany nadzór (przez EIDO i krajowe organy ochrony danych) nad wielkoskalowymi systemami informatycznymi.

Rozdział 5 – Komunikacja – przedstawia działania i osiągnięcia EIDO w zakresie informacji i komunikacji, w tym komunikacji zewnętrznej z mediami, wydarzeń służących zwiększaniu świadomości, informacji dla społeczeństwa oraz narzędzi informacyjnych on-line.

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

Rozdział 7 – Inspektor Ochrony Danych (IOD) EIOD – przedstawia prace nowego zespołu IOD EIOD. Bazując na planie działania IOD i przyjętych przepisach wykonawczych, podkreśla on postęp osiągnięty w zakresie rejestru powiadomień, w zakresie zgodności z operacją „Wiosna" oraz w zakresie zapotrzebowania na informacje i zwiększanie świadomości.

Rozdział 8 – Główne cele na 2011 r. – opisuje pokrótce przyszłe działania i najważniejsze priorytety na 2011 r.

Sprawozdanie uzupełnia szereg **załączników**. Zawierają one przegląd właściwych ram prawnych, w tym przepisów rozporządzenia (WE) nr 45/2001, wykaz inspektorów ochrony danych, wykazy opinii EIOD dotyczących kontroli wstępnych i opinii konsultacyjnych, informacje o wystąpieniach EIOD i jego zastępcy, a także skład Sekretariatu EIOD.

Dostępne jest również streszczenie niniejszego sprawozdania, którego celem jest przedstawienie w skrótowej formie najważniejszych aspektów działalności EIOD w 2010 r.

Więcej informacji na temat EIOD można uzyskać na naszej stronie internetowej pod adresem http://www.edps.europa.eu. Można tam również zaprenumerować nasz biuletyn.

Egzemplarze papierowe sprawozdania rocznego i streszczenia można zamówić bezpłatnie w EU Bookshop (http://www.bookshop.europa.eu).

DEKLARACJA MISJI

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

EIOD jest odpowiedzialny za:

- monitorowanie i zapewnienie przestrzegania przepisów rozporządzenia (WE) nr 45/2001[1], jak również innych aktów UE dotyczących ochrony podstawowych praw i wolności w trakcie przetwarzania danych osobowych przez instytucje i organy UE („nadzór");
- doradzanie instytucjom i organom UE we wszystkich sprawach związanych z przetwarzaniem danych osobowych; obejmuje to konsultacje w sprawie wniosków ustawodawczych oraz monitorowanie nowych wydarzeń, które mają wpływ na ochronę danych osobowych („konsultacje");
- współpracę z krajowymi instytucjami oraz organami nadzorczymi w ramach dawnego „trzeciego filaru" UE w celu poprawienia spójności ochrony danych osobowych („współpraca").

W związku z powyższym EIOD stawia sobie za cel prowadzenie strategicznych działań służących:

- promowaniu „kultury ochrony danych" w instytucjach i organach, przyczyniając się również tym samym do poprawy standardów dobrej administracji;
- włączeniu poszanowania zasad ochrony danych do prawodawstwa i polityki UE we wszystkich stosownych przypadkach;
- poprawieniu jakości polityki UE we wszelkich sytuacjach, gdy skuteczna ochrona danych stanowi podstawowy warunek jej powodzenia.

[1] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 2001, s. 1).

PRZEDMOWA

Mamy przyjemność przedłożyć Parlamentowi Europejskiemu, Radzie i Komisji Europejskiej roczne sprawozdanie z działalności Europejskiego Inspektora Ochrony Danych (EIOD) zgodnie z rozporządzeniem (WE) nr 45/2001 Parlamentu Europejskiego i Rady oraz z art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, który zastąpił obecnie art. 286 Traktatu WE.

Niniejsze sprawozdanie obejmuje rok 2010 jako szósty pełny rok działalności EIOD w charakterze nowego, niezależnego organu nadzoru mającego za zadanie zapewnienie poszanowania przez instytucje i organy UE podstawowych praw i wolności osób fizycznych, w szczególności ich prywatności, w odniesieniu do przetwarzania danych osobowych. Obejmuje ono również drugi rok wspólnej pięcioletniej kadencji obecnych członków tego organu.

Omawiany rok był ponownie bardzo ważny z punktu widzenia podstawowego prawa do ochrony danych. Traktat lizboński, zapewniający mocne podstawy prawne całościowej ochrony danych we wszystkich dziedzinach polityki UE, miał coraz bardziej widoczny wpływ. Proces przeglądu ram prawnych UE w zakresie ochrony danych postępuje i przyciąga coraz większą uwagę. Dwa kluczowe programy polityczne – program sztokholmski w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz agenda cyfrowa jako podstawa strategii „Europa 2020" – podkreślają istotność ochrony danych jako podstawowego elementu zasadniczości oraz skuteczności działań w obu obszarach.

EIOD wykazał się dużym zaangażowaniem w tych poszczególnych kontekstach i pragnie w najbliższej przyszłości kontynuować ten kierunek działań. Jednocześnie zapewniliśmy wywiązywanie się z roli niezależnego organu nadzoru we wszystkich podstawowych obszarach działalności i w pełni odpowiednią jej organizację. Doprowadziło to do znaczących postępów zarówno w nadzorze nad przetwarzającymi dane osobowe instytucjami i organami UE, jak i w konsultacjach dotyczących nowej polityki oraz środków legislacyjnych, a także w zakresie ścisłej współpracy z innymi organami nadzorczymi w celu zapewnienia bardziej spójnej ochrony danych.

Chcielibyśmy zatem skorzystać ze sposobności, aby podziękować wszystkim tym w Parlamencie Europejskim, Radzie i Komisji, którzy wspierają naszą pracę, a także wielu innym osobom w różnych instytucjach i organach, które są odpowiedzialne za sposób realizacji ochrony danych w praktyce. Kierujemy też słowa zachęty do osób stawiających czoła ważnym wyzwaniom przyszłości.

Wreszcie pragniemy szczególnie podziękować naszym pracownikom. Nieprzeciętne zalety personelu EIOD wydatnie zwiększają skuteczność naszych działań.

Peter Hustinx
Europejski Inspektor Ochrony Danych

Giovanni Buttarelli
Zastępca Inspektora

1 NAJWAŻNIEJSZE WYDARZENIA 2010 R.

1.1. Najważniejsze wydarzenia

Kilka ostatnich wydarzeń przyczyniło się do postawienia **praw podstawowych i ochrony danych** w centrum europejskiej agendy. **Traktat lizboński**, wchodząc w życie w dniu 1 grudnia 2009 r., zwiększył ochronę praw podstawowych w Unii Europejskiej (UE) poprzez przyznanie Karcie Praw Podstawowych takiego samego znaczenia prawnego jak traktatom oraz uprawnienie UE do przystąpienia do **Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności (EKPC).** Poprzez szczególne uwzględnienie ochrony danych art. 16 TFUE stanowi ogólną podstawę prawną dla ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucje i organy UE oraz przez państwa członkowskie, kiedy wykonują one zadania, które mieszczą się w zakresie prawa UE.

Istotność praw podstawowych w ogólności i ochrony danych w szczególności została ponadto podkreślona w **programie sztokholmskim**, obecnym pięcioletnim programie politycznym w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Program kładzie nacisk na potrzebę zapewnienia poszanowania praw podstawowych, wolności i integralności osób, przy jednoczesnym zagwarantowaniu bezpieczeństwa. Odpowiednio poszanowanie praw człowieka i godności oraz innych praw ustanowionych w Karcie i w EKPC, w szczególności prawo do prywatności i ochrony danych, zostały określone jako kluczowe wartości dla działań Europy w tym obszarze. Co ważne – Rada Europejska zwróciła się do Komisji o złożenie wniosku o przystąpienie Unii do EKPC „w trybie pilnym".

Te wydarzenia były również wspierane przez inne instytucje. W związku z programem sztokholmskim Parlament Europejski znacząco podkreślił rolę praw podstawowych dla dalszego rozwoju przestrzeni wolności, bezpieczeństwa i sprawiedliwości[2]. Sama Komisja niedawno przyjęła komunikat określający strategię skutecznego wprowadzania w życie Karty w nowym środowisku prawnym istniejącym od chwili wejścia w życie traktatu lizbońskiego.

Proces przeglądu ram ochrony danych rozpoczęty w 2009 r. i kontynuowany w 2010 r., jest zasadniczym elementem Europy praw podstawowych. W listopadzie 2010 r. Komisja opublikowała komunikat przedstawiający całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej. Komunikat przedstawia podejście Komisji do unowocześnienia ram prawnych UE w zakresie ochrony danych osobowych we wszystkich obszarach działalności Unii. Komunikat ma na celu stawienie czoła wyzwaniom wynikającym z globalizacji i nowych technologii, w celu zapewnienia wysokiego poziomu ochrony danych w przyszłości. EIOD śledzi uważnie proces przeglądu i wpływał już na ten proces na wielu etapach. Projekt ten będzie również jednym z jego głównych priorytetów w 2011 r.

W 2010 r. Komisja poczyniła również znaczne wysiłki w celu wdrożenia różnych inicjatyw związanych z programem sztokholmskim. Kilka z tych

[2] Rezolucja Parlamentu Europejskiego z dnia 25 listopada 2009 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady: „Przestrzeń wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli" – program sztokholmski, P7_TA(2009)0090.

wniosków jest oparte na intensywnej wymianie danych pomiędzy organami ścigania lub bezpieczeństwa publicznego poszczególnych państw i, tym samym, ma znaczący wpływ na prywatność i ochronę danych osób fizycznych. Rozwijając **przestrzeń wolności, bezpieczeństwa i sprawiedliwości,** europejskie władze prawodawcze ciągle muszą utrzymywać równowagę pomiędzy bezpieczeństwem, swobodnym przepływem obywateli i ochroną ich prywatności i danych osobowych. Wdrożenie programu sztokholmskiego jest kluczowym elementem działań EIOD w 2010 r. i prawdopodobnie będzie nim nadal w przyszłości.

Inne ważne wydarzenia tego roku dotyczą problematyki ochrony danych w kontekście **nowych technologii.** Dzisiejsza technologia pozwala na wymianę i przetwarzanie danych na bezprecedensową skalę. Jednocześnie przetwarzanie danych stało się bardziej subtelne i trudniejsze do wykrycia. Sieci społecznościowe, obliczenia rozproszone, pobieranie opłat drogowych, urządzenia geolokacyjne, reklama behawioralna i inne podobne nowe usługi – wszystkie stanowią ogromne wyzwanie dla ochrony danych. Przegląd ram prawnych ochrony danych będzie musiał skutecznie stawić czoła tym wyzwaniom w celu zapewnienia wysokiego poziomu ochrony danych w świecie napędzanym technologiami. Nowe technologie są również w centrum inicjatyw zawartych w europejskiej agendzie cyfrowej Komisji. EIOD będzie analizował i oceniał te inicjatywy w każdym przypadku, gdy będą one wiązały się z zagadnieniami ochrony danych osób fizycznych.

1.2. Ogólny przegląd 2010 r.

Najważniejsze działania EIOD w 2010 r. opierały się na tej samej strategii ogólnej co poprzednio, ale nadal zwiększała się zarówno ich skala, jak i zakres. Poprawie uległy także możliwości skutecznego i sprawnego działania EIOD.

Ramy prawne[3], wewnątrz których działa EIOD, obejmują liczne zadania i uprawnienia. Można tu rozróżnić trzy podstawowe funkcje. Funkcje te stanowią nadal strategiczne płaszczyzny działań EIOD i są ujęte w deklaracji misji:

- **funkcja nadzorcza** polegająca na monitorowaniu i zapewnieniu poszanowania przez instytucje i organy UE[4] istniejących gwarancji prawnych podczas przetwarzania danych osobowych;
- **funkcja konsultacyjna** polegająca na udzielaniu instytucjom i organom UE porad we wszystkich stosownych kwestiach, w szczególności w sprawie wniosków ustawodawczych mających wpływ na ochronę danych osobowych;
- **funkcja współpracy** z krajowymi instytucjami oraz organami nadzorczymi w ramach dawnego „trzeciego filaru" UE, obejmująca współpracę policyjną i wymiarów sprawiedliwości w sprawach karnych w celu poprawienia spójności ochrony danych osobowych.

Funkcje te zostaną szerzej omówione w rozdziałach 2, 3 i 4 niniejszego sprawozdania rocznego, w których przedstawiono główne działania EIOD i postępy poczynione w 2010 r. Niektóre najważniejsze elementy zostaną podsumowane w niniejszej części.

Znaczenie informowania i komunikowania o tych działaniach w pełni uzasadnia odrębne omówienie komunikacji w rozdziale 5. Wszystkie powyższe działania bazują na skutecznym zarządzaniu zasobami finansowymi, ludzkimi i innymi, co przedstawiono w rozdziale 6.

Nadzór

Zadania nadzoru obejmują doradztwo i wparcie dla inspektorów ochrony danych poprzez kontrole wstępne stanowiące zagrożenie operacji przetwarzania danych, jak również prowadzenie dochodzeń (w tym kontroli na miejscu) oraz rozpatrywanie skarg. Pozostałe doradztwo dla administracji UE może też przyjąć postać konsultacji w sprawie środków administracyjnych lub publikacji wytycznych tematycznych.

Każda instytucja i organ UE musi zatrudniać co najmniej jednego **inspektora ochrony danych** (IOD). W 2010 r. łączna liczba inspektorów ochrony danych

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

[4] Terminy „instytucje" i „organy" z rozporządzenia (WE) nr 45/2011 są używane w całym sprawozdaniu. Obejmują one także agencje UE. Ich pełną listę można znaleźć pod adresem: http//europa.eu/agencies/community_agencies/index.en.htm

wzrosła do 47. Regularne kontakty z inspektorami i siecią, w ramach której działają, są ważnym warunkiem skutecznego nadzoru. W celu koordynacji sieci inspektorów ochrony danych utworzony został „kwartet IOD" złożony z czterech inspektorów (Rady, Parlamentu Europejskiego, Komisji Europejskiej oraz Centrum Tłumaczeń dla Organów Unii Europejskiej). EIOD blisko współpracuje z tym kwartetem.

Kontrole wstępne operacji przetwarzania danych stwarzających zagrożenie pozostawały w 2010 r. głównym aspektem nadzoru. EIOD przyjął 55 opinii dotyczących kontroli wstępnych związanych ze standardowymi procedurami administracyjnymi, takimi jak ocena pracowników, rekrutacja i procedury awansowania, ale również w zakresie podstawowej działalności, takiej jak system wczesnego ostrzegania i reagowania do wymiany informacji o chorobach zakaźnych. Opinie te są publikowane na stronach internetowych EIOD, a wykonanie zaleceń jest systematycznie monitorowane.

Systematycznie monitorowane jest również **wdrażanie rozporządzenia** przez instytucje i organy – regularnie badane są wskaźniki wydajności dla wszystkich instytucji i organów UE. Od opearcji dotyczącej ogólnego monitorowania, przeprowadzonej wiosną 2009 r., EIOD kontynuuje monitorowanie wdrożenia reguł i zasad ochrony danych przez zaangażowane instytucje i organy. Kolejna opearcja dotycząca ogólnego monitorowania (opearcja „Wiosna 2011") rozpocznie się na początku 2011 r. Tam gdzie w wyniku wykonywanych przez EIOD czynności nadzorczych pojawiły się obawy co do poziomu przestrzegania przepisów przez konkretne instytucje lub organy, przeprowadzono również ukierunkowane działania monitorujące. Niektóre z nich były oparte na korespondencji, podczas gdy inne miały formę wizyt w odpowiednich organach. W 2010 r. EIOD odbył dwie takie wizyty. EIOD przeprowadził również kontrolę na miejscu we Wspólnym Centrum Badawczym Komisji w Isprze w celu weryfikacji zgodności z przepisami w zakresie wybranych zagadnień.

W 2010 r. łączna liczba skarg wyniosła 94, lecz tylko 25 z nich zostały uznane za dopuszczalne. Wiele niedopuszczalnych skarg dotyczyło zagadnień na szczeblu krajowym, które nie wchodzą w zakres kompetencji EIOD. Większość dopuszczalnych skarg dotyczyła domniemanego naruszenia poufności związanego z dostępem do danych i ich poprawianiem, bezprawnego wykorzystania danych, gromadzenia nadmiernej ilości danych i usuwania danych. W 11 przypadkach EIOD doszedł do wniosku, że zasady ochrony danych zostały naruszone.

Podejmowano również dalsze prace związane z **konsultacjami w sprawie środków administracyjnych** planowanych przez instytucje i organy UE w odniesieniu do przetwarzania danych osobowych. Pojawiły się różnorodne zagadnienia, w tym międzynarodowe przekazywanie danych, dostęp do tożsamości informatora, wewnętrzne wykorzystania e-maili i zdalne monitorowanie.

EIOD przyjął **wytyczne** w zakresie dochodzeń administracyjnych i postępowań dyscyplinarnych oraz nadzoru wideo.

W grudniu 2010 r. EIOD przyjął dokument zatytułowany „Monitorowanie i zapewnianie zgodności z rozporządzeniem (WE) nr 45/2001" (*Monitoring and Ensuring Compliance with Regulation (EC) 45/2001*). Dokument ten określa ramy, w których EIOD monitoruje, ocenia i zapewnia zgodność ochrony danych w administracji UE. Przedstawia on charakter różnych **uprawnień do egzekwowania prawa** dostępnych dla EIOD i określa czynniki i warunki wszelkich działań formalnych, które mogą zostać przez niego podjęte.

Konsultacje

W 2010 r. Komisja poczyniła znaczący postęp w kierunku nowych, **zmodernizowanych ram prawnych ochrony danych w Europie**. Konsultacja społeczna rozpoczęta w 2009 r. została zakończona i uzupełniono ją o dalsze, ukierunkowane konsultacje z wieloma kluczowymi zainteresowanymi stronami. W listopadzie 2010 r. Komisja wydała komunikat określający całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej, identyfikując ścisłe priorytety i kluczowe cele dla przeglądu istniejących zasad.

EIOD poświęcał szczególną uwagę procesowi przeglądu przez 2010 r. i przekazywał swoje uwagi na różne sposoby. W szczególności EIOD zorganizował specjalną konferencję prasową tuż po publikacji komunikatu w celu publicznego wyrażenia swojego poglądu na temat nowych ram prawnych. Przy tej okazji EIOD podkreślił ważność przeglądu, który w jego ocenie ma miejsce w odpowiednim momencie i wyraził opinię na temat głównych elementów nowych ram.

EIOD nadal wdrażał ogólną **politykę w dziedzinie konsultacji**, wydając rekordową liczbę 19 opinii

dotyczących wniosków ustawodawczych z różnych dziedzin. Polityka ta obejmuje także aktywne podejście oparte na regularnym sporządzaniu spisu wniosków ustawodawczych, które mają zostać przedłożone do konsultacji, oraz gotowości do zgłaszania nieoficjalnych uwag na etapie przygotowywania wniosków ustawodawczych. Większość opinii EIOD była później omawiana w Parlamencie i Radzie.

W 2010 r. EIOD śledził dokładnie kilka z inicjatyw bezpośrednio związanych z wdrożeniem **programu sztokholmskiego**. Między innymi EIOD zajmował się zasadniczymi kwestiami ochrony danych związanymi ze strategią bezpieczeństwa wewnętrznego UE, zarządzaniem informacją w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, unijną polityką zwalczania terroryzmu, rozporządzeniami Frontex i Eurodac. Ogólnie rzecz biorąc, działania dotyczące programu sztokholmskiego były dominującym elementem w haromonogramie prac EIOD i tak będzie też w najbliższych latach.

Związek pomiędzy prywatnością a postępem technicznym był również obszarem, w którym EIOD aktywnie działał. W maju 2010 r. Komisja opublikowała komunikat dotyczący europejskiej agendy cyfrowej, którego celem było określenie priorytetów UE w obszarze Internetu i technologii cyfrowych. W marcu 2010 r. EIOD przyjął opinię w sprawie „wspierania zaufania w społeczeństwie informacyjnym poprzez działanie na rzecz ochrony danych i prywatności" jako swój wkład do strategii cyfrowej. Interweniował on na różne sposoby w inicjatywy związane z Internetem i neutralnością sieci, przeglądem dyrektywy w sprawie zatrzymywania danych, dyrektywy w sprawie e-odpadów, rozporządzenia w sprawie agencji ENISA oraz e-sprawiedliwości.

EIOD wypowiadał się również na temat różnych inicjatyw w obszarze **współpracy międzynarodowej w dziedzinie bezpieczeństwa i egzekwowania prawa**, takich jak ogólna umowa UE-USA w sprawie wymiany danych w celu egzekwowania prawa oraz umowa w sprawie wymiany danych finansowych do celów programu śledzenia środków finansowych należących do terrorystów (TFTP II). Interweniował on również w odniesieniu do umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA) oraz umów w sprawie wymiany danych dotyczących przelotu pasażera (PNR).

EIOD interweniował również w innych obszarach, takich jak podatki i cło (w tym współpraca administracyjna w obszarze opodatkowania i międzynarodowa współpraca celna), wielkoskalowa wymiana danych w kontekście systemu wymiany informacji na rynku wewnętrznym, użytkowanie skanerów ciała w portach lotniczych oraz różne sprawy sądowe dotyczące związku między dostępem publicznym a ochroną danych.

Współpraca

Podstawową platformą współpracy między organami ochrony danych w Europie jest **Grupa Robocza Art. 29 ds. Ochrony Danych**. EIOD bierze udział w działaniach Grupy Roboczej, która odgrywa ważną rolę w jednolitym stosowaniu dyrektywy o ochronie danych.

EIOD oraz Grupa Robocza Art. 29 nawiązali owocną współpracę w wielu kwestiach, szczególnie jednak w związku z wdrożeniem dyrektywy o ochronie danych i interpretacją niektórych z jej kluczowych zapisów. EIOD wspierał aktywnie inne obszary, takie jak opinie w sprawie pojęcia „administratora danych" i „przetwarzającego", zasady rozliczalności i prawa właściwego.

EIOD uczestniczy również w spotkaniach i działaniach Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości, grupy doradczej zajmującej się zagadnieniami z obszaru dawnego trzeciego filaru.

Jedno z najważniejszych zadań EIOD w ramach współpracy wiąże się z systemem **Eurodac** – w którym odpowiedzialność za nadzór spoczywa równocześnie na Inspektorze oraz na krajowych organach ochrony danych. Grupa ds. Koordynowania Nadzoru nad Systemem Eurodac, w skład której wchodzą krajowe organy ochrony danych oraz EIOD, zebrała się w Brukseli trzykrotnie, w marcu, październiku i grudniu 2010 r. Grupa rozpoczęła prace nad przygotowaniem pełnego audytu bezpieczeństwa, który miałby zostać przeprowadzony przez organy ochrony danych, zarówno na poziomie krajowym, jak i centralnym (UE). Nowa, skoordynowana kontrola została rozpoczęta pod koniec 2010 r. i oczekuje się jej wyników w 2011 r.

W odniesieniu do nadzoru nad **systemem informacji celnej (CIS)** EIOD zwołał w 2010 r. dwa spotkania z Grupą ds. Koordynowania Nadzoru nad Systemem CIS. Spotkania zgromadziły przedstawicieli krajowych organów ochrony danych, jak również przedstawicieli Wspólnego Celnego Organu Nadzorczego i Sekretariatu Ochrony Danych. Podczas grudniowego spotkania Grupa przyjęła regulamin wewnętrzny, który będzie regulował przyszłe

prace w zakresie CIS oraz omówiła możliwe działania do podjęcia w latach 2011-2012 w celu zapewnienia całościowego nadzoru nad ochroną danych w ramach systemu.

EIOD kontynuował ścisłą współpracę z organami utworzonymi w celu przeprowadzenia **wspólnego nadzoru nad wielkoskalowymi systemami informatycznymi w UE**.

Zainteresowanie budziła nadal współpraca na **innych forach międzynarodowych**, zwłaszcza podczas Europejskiej i Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, które miały miejsce, odpowiednio, w Pradze i Jerozolimie.

We współpracy z Uniwersytetem Europejskim we Florencji, EIOD zorganizował również warsztat na temat „**ochrony danych w organizacjach międzynarodowych**". Warsztat analizował różne wyzwania, z którymi mierzą się organizacje międzynarodowe próbujące zapewnić dobry poziom ochrony danych w niejednokrotnie trudnych warunkach i bez jasnych podstaw prawnych.

1.3. Wyniki 2010

Poniższe najważniejsze cele określono w 2009 r. Większość z nich została w pełni lub częściowo zrealizowana.

- **Wspieranie sieci inspektorów ochrony danych**

EIOD nadal mocno wspierał inspektorów ochrony danych, zachęcając ich do wymiany wiedzy fachowej i najlepszych praktyk. W ramach swojej sieci

Najważniejsze dane liczbowe dotyczące działalności EIOD w 2010 r.

➔ **Przyjęto 55 opinii dotyczących kontroli wstępnych** związanych z danymi dotyczącymi zdrowia, oceną personelu, rekrutacją, zarządzaniem czasem, dochodzeniami w sprawie bezpieczeństwa, nagrywaniem rozmów telefonicznych oraz narzędziami do pomiaru wydajności

➔ **Wpłynęły 94 skargi, z tego 25 dopuszczalne.** Główne rodzaje zarzucanych naruszeń: naruszenie poufności danych, gromadzenie nadmiernej ilości danych lub bezprawne wykorzystanie danych przez administratora.

•**Rozstrzygnięto 10 spraw**, w których EIOD nie stwierdził naruszenia zasad ochrony danych

•**11 stwierdzonych przypadków niezgodności** z zasadami ochrony danych

➔ **35 konsultacji dotyczących środków administracyjnych.** Udzielano porad dla szeregu kwestii prawnych związanych z przetwarzaniem danych osobowych przez instytucje i organy UE

➔ **Przeprowadzono 1 kontrolę na miejscu**

➔ **Opublikowano 2 zestawy wytycznych** w zakresie dochodzeń administracyjnych i postępowań dyscyplinarnych oraz nadzoru wideo

➔ **Wydano 19 opinii w zakresie wniosków ustawodawczych**, dotyczących przestrzeni wolności, bezpieczeństwa i sprawiedliwości, postępu technicznego, współpracy międzynarodowej, przekazywania danych, podatków i ceł

➔ **Wydano 7 oficjalnych uwag** dotyczących między innymi zmian w rozporządzeniu Frontex, otwartego Internetu i neutralności sieci, systemu wymiany informacji na rynku wewnętrznym, skanerów ciała, międzynarodowych umów w sprawie wymiany danych

➔ **Zorganizowano 3 spotkania Grupy ds. Koordynowania Nadzoru nad Systemem Eurodac**, w wyniku których rozpoczęto nową skoordynowaną kontrolę, a także przygotowania do pełnego audytu bezpieczeństwa

➔ **zatrudniono 12 nowych urzędników**

inspektorzy ochrony danych opracowali dokument „Profesjonalne standardy dla inspektorów ochrony danych instytucji i organów UE pracujących na podstawie rozporządzenia (WE) nr 45/2001" (*Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) No 45/2001*). Dokument ten został ukończony w październiku 2010 r. EIOD wysłał pismo do szefów wszystkich instytucji i agencji, zatwierdzające standardy i podkreślające istotną rolę inspektorów ochrony danych w osiągnięciu zgodności z zasadami ochrony danych określonymi w rozporządzeniu.

- **Rola kontroli wstępnych**

EIOD prawie już zakończył kontrole wstępne prowadzonych operacji przetwarzania danych w przypadku większości instytucji i organów działających od dłuższego czasu, kładąc coraz większy nacisk na monitorowanie realizacji zaleceń. W tym roku 137 spraw zostało zamkniętych. Szczególną uwagę poświęcono kontrolom wstępnym operacji przetwarzania danych wspólnych dla większej liczby agencji, czego efektem było ujęcie tych spraw we wspólnych opiniach.

- **Wytyczne horyzontalne**

W celu zapewnienia przestrzegania przepisów przez instytucje i organy oraz usprawnienia procedur kontroli wstępnych EIOD opublikował wytyczne w zakresie dochodzeń administracyjnych i postępowań dyscyplinarnych oraz nadzoru wideo.

- **Polityka kontroli**

W 2010 r. EIOD kontynuował działania następcze wynikające z wcześniejszych kontroli. Ponadto EIOD przeprowadził kontrolę we Wspólnym Centrum Badawczym (JRC) Komisji w Isprze. W grudniu 2010 r. EIOD opublikował całościową politykę w zakresie monitorowania zgodności z zadami ochrony danych i ich egzekwowania w instytucjach i organach.

- **Zakres konsultacji**

Sporządziwszy systematyczny spis stosownych tematów i priorytetów, EIOD wydał rekordową liczbę 19 opinii i 7 zestawów oficjalnych uwag na temat wniosków dotyczących nowego prawodawstwa; zapewniono też właściwe dalsze monitorowanie tych spraw. Wszystkie opinie i uwagi, jak też sam spis dostępne są na stronie internetowej. Szczególną uwagę przywiązano do planu działania w zakresie wdrażania programu sztokholmskiego.

- **Przegląd ram prawnych**

Przy różnych okazjach, przy użyciu różnych narzędzi EIOD dążył do ambitnego podejścia w celu stworzenia nowoczesnych, całościowych ram ochrony danych, które pokrywałyby wszystkie obszary polityki UE i zapewniały skuteczną ochronę w praktyce, dzięki czemu uzyskano by pewność prawa na wiele lat. Poglądy EIOD zostały obecnie także przedstawione w opinii wydanej w styczniu 2011 r.

- **Agenda cyfrowa**

EIOD skoncentrował działania w obszarze konsultacji na najważniejszych wyzwaniach dla skutecznej ochrony danych osobowych. Oznacza to zapewnienie właściwej równowagi pomiędzy potrzebą bezpieczeństwa i ochrony danych, przy uwzględnieniu postępu technicznego i skutków przepływów danych w skali globalnej. Szczególną uwagę poświęcono agendzie cyfrowej Komisji w opinii przyjętej w marcu 2010 r., omawiając szczegółowo zasadę „wbudowanej ochrony prywatności".

- **Działania informacyjne**

EIOD w dalszym ciągu zwiększał jakość i skuteczność działań komunikacyjnych i narzędzi informacyjnych. Znaczącym osiągnięciem w tym zakresie było wprowadzenie języka niemieckiego jako trzeciego języka, po angielskim i francuskim, w działaniach prasowych i komunikacyjnych.

- **Organizacja wewnętrzna**

Sekretariat EIOD został przeorganizowany w celu uściślenia zakresów obowiązków i zapewnienia bardziej wydajnego i skutecznego wykonania poszczególnych zadań i ról. W nowej strukturze organizacyjnej dyrektor zapewnia wdrożenie strategii i koordynację horyzontalną działań mających miejsce w pięciu różnych sektorach. Nowa struktura organizacyjna jest dostępna na stronie internetowej.

- **Zarządzanie zasobami**

W ciągu 2010 r. znacząco (o jedną trzecią) wzrosła liczba pracowników EIOD. W związku z wewnętrzną reorganizacją wymagane były nowe działania w zakresie planowania, procedur wewnętrznych i wykonania budżetu. Szczególną uwagę poświęcono potrzebie zapewnienia dodatkowej przestrzeni biurowej i rozwojowi systemu zarządzania obiegiem spraw.

2 NADZÓR I EGZEKWOWANIE PRAWA

2.1. Wprowadzenie

Zadaniem EIOD, w ramach powierzonej mu roli niezależnego nadzorcy, jest monitorowanie przeprowadzanego przez instytucje lub organy UE procesu przetwarzania danych (z wyjątkiem Trybunału Sprawiedliwości, który działa jako władza sądownicza). Rozporządzenie (WE) nr 45/2001 („rozporządzenie") określa i wskazuje szereg obowiązków oraz uprawnień umożliwiających EIOD wykonywanie tego zadania.

Wraz z wprowadzeniem art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, który zastępuje art. 286 Traktatu WE, traktat lizboński wprowadza zmianę do ram prawnych ochrony danych w administracji europejskiej. Rezygnacja z filarowej struktury doprowadziła do sytuacji, w której zadania nadzorcze EIOD zasadniczo obejmują obecnie wszystkie instytucje i organy UE – w tym w obszarach wychodzących całkowicie poza zakres tego, co niegdyś określano jako „prawo wspólnotowe"[5] – z wyjątkiem przypadków, w których inne akty UE stanowią wyraźnie inaczej. Dokładne skutki tych zmian w zakresie działań nadzorczych EIOD nadal podlegają analizie i mogą wymagać szczegółowego omówienia.

Kontrola wstępna czynności przetwarzania pozostawała ważnym aspektem nadzoru w 2010 r. (zob. pkt 2.3), ze szczególnym naciskiem na monitorowanie zaleceń poczynionych w jego opiniach. EIOD rozwinął również inne formy nadzoru, takie jak rozpatrywanie skarg, kontrole, doradztwo w zakresie środków administracyjnych oraz opracowywanie wytycznych tematycznych. Specyficznym obszarem działalności EIOD, wymagającym ścisłej współpracy z krajowymi organami ochrony danych, jest nadzór nad systemem Eurodac (zob. pkt 4.2).

EIOD przyjął również politykę w zakresie przestrzegania i egzekwowania prawa, sygnalizującą zmianę kierunku we wdrażaniu rozporządzenia.

2.2. Inspektorzy ochrony danych

Interesującą zasadą w zakresie ochrony danych w instytucjach Unii Europejskiej jest obowiązek wyznaczenia inspektora ochrony danych (IOD) (art. 24 ust. 1 rozporządzenia). Niektóre instytucje oprócz inspektora powołały również jego zastępcę. Komisja wyznaczyła także inspektora ochrony danych dla Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF – jedna z dyrekcji generalnych Komisji). Wiele instytucji wyznaczyło też koordynatorów ds. ochrony danych w celu koordynowania wszystkich aspektów ochrony danych w danej dyrekcji lub dziale.

W 2010 r. w nowych agencjach lub w ramach wspólnych przedsięwzięć mianowano 2 nowych inspektorów, w wyniku czego ich łączna liczba wyniosła 47.

Od kilku lat inspektorzy spotykają się regularnie w celu wymiany wspólnych doświadczeń

5 Zob. art. 3 ust. 1 rozporządzenia (WE) nr 45/2001, który ma obecnie mniejsze znaczenie niż przed dniem 1 grudnia 2009 r.

i omówienia ogólnych zagadnień. Ta nieformalna sieć okazała się przydatnym narzędziem współpracy i funkcjonowała także w 2010 r.

W celu koordynacji sieci utworzono „kwartet" złożony z czterech inspektorów (Rady, Parlamentu Europejskiego, Komisji Europejskiej oraz Centrum Tłumaczeń dla Organów Unii Europejskiej). EIOD ściśle współpracował z tym kwartetem.

EIOD brał udział w spotkaniach inspektorów zorganizowanych w marcu 2010 r. w Europejskim Banku Inwestycyjnym w Luksemburgu oraz w Europejskiej Agencji Leków w Londynie w październiku 2010 r., wykorzystując tę okazję na przekazanie inspektorom aktualnych informacji o swojej pracy, przedstawienie przeglądu najnowszych wydarzeń w dziedzinie ochrony danych w UE oraz omówienie zagadnień będących przedmiotem zainteresowania obu stron.

EIOD wykorzystał to forum do wyjaśnienia i omówienia procedury kontroli wstępnych, przedstawienia postępów w powiadamianiu o kontrolach wstępnych; zaktualizowania wiedzy inspektorów o dyskusjach w komitetach międzyinstytucjonalnych; wyjaśnienia nowej struktury EIOD i przedstawienia wytycznych tematycznych EIOD. EIOD poinformował również inspektorów o przyjęciu polityki przestrzegania i egzekwowania prawa. Forum jest również wykorzystywane do wymiany informacji na temat inicjatyw związanych z Europejskim Dniem Ochrony Danych (28 stycznia).

W ramach swojej sieci inspektorzy ochrony danych opracowali dokument „Profesjonalne standardy dla inspektorów ochrony danych instytucji i organów UE pracujących na podstawie rozporządzenia (WE) nr 45/2001". Dokument ten został ukończony podczas spotkania sieci IOD w dniu 14 października 2010 r. EIOD wysłał pismo do szefów wszystkich instytucji i agencji, zatwierdzający standardy i podkreślający istotną rolę inspektorów ochrony danych w osiągnięciu zgodności z zasadami ochrony danych określonymi w rozporządzeniu. EIOD planuje w oparciu o ten dokument budować, w stosownych przypadkach, swoją rolę nadzorczą w odniesieniu do instytucji i organów.

2.3. Kontrole wstępne

2.3.1. Podstawa prawna

Artykuł 27 ust. 1 rozporządzenia (WE) nr 45/2001 przewiduje, że operacje przetwarzania, mogące ze swej natury przez swój zakres lub swoje cele stworzyć konkretne zagrożenia dla praw i wolności podmiotów danych, podlegają uprzedniemu sprawdzeniu przez EIOD (art. 27 ust. 1).

Artykuł 27 ust. 2 rozporządzenia zawiera przykładowy wykaz operacji przetwarzania danych, które mogą stworzyć takie zagrożenia. Przy interpretacji

Inspektorzy ochrony danych w czasie spotkania w Brukseli (marzec 2010 r.).

tego przepisu nadal stosowano kryteria opracowane w poprzednich latach[6] – zarówno przy decydowaniu, że dane powiadomienie ze strony inspektora ochrony danych nie podlega kontroli wstępnej, jak i w związku z doradztwem dotyczącym potrzeby przeprowadzenia kontroli wstępnej (zob. też pkt 2.3.4).

2.3.2. Procedura

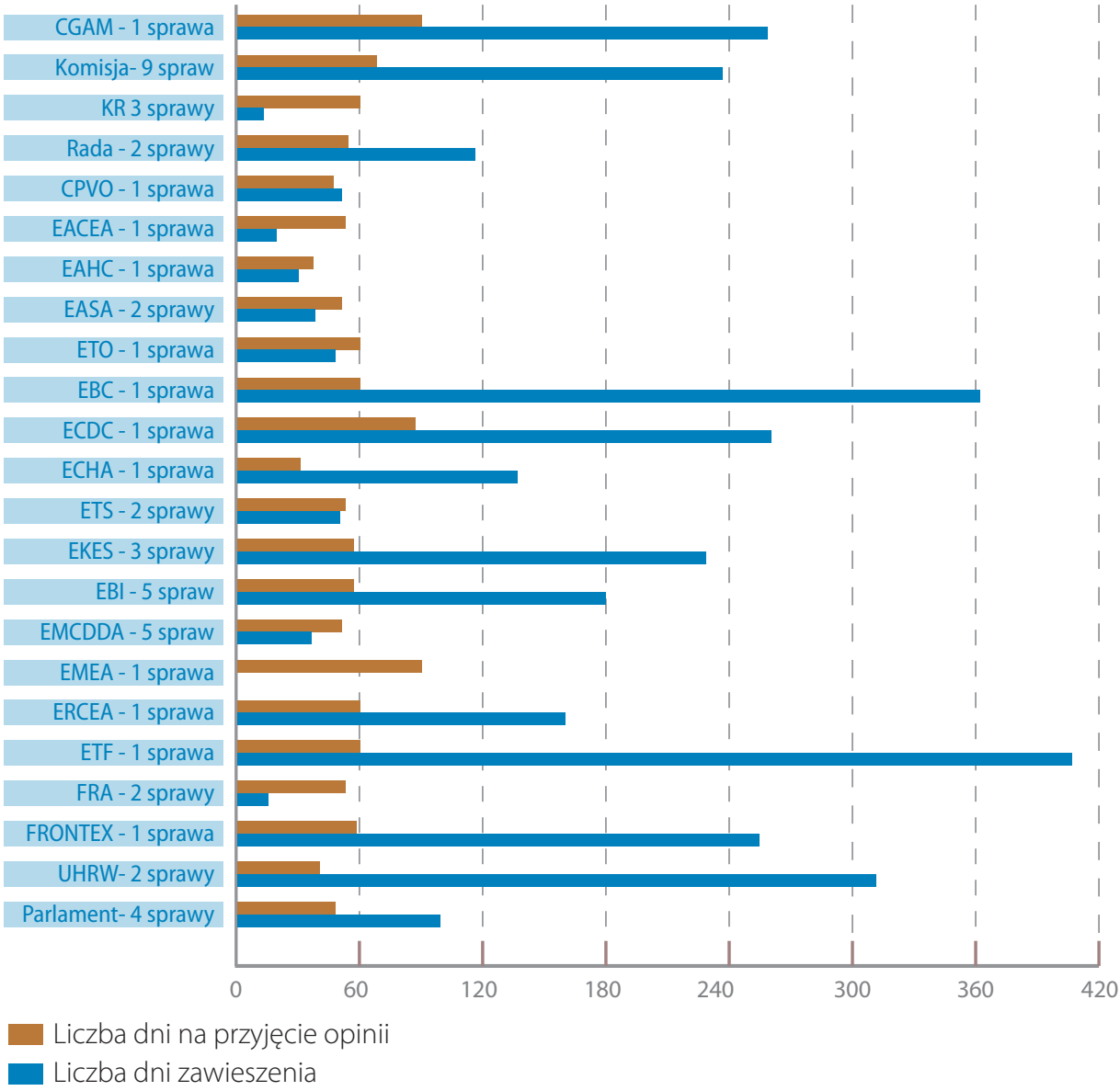
Powiadomienie

EIOD ma obowiązek przeprowadzać kontrole wstępne po otrzymaniu powiadomienia ze strony inspektora ochrony danych. W przypadku gdy inspektor ma wątpliwości, czy daną operację przetwarzania należy poddać kontroli wstępnej, może skonsultować się z EIOD (zob. pkt 2.3.4).

Kontrole wstępne dotyczą nie tylko operacji, które jeszcze się nie rozpoczęły, lecz również przetwarzania, które rozpoczęło się przed dniem 17 stycznia 2004 r. (data mianowania pierwszego EIOD oraz jego zastępcy) lub przed wejściem rozporządzenia w życie (kontrole wstępne *ex post*). W takich sytuacjach kontrola na podstawie art. 27 nie może być „wstępna" w ścisłym sensie tego słowa, lecz musi nastąpić na zasadzie *ex post*.

6 Zob. sprawozdanie roczne 2005, pkt 2.3.1

Średni czas według instytucji/agencji



Termin, zawieszenie i przedłużenie

EIOD musi wydać opinię w terminie dwóch miesięcy od otrzymania powiadomienia[7]. W przypadku gdy EIOD zwraca się z wnioskiem o dostarczenie dodatkowych informacji, bieg tego dwumiesięcznego terminu ulega zwykle zawieszeniu do chwili uzyskania takich informacji przez EIOD. Ten okres zawieszenia obejmuje czas przysługujący danemu inspektorowi ochrony danych na zgłoszenie uwag oraz w razie potrzeby – na przedłożenie dodatkowych informacji dotyczących wersji ostatecznej. W złożonych przypadkach EIOD może również przedłużyć początkowy okres o kolejne dwa miesiące. Jeżeli do końca dwumiesięcznego okresu lub jego przedłużenia nie zostanie doręczona żadna decyzja, przyjmuje się, że opinia EIOD jest pozytywna. Do tej pory nie było przypadku wydania takiej milczącej zgody.

Rejestr

W 2010 r. EIOD otrzymał 89 powiadomień dotyczących kontroli wstępnych. Liczba ta jest nieznacznie niższa w porównaniu z 2009 r., gdyż EIOD likwiduje ostatnie zaległości związane z kontrolami wstępnymi ex post.

Rozporządzenie stanowi, że EIOD musi prowadzić rejestr wszystkich operacji przetwarzania, o których został powiadomiony w celu przeprowadzenia kontroli wstępnej (art. 27 ust. 5). Rejestr ten musi zawierać informacje, o których mowa w art. 25, i być ogólnodostępny. Aby zapewnić przejrzystość, wszystkie informacje są zawarte w publicznym rejestrze dostępnym na stronie internetowej EIOD (z wyjątkiem środków bezpieczeństwa, które nie są wymieniane w rejestrze).

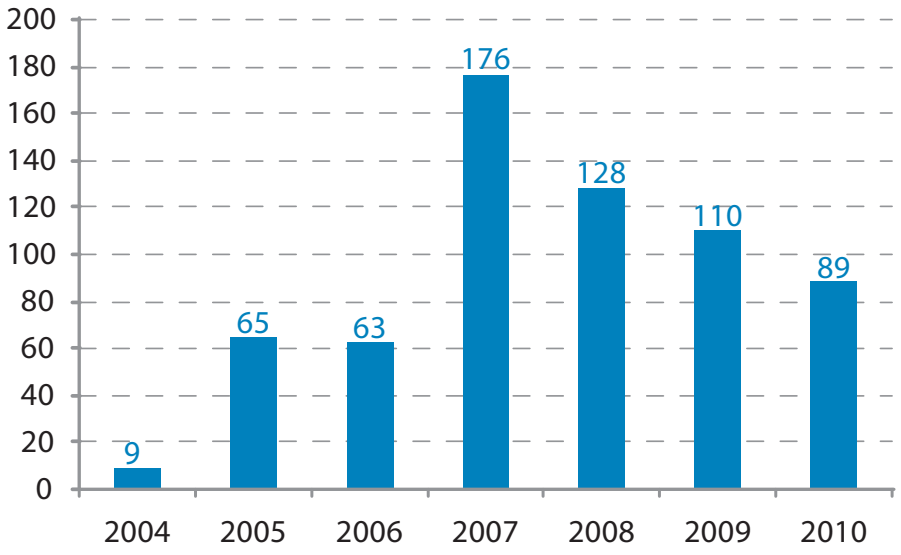
Opinie

Stanowisko końcowe EIOD przyjmuje formę opinii, o której należy powiadomić administratora danej operacji przetwarzania danych oraz inspektora ochrony danych danej instytucji lub organu (art. 27 ust. 4). W 2010 r. EIOD wydał **55 opinii dotyczących kontroli wstępnych** (zob. wykres „Liczba opinii EIOD dotyczących kontroli wstępnych rocznie" powyżej) i **8 opinii dotyczących kontroli niewstępnych** (zob. powyżej pkt 2.3.5). Jest to spadek w porównaniu z poprzednimi latami, należy jednak zauważyć, że po wydaniu wytycznych w zakresie nadzoru wideo i rekrutacji EIOD miał do czynienia ze znaczną liczbą spraw w ramach wspólnych opinii, dzięki czemu analizował te kwestie w bardziej wydajny sposób.

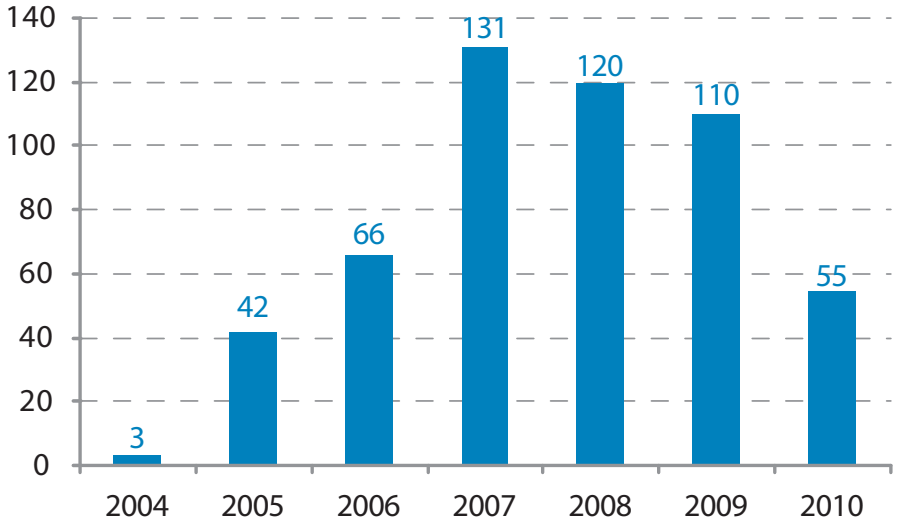
Większość tych opinii została sporządzona dla **dużych instytucji**: dziewięć opinii dotyczących kontroli wstępnych (i trzy opinie dotyczące kontroli niewstępnych) odnosiło się do operacji przetwarzania danych w Komisji Europejskiej, cztery – do operacji w Parlamencie Europejskim i trzy – w Radzie (zob. wykres „Opinie EIOD według instytucji"). Agencje kontynuowały również wystosowywanie powiadomień o swojej podstawowej działalności i standardowych procedurach

7 Spraw ex-post, które wpłynęły przed dniem 1 września 2010 r. sierpnia, nie policzono ani dla instytucji i organów, ani dla EIOD.

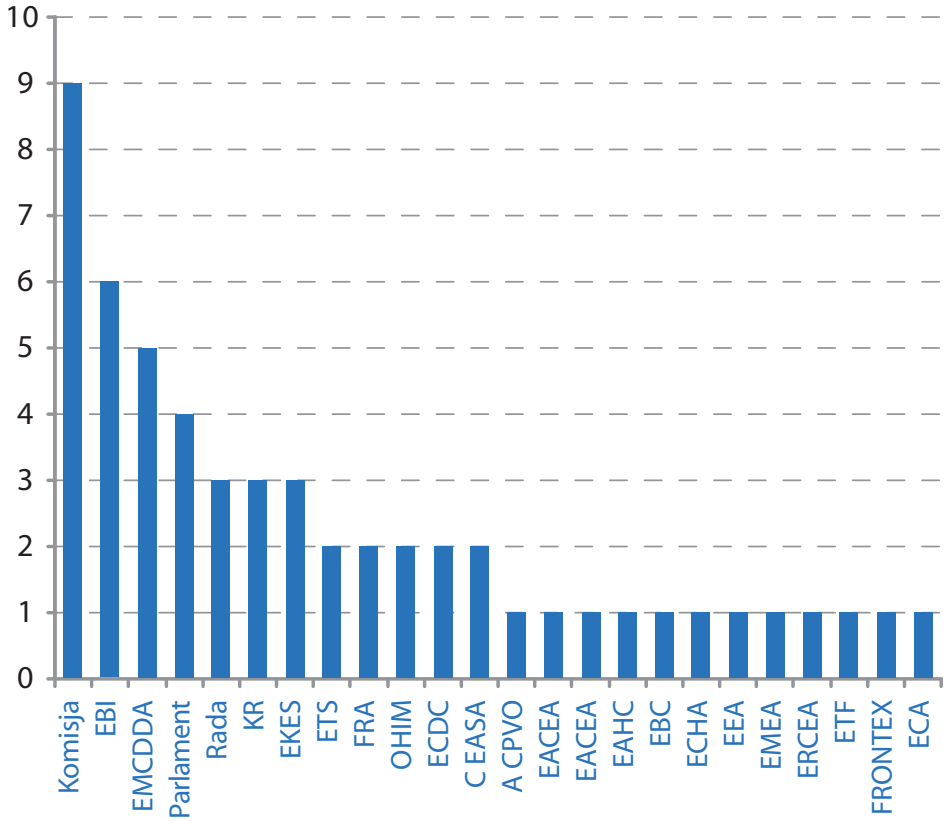
Powiadomienia kierowane do EIOD



Liczba opinii EIOD dotyczących kontroli wstępnych rocznie



Liczba opinii EIOD dotyczących kontroli wstępnych według instytucji w 2010 r.



administracyjnych zgodnie ze stosownymi procedurami opracowanymi przez EIOD (zob. pkt 2.3.2).

Opinie zawierają opis postępowania, podsumowanie stanu faktycznego oraz analizę prawną stwierdzającą, czy operacja przetwarzania danych jest zgodna ze stosownymi przepisami rozporządzenia. W razie potrzeby wydawane są zalecenia dla administratora danych służące zapewnieniu zgodności z rozporządzeniem. We wnioskach EIOD stwierdza zazwyczaj, że przetwarzanie danych nie wydaje się naruszać przepisów rozporządzenia pod warunkiem uwzględnienia wydanych zaleceń.

Opinie wydawane przez EIOD są upubliczniane. Wszystkie opinie są dostępne na stronie internetowej EIOD wraz z podsumowaniem danej sprawy.

Opracowany podręcznik zapewnia opieranie się przez cały zespół na takich samych podstawach i przyjmowanie opinii EIOD po pełnej analizie wszystkich istotnych informacji. Zawiera on szablon opinii opracowany na podstawie zebranego doświadczenia i jest stale aktualizowany. Wdrożono system przepływu pracy, który ma zapewnić monitorowanie wszystkich zaleceń w danej sprawie oraz w stosownych przypadkach – wdrożenie wszystkich decyzji wykonawczych (zob. pkt 2.3.6).

Procedura kontroli wstępnych *ex post* w agencjach

W październiku 2008 r. EIOD wdrożył nową procedurę przeprowadzania kontroli wstępnych *ex post* w agencjach UE. Ponieważ standardowe procedury są takie same w większości agencji UE i opierają się na decyzjach Komisji, polega ona na zebraniu powiadomień na podobne tematy i przyjęciu opinii zbiorczej (dla różnych agencji) lub przeprowadzeniu „minikontroli wstępnej" dotyczącej jedynie cech szczególnych konkretnej agencji. Aby pomóc agencjom w sporządzeniu powiadomień, EIOD przedkłada podsumowanie najważniejszych punktów i wniosków na dany temat w oparciu o poprzednie opinie dotyczące kontroli wstępnych w formie wytycznych tematycznych (zob. pkt 2.7 Wytyczne tematyczne).

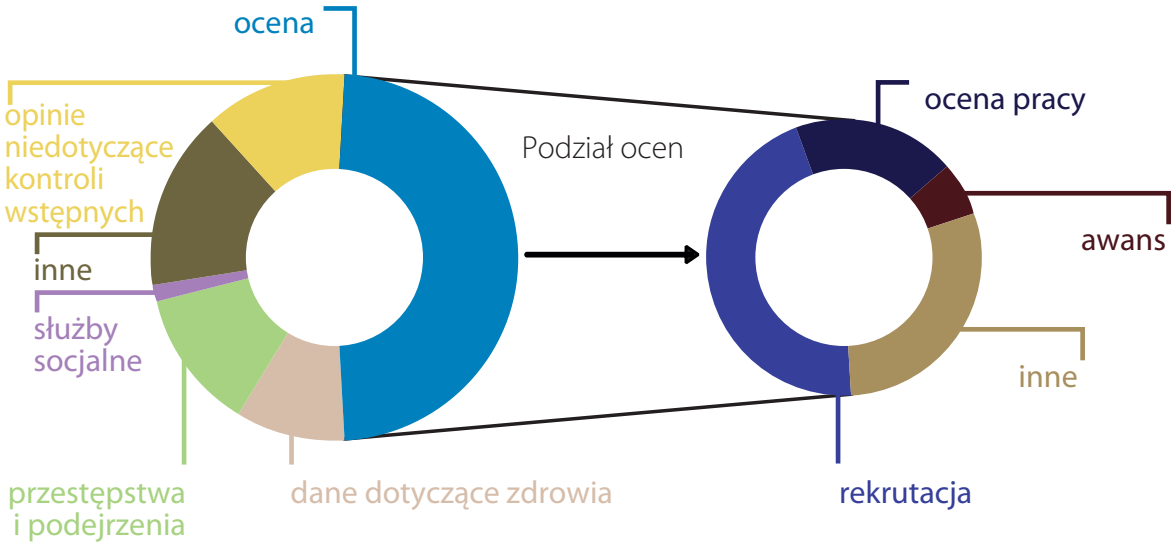
Pierwszym tematem była **rekrutacja**, w związku z którą EIOD wydał w maju 2009 r. opinię horyzontalną obejmującą powiadomienia z 12 agencji. Drugi zestaw wytycznych na temat **przetwarzania danych dotyczących zdrowia** przesłano agencjom pod koniec września 2009 r. W czasie sporządzania wytycznych EIOD przesłał projekt swojej opinii horyzontalnej do 19 agencji mających przedstawić swoje uwagi do niej i liczy na przyjęcie jej na początku 2011 r. W kwietniu 2010 r. EIOD wydał wytyczne dotyczące przetwarzania danych osobowych w **dochodzeniach administracyjnych i postępowaniach dyscyplinarnych** prowadzonych przez europejskiej instytucje i organy. Obecnie EIOD otrzymuje powiadomienia od agencji z tej dziedziny i zamierza przyjąć wspólną opinię w pierwszej połowie 2011 r.

2.3.3. Najważniejsze zagadnienia związane z kontrolami wstępnymi

2.3.3.1. System wczesnego ostrzegania i reagowania – Komisja Europejska

System wczesnego ostrzegania i reagowania (EWRS) jest narzędziem komunikacji wykorzystywanym przez Komisję, Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) i państwa członkowskie UE do wymiany informacji dotyczących zapobiegania chorobom zakaźnym (takim jak gruźlica, odra, SARS, H1N1 i inne) w celu ułatwienia działań transgranicznych. Jednym z elementów EWRS jest „**ustalanie kontaktów**" – procedura wykorzystywana do

Opinie w 2009 r. według kategorii



zidentyfikowania osób, które mogły wejść w kontakt z zarażoną osobą, i skontaktowania się z nimi. Po ustaleniu kontaktów można przebadać takie osoby i zastosować leczenie. Ustalenie kontaktów służy także ogólnym interesom zdrowia publicznego poprzez ograniczanie lub uniemożliwianie dalszego rozprzestrzeniania się choroby.

W swojej opinii (sprawa 2009-0137) EIOD skoncentrował się na potrzebie **wyraźnego wyznaczenia ról, zadań i obowiązków** stron zaangażowanych w obsługę i stosowanie systemu, w szczególności ról Komisji i ECDC. Należy jasno określić administratorów danych i podmioty przetwarzające zgodnie z ich odpowiednimi faktycznymi rolami oraz ustalić status prawny zaangażowanych organizacji.

Należy jasno określić obowiązki stron zaangażowanych i sposób, w jaki osoby, których dane dotyczą, mogą wykonywać swoje prawa. Tymczasowo zalecono, by EWRS przyjął zestaw wytycznych w zakresie ochrony danych. Zachęcano również Komisję do przeglądu ram prawnych w celu zapewnienia bezpieczniejszej podstawy prawnej i jasnego podziału obowiązków.

Ponadto EIOD podkreślił potrzebę wdrożenia zasady „**wbudowanej ochrony prywatności**" i włączenia ochrony danych do szkolenia oferowanego użytkownikom. Powinno się zapewnić jasny mechanizm wykonywania **prawa dostępu** dla osób, których dane dotyczą. W końcu, w celu zapewnienia spójności i przejrzystości operator EWRS powinien zapewnić na stronie internetowej systemu pełne i przyjazne dla użytkownika informacje dla osób, których dotyczą. Obok tego powinny funkcjonować powiadomienia dostarczane przez punkty kontaktowe państw członkowskich zgodnie z krajowymi przepisami w zakresie ochrony danych.

2.3.3.2. Europejski System Nadzoru ('TESSy') – Europejskie Centrum ds. Zapobiegania i Kontroli Chorób

Dnia 3 września 2010 r. EIOD wydał opinię dotyczącą kontroli wstępnej (sprawa 2009-0474) w zakresie aspektów ochrony danych TESSy. TESSy to narzędzie komunikacji Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób, mające zapewnić szybką i efektywną wymianę danych na temat nadzoru epidemiologicznego pomiędzy państwami członkowskimi UE.

System EWRS to narzędzie komunikacji do wymiany informacji na temat chorób zakaźnych.

Opinia wyjaśnia, że **dane statystyczne** nadal uważa się za „dane osobowe", a więc nadal są one objęte rozporządzeniem, jeśli osoby fizyczne można co najmniej pośrednio zidentyfikować. Fakt „zastosowania" pewnych „technik anonimizacji" niekoniecznie oznacza, że dane uznaje się za „zanonimizowane" w rozumieniu motywu 8 rozporządzenia, a tym samym przestaje się je uznawać za „dane osobowe".

EIOD przywołał wiele zaleceń wystosowanych w jego opinii dotyczącej EWRS (zob. powyżej) i dodał, że należy niezwłocznie przyjąć szczegółową polityką bezpieczeństwa w celu zapewnienia bezpieczeństwa TESSy.

2.3.3.3. Wspólny program ubezpieczeń zdrowotnych

Wspólny Komitet ds. Zarządzania Ubezpieczeniami Zdrowotnymi (JSIMC) jest odpowiedzialny za funkcjonowanie wspólnego programu ubezpieczeń zdrowotnych. JSIMC składa się z przedstawicieli pracowników wyznaczonych przez Komitety Pracownicze każdej instytucji oraz przedstawicieli administracji. Rozpatruje on wszelkie zmiany regulaminu, skargi członków oraz wydaje opinie, zalecenia i wnioski dotyczące funkcjonowania programu.

EIOD spotkał się z JSIMC w listopadzie 2008 r. w celu omówienia kwestii ochrony danych w odniesieniu do dokumentacji, którą zarządza JSIMC. Ponieważ skargi członków stowarzyszonych zawierają dane szczególnie chronione, postanowiono, że Komitet prześle powiadomienie do EIOD.

Powiadomienie to zaowocowało opinią (sprawa 2009-0070), wydaną w dniu 18 stycznia 2010 r., w której EIOD wystosował zalecenia w szczególności w zakresie **przekazywania danych osobowych do** JSIMC; **okresu zatrzymywania danych** w CIRCA (aplikacja sieciowa dla zespołów pracowniczych korzystających ze wspólnych danych) oraz przyjęcia **odpowiedniej polityki bezpieczeństwa** w ciągu sześciu miesięcy od dnia przyjęcia opinii.

2.3.3.4. Kontrole bezpieczeństwa – Komisja Europejska (DG ds. Wspólnego Centrum Badawczego w Isprze)

W dniu 6 września 2010 r. (sprawa 2009-0682) EIOD wydał opinię dotyczącą kontroli wstępnej w zakresie kontroli bezpieczeństwa we Wspólnym Centrum Badawczym Komisji Europejskiej w Isprze. Dotyczyła ona operacji przetwarzania danych przeprowadzonych w celu utrzymania i poprawy obowiązujących norm bezpieczeństwa.

EIOD uznał, że „Procedura in caso d'infortunio" wiąże się z przetwarzaniem danych dotyczących zdrowia przez kilka stron w celu zapobiegania skutkom podobnych zdarzeń istotnych z punktu widzenia bezpieczeństwa i minimalizowania ich występowania na terenie Ispry.

EIOD wydał zalecenia w celu **zagwarantowania przestrzegania zasady „celowości" w przypadku przekazywania danych** oraz **zgodności z zasadami jakości danych** mających zastosowanie do przechowywania i dalszego przetwarzania danych osobowych przetwarzanych w tym kontekście. Zalecono również odpowiednią zmianę istniejącego oświadczenia o ochronie prywatności.

2.3.3.5. Role zespołowe BELBINa – Europejska Szkoła Administracji

Celem przetwarzania danych jest umożliwienie uczestnikom szkoleń Europejskiej Szkoły Administracji (EAS) uzyskania informacji zwrotnej w formie sprawozdania na temat preferowanej roli w zespole. Dane nie są wykorzystywane do jakiejkolwiek formy oceny danej osoby. W swojej opinii z dnia 15 marca 2010 r. (sprawa 2009-0377) EIOD skoncentrował się na dwóch aspektach:

- **związek pomiędzy administratorem danych, podmiotem przetwarzającym a podwykonawcą:** nawet jeśli EAS nie ma dostępu do danych przetwarzanych przez podwykonawcę, podwykonawca musi działać zgodnie z instrukcjami przekazanymi wykonawcy przez EAS. EAS pełni rolę administratora danych tych czynności przetwarzania danych, ponieważ to ona określa cele i sposoby wykorzystania danych (narzędzie sieciowe). Trzej wykonawcy odpowiedzialni za ofertę szkolenia oraz podwykonawca odpowiedzialny za narzędzie sieciowe – wszystkie te podmioty uznaje się za

podmioty przetwarzające dane osobowe, działające w imieniu EAS. Podwykonawca nie jest upoważniony do przeprowadzenia żadnych czynności przetwarzania danych poza określonymi przez EAS i wyszczególnionymi w umowie pomiędzy podwykonawcą a wykonawcą, zgodnie z umową pomiędzy EAS a wykonawcą;

- **anonimowy charakter danych:** sprawozdań przedstawionych uczestnikom nie można uznać za „anonimowe", ponieważ podwykonawca może połączyć odpowiedzi z osobami, których dane dotyczą, jako że uczestnicy zazwyczaj używają adresu e-mail, który określa ich imię i nazwisko.

EIOD wydał zalecenia w dwóch powyższych aspektach, w szczególności wskazując, że umowa powinna zawierać klauzule dotyczące wszystkich wymaganych elementów, w szczególności **poufności i bezpieczeństwa przetwarzania danych** pomiędzy wykonawcą a podwykonawcą.

2.3.3.6. Zdalne monitorowanie — Trybunał Obrachunkowy

Procedura **dostępu do prywatnych dysków i e-maili** została opracowana przez **Trybunał Obrachunkowy** (ETO) z myślą o różnych sytuacjach (np. śmierć pracownika, odejście pracownika z instytucji lub niestawienie się w pracy), w których to informacje zawarte na tych nośnikach są niezbędne dla funkcjonowania instytucji. Proponowana procedura wymaga od osoby składającej wniosek o informacje wypełnienia standardowego formularza. Wniosek powinien zawierać szczegółowy opis powodu(ów) uzasadniającego(-ych) udzielenie dostępu, nazwę pliku(-ów) lub konta e-mail, lub przedmiot informacji. Formularz należy przesłać do kierownika ds. bezpieczeństwa informacji, a pod jego nieobecność, do kierownika ds. bezpieczeństwa fizycznego.

Procedura dostępu do prywatnych dysków i e-maili została opracowana w Trybunale Obrachunkowym.

Pierwotnie wniosek został przesłany do EIOD do konsultacji, jako że ta procedura **potencjalnie dotyczyła dostępu do poufnych danych**, a EIOD rzeczywiście uznał, że operacja przetwarzania wiąże się ze szczególnym ryzykiem wymagającym powiadomienia do celów kontroli wstępnej.

W opinii z dnia 10 stycznia 2010 r. (sprawa 2009-0620) EIOD zalecił przyjęcie przez ETO **specjalnej podstawy prawnej** dla wykorzystania i przechowywania prywatnej poczty elektronicznej i wprowadzenie przez Trybunał jasnych wytycznych dla użytkownika w zakresie wykorzystania zasobów sieci i e-maili.

2.3.3.7. Obniżenie pensji w razie strajku – Europejski Bank Centralny

Zgodnie z art. 1.4 regulaminu pracowniczego Europejskiego Banku Centralnego (EBC) pracownicy mają prawo do strajku. Art. 1.4.5 stanowi, że „O ile Zarząd nie postanowi inaczej, całkowity okres strajku jest odliczany od wypłat pensji pracownika biorącego udział w strajku". Ponadto „nie można podjąć żadnych czynności dyscyplinarnych wobec pracownika biorącego udział w strajku, chyba że został on wyznaczony do wykonania minimalnych usług opisanych powyżej i nie wykonuje ich ze względu na udział w strajku" (art. 1.4.7).

Zważywszy, że udział w strajku wiąże się z automatycznym obniżeniem pensji i innych dodatków, przetwarzanie danych związane z tym obniżeniem podlega kontroli wstępnej przez EIOD, ponieważ wiąże się z przetwarzaniem danych, które pozbawia jednostki prawa lub świadczenia lub wyłącza je z umowy.

W dniu 28 września 2010 r. EIOD wydał opinię dotyczącą kontroli wstępnej (sprawa 2009-0514) w zakresie takiej operacji przetwarzania danych, wystosowując zalecenia dotyczące **okresów zatrzymywania** dokumentacji przechowywanej w systemie elektronicznych dokumentów i zapisów EBC oraz **informacji**, jakie należy dostarczyć osobom, których dane dotyczą.

2.3.3.8. Dochodzenia w sprawie nadużyć finansowych – Europejski Bank Inwestycyjny

Wydział Dochodzeń w sprawie Nadużyć Finansowych (IG/IN) Europejskiego Banku Inwestycyjnego (EBI) analizuje zarzuty zakazanych praktyk zgodnie z procedurami zwalczania nadużyć finansowych EBI. Do celów przeprowadzenia dochodzeń IG/IN ma pełny dostęp do wszystkich istotnych informacji, dokumentów i danych na temat pracowników, w tym danych elektronicznych w obrębie EBI, choć niedozwolone jest przechwytywanie wiadomości czy rozmów. Kierownik IG/IN określi, czy skarga lub zarzut są uzasadnione i przekaże sprawę odpowiednim organom w obrębie lub poza EBI, by podjęły odpowiednie działania. Jeśli po odpowiednim dochodzeniu IG/IN ustali, że skarga lub zarzut nie były uzasadnione, udokumentuje wnioski w piśmie dołączonym do akt i zamknie sprawę.

EIOD wydał opinię dotyczącą kontroli wstępnej (sprawa 2009-0459) w zakresie operacji przetwarzania danych w odniesieniu do takich dochodzeń w sprawie nadużyć finansowych i zalecił, by EBI przeanalizował **podstawę prawną** tych dochodzeń; przyjął **oficjalny protokół do prowadzenia komputerowych oficjalnych** dochodzeń; ujednolicił okresy zatrzymywania danych i zapewnił informacje osobom, których dane dotyczą.

2.3.3.9. Empiryczna analiza korelacji pomiędzy zmiennymi systemu pracy a procesem decyzyjnym – Urząd Harmonizacji Rynku Wewnętrznego

Ta wstępna kontrola (sprawa 2010-0468) obejmowała aspekty ochrony danych projektu prowadzonego przez Urząd Harmonizacji Rynku Wewnętrznego (UHRW) zatytułowanego „Empiryczna analiza korelacji pomiędzy zmiennymi systemu pracy a procesem decyzyjnym". Celem tej analizy było umożliwienie określenia porównywalnych profili stanowisk i opracowanie najlepszych praktyk w zarządzaniu zasobami ludzkimi dla tych profili. Obok praktycznych korzyści dla UHRW projekt miał także dodatkowe cele naukowe, ponieważ analityk przeprowadzający badanie zaplanował publikację wniosków

Wydział Dochodzeń w sprawie nadużyć finansowych EBI bada zarzuty dotyczące zakazanych praktyk.

w pracy doktorskiej (po ostrożnym zredagowaniu tekstu w celu ochrony prywatności osób uczestniczących w projekcie). EIOD wystosował kilka zaleceń, w szczególności odnośnie do zatrzymywania danych, przekazywania danych osobom trzecim i informacji dla osób, których dane dotyczą.

EIOD zalecił, by wszystkie dane osobowe z serwerów UHRW zostały usunięte na koniec okresu zatrzymywania danych (2011 r.). EIOD zalecił również analitykowi uwzględnienie obowiązujących przepisów krajowych odnoszących się do danych jednostkowych zatrzymywanych do potencjalnych przyszłych celów badawczych lub przekazywanych osobom trzecim w celu zapewnienia zgodności z wymogami w zakresie konieczności, celu i poufności.

2.3.3.10. Centralna baza danych o wykluczeniach – Komisja Europejska

W celu ochrony finansowych interesów instytucji, na podstawie rozporządzenia finansowego Komisja Europejska przetwarza dane, które są zawarte w centralnej bazie danych o wykluczeniach. Takie dane mogą zostać wykorzystane wyłącznie do celów wykluczenia jednostek, które stanowią zagrożenie dla europejskich interesów finansowych, ze wszelkich procedur dotyczących zamówień lub dotacji finansowanych z funduszy UE lub Europejskiego Funduszu Rozwoju.

Od wstępnego etapu EIOD przeprowadzał swoją analizę (sprawa 2009-0681) w pełnej współpracy z instytucją.

EIOD doszedł do wniosku, iż nie było podstaw, aby uznać, że doszło do naruszenia przepisów rozporządzenia o ochronie danych. Wydał on jednak pewne zalecenia dotyczące wcześniejszych informacji dla kandydatów, uczestniczących w przetargach i wnioskujących o dotacje, które powinny być podawane w zaproszeniach do składania wniosków i ofert.

2.3.3.11. Wspólne działania dotyczące powrotów - FRONTEX

Dnia 26 kwietnia 2010 r. EIOD wydał opinię (sprawa 2009-0281) na temat przetwarzania danych osobowych przez FRONTEX w zakresie „gromadzenia nazwisk oraz pewnych innych odpowiednich danych o osobach powracających w ramach wspólnych działań dotyczących powrotów". Celem przetwarzania jest przygotowanie i realizacja wspólnych działań dotyczących powrotów wspieranych przez FRONTEX w celu zapewnienia liniom lotniczym listy pasażerów i uzyskania wiedzy, między innymi, na temat liczby i tożsamości osób powracających, zagrożeń związanych z osobami powracającymi oraz w celu zapewnienia odpowiedniej pomocy medycznej podczas wspólnych działań dotyczących powrotów dla bezpieczeństwa tych działań oraz stanu zdrowia osób powracających.

FRONTEX poinformował EIOD, że dane osobowe nie były do tej pory przetwarzane dla działań operacyjnych, ale że będzie to niezbędne w bliskiej przyszłości dla 1) lepszego wykonania i dalszego rozwoju zadań Agencji w kontekście wspólnych działań dotyczących powrotów, 2) wsparcia organizujących państw członkowskich bądź państw stowarzyszonych w Schengen w opracowaniu list pasażerów i ich uaktalnianiu, 3) zapewnienia ciągłego nadzoru nad tym, które państwa członkowskie lub państwo stowarzyszone w Schengen dostarczyły (lub nie) wymaganych danych państwu organizującemu, 4) zwiększenia skuteczności i efektywności pomocy FRONTEX w organizacji wspólnych działań dotyczących powrotów.

EIOD poświęcił szczególną uwagę podstawie prawnej przetwarzania danych. EIOD uznał, że pewien zakres przetwarzania danych osobowych może być niezbędny dla prawidłowego wykonania zadań Agencji w kontekście wspólnych działań dotyczących powrotów i dla których Agencja powinna być postrzegana jako administrator danych osobowych. Jednakże, ze względu na szczególną ochronę danych i odnośne działania dotyczące słabszej populacji, zdaniem EIOD art. 9 rozporządzenia FRONTEX (współpraca przy powrotach) i art. 5 lit. a) rozporządzenia o ochronie danych mogą stanowić jedynie tymczasową podstawę prawną dla działań w zakresie przetwarzania danych, a podstawa ta powinna być przedmiotem starannego przeglądu pod kątem potrzeby ustanowienia bardziej szczegółowych podstaw prawnych.

Ponadto EIOD zażądał od FRONTEX wdrożenia koniecznych **procedur gwarantujących prawa osób, których dotyczą dane,** i wdrożenia **obowiązku informowania,** zanim działania w zakresie przetwarzania mają miejsce.

2.3.4. Konsultacje dotyczące potrzeby przeprowadzania kontroli wstępnych

Sama możliwość wystąpienia **danych szczególnie chronionych** nie jest automatycznie uzasadnieniem dla kontroli wstępnych. Przetwarzanie danych szczególnie chronionych odnoszących się, przykładowo, do zdrowia lub czynów bezprawnych oznacza, że należy ze szczególną uwagą podejść do przyjęcia odpowiednich środków bezpieczeństwa zgodnie z art. 22 rozporządzenia.

W razie wątpliwości instytucje i organy UE mogą konsultować się z EIOD na temat potrzeby kontroli wstępnych. W ciągu 2010 r., EIOD uzyskał sześć takich wniosków o konsultację od inspektorów ochrony danych.

Wśród kwestii analizowanych przez EIOD znajdowały się procedury wyboru pracowników wyższego szczebla; listy obecności członków stowarzyszeń biorących udział w wydarzeniach w instytucji; czynności przetwarzania danych Komitetu Pracowniczego i polityka szkoleń dla pracowników.

2.3.5. Powiadomienia niepodlegające kontroli wstępnej lub wycofane

W 2010 r. okazało się, w wyniku wnikliwej analizy, że osiem spraw nie podlega kontroli wstępnej. W takich sytuacjach (zwanych również „kontrolami niewstępnymi") EIOD może mimo to wydać zalecenia. Ponadto trzy wnioski zostały wycofane, a jeden został zastąpiony innym.

W sprawie dotyczącej szkoleń (sprawa 2010-0638) informacje uzupełniające otrzymane od Europejskiego Urzędu ds. Bezpieczeństwa Żywności (EFSA) w kontekście powiadomienia wyjaśniły, że gromadzone dane dotyczyły głównie statystyk, a ich celem było jedynie zapewnienie jakości polityki szkoleniowej EFSA. Mimo że dane dotyczące oceny prowadzącego szkolenia mogą być ujęte w sprawozdaniu, jego celem nie była ocena poszczególnych prowadzących szkolenia. Na podstawie tych informacji EIOD uznał, że powiadomienie to nie podlegało kontroli wstępnej.

2.3.6. Działania następcze po wydaniu opinii dotyczących kontroli wstępnych

*Opinia EIOD dotycząca kontroli wstępnej zazwyczaj będzie zawierać wniosek, że dana operacja przetwarzania danych nie narusza rozporządzenia pod warunkiem wdrożenia pewnych **zaleceń**. Zalecenia są również wydawane, kiedy dana sprawa zostaje przeanalizowana w celu podjęcia decyzji dotyczącej potrzeby przeprowadzenia kontroli wstępnej i wydaje się, że pewne zasadnicze aspekty wymagają podjęcia środków naprawczych. W przypadku gdy administrator danych nie stosuje się do tych zaleceń, EIOD może skorzystać z uprawnień przyznanych mu na mocy art. 47 rozporządzenia (WE) nr 45/2001.*

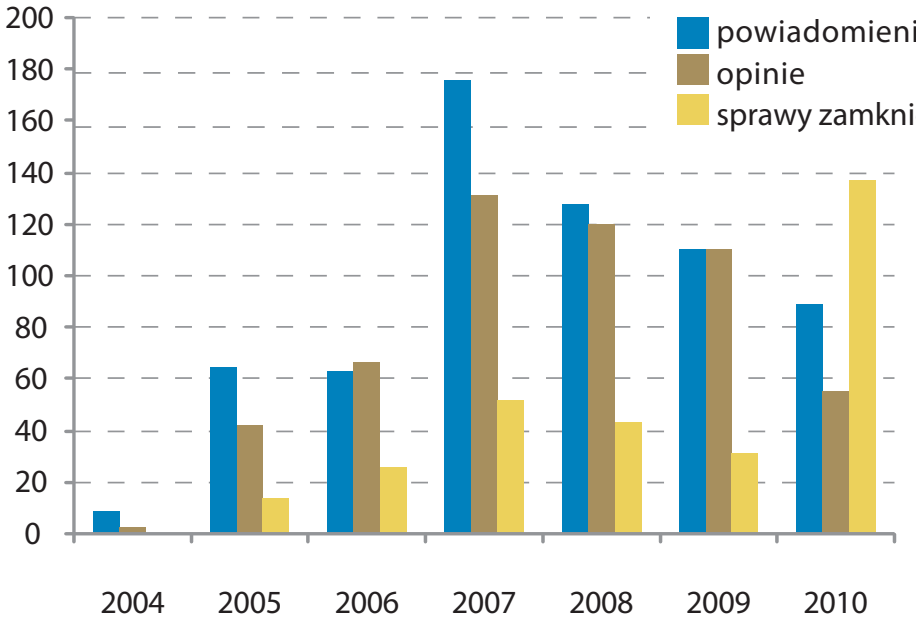
Instytucje oraz organy stosują się do tych zaleceń i do tej pory decyzje wykonawcze nie były potrzebne. W oficjalnym piśmie przesyłanym wraz z opinią EIOD zwraca się do danej instytucji lub organu o zawiadomienie go w terminie trzech miesięcy o środkach podjętych w celu realizacji zaleceń.

EIOD uważa działania następcze za **podstawowy czynnik w osiągnięciu pełnej zgodności** z rozporządzeniem. W nawiązaniu do ostatnio wydanego dokumentu strategicznego „Monitorowanie i zapewnianie zgodności z rozporządzeniem (WE) nr 45/2001" EIOD oczekuje od instytucji i organów wzięcia **odpowiedzialności** za wszelkie poczynione zalecenia. Oznacza to, że muszą być one odpowiedzialne za wdrożenie tych zaleceń i być w stanie wykazać to wdrożenie EIOD. Każda instytucja i organ niestosujące się do zaleceń naraża się na formalne postępowanie egzekwujące.

2.3.7. Wnioski

55 opinii wydanych przez EIOD jest wartościowym wkładem w operacje przetwarzania danych przez administrację europejską oraz umożliwia EIOD rozwijanie swoich kompetencji i wydawanie ogólnych wytycznych w wybranych obszarach, takich jak wspólne procedury administracyjne. Jest tak w przypadku przetwarzania danych związanego z dochodzeniami administracyjnymi i postępowaniami dyscyplinarnymi (zob. pkt 2.7 na temat wytycznych tematycznych). EIOD będzie w dalszym ciągu kierował takie wytyczne do instytucji

Porównanie sytuacji



i agencji, będzie również kontynuował usprawnianie procesu składania powiadomień przez agencje.

Jako że większość instytucji zakończyła składanie powiadomień o istniejących operacjach przetwarzania danych w standardowych procedurach administracyjnych, EIOD otrzymał w ciągu 2010 r. wiele powiadomień dotyczących podstawowych procesów operacyjnych, charakterystycznych dla pewnych instytucji czy agencji.

EIOD osiągnął ważny punkt w działaniach następczych w zakresie opinii dotyczących kontroli wstępnych, jako że 137 spraw zostało zamkniętych w 2010 r. EIOD będzie kontynuował ścisłe monitorowanie działań następczych w celu dopilnowania, by instytucje i agencje wdrażały zalecenia poczynione przez EIOD w terminowy i zadowalający sposób.

2.4. Skargi

2.4.1. Mandat EIOD

Zgodnie z rozporządzeniem (WE) nr 45/2001 EIOD, w ramach swoich podstawowych obowiązków, „wysłuchuje i bada skargi" oraz „przeprowadza dochodzenia zarówno z własnej inicjatywy, jak i na podstawie skarg" (art. 46).

Zasadą jest, że dopuszczalne są jedynie skargi osób fizycznych dotyczące domniemanego naruszenia ich praw w związku z ochroną ich danych osobowych. W związku z domniemanymi naruszeniami zasad ochrony danych skargi może składać jedynie personel UE niezależnie od tego, czy przetwarzanie danych dotyczy bezpośrednio skarżącego, czy też nie. Regulamin pracowniczy urzędników Unii Europejskiej również dopuszcza składanie skarg do EIOD (art. 90b).

Zgodnie z rozporządzeniem EIOD może rozpatrywać wyłącznie skargi przedłożone przez **osoby fizyczne**. Skargi przedkładane przez przedsiębiorstwa lub inne osoby prawne nie są dopuszczalne.

Skarżący muszą także podać swoje dane, anonimowe wnioski nie są traktowane jako skargi. Informacje anonimowe mogą jednak być brane pod uwagę w ramach innej procedury (np. dochodzenie prowadzone z własnej inicjatywy lub wniosek o powiadomienie o operacji przetwarzania danych itp.).

Skarga do EIOD może dotyczyć jedynie przetwarzania danych osobowych. *EIOD nie ma kompetencji, by badać sprawy dotyczące ogólnego niewłaściwego administrowania, modyfikować treść dokumentów, które skarżący pragnie zmienić, lub przyznawać odszkodowanie finansowe za poniesione szkody.*

Każdy może złożyć skargę do EIOD w zakresie przetwarzania danych osobowych przez administrację UE.

Pracownik Komisji Europejskiej zakwestionował treść jego sprawozdania oceniającego przygotowanego przez zwierzchników. Zwrócił się do EIOD o polecenie Komisji poprawienia sprawozdania, ponieważ zawierało one jego dane osobowe. EIOD nie zgadzał się z rozumowaniem skarżącego. Nawet jeśli dane z oceny to dane osobowe, są one z definicji subiektywną oceną, której nie można automatycznie poprawić w oparciu o zasady ochrony danych. Należałoby zastosować specjalną procedurę do kwestionowania treści sprawozdań oceniających, aby zakwestionować włączenie danych.

*Przetwarzanie danych osobowych, które stanowi temat skargi, musi być czynnością wykonywaną przez **instytucję lub organ UE**. Ponadto EIOD nie jest instancją odwoławczą w stosunku do krajowych organów ochrony danych.*

2.4.2. Procedura rozpatrywania skarg

EIOD rozpatruje skargi zgodnie z istniejącymi ramami prawnymi, ogólnymi zasadami prawa UE oraz dobrymi praktykami administracyjnymi wspólnymi dla instytucji i organów UE. W grudniu 2009 r. EIOD przyjął **podręcznik wewnętrzny**, który zawiera wytyczne dla personelu rozpatrującego skargi. EIOD wdrożył też **narzędzie statystyczne** służące monitorowaniu działań związanych ze skargami, w szczególności monitorowaniu postępów w konkretnych sprawach.

Na wszystkich etapach rozpatrywania skarg EIOD kieruje się zasadami proporcjonalności i racjonalności. Z uwzględnieniem zasady przejrzystości i niedyskryminacji podejmuje właściwe działania, biorąc pod uwagę:

- charakter i wagę zarzucanego naruszenia zasad ochrony danych;
- wagę szkody doznanej rzeczywiście lub potencjalnie przez jedną lub większą liczbę osób, których dane dotyczą, w wyniku naruszenia;
- potencjalne ogólne znaczenie sprawy w odniesieniu do innych odpowiednich interesów publicznych lub prywatnych;

- prawdopodobieństwo stwierdzenia, że doszło do naruszenia;

- dokładną datę wydarzeń, wszelkie postępowanie, które nie ma już konsekwencji, usunięcie tych konsekwencji lub stosowne gwarancje ich usunięcia.

Każda skarga wpływająca do EIOD jest wnikliwie badana. Wstępne badanie skargi ma w szczególności na celu weryfikację, czy skarga spełnia warunki do wszczęcia dalszego dochodzenia, w tym czy istnieją wystarczające podstawy do wszczęcia dochodzenia.

Skarga, do rozpatrzenia której EIOD **nie jest właściwy**, zostaje uznana za niedopuszczalną, o czym poinformowany zostaje skarżący. W takich przypadkach EIOD, jeśli jest taka potrzeba, może zalecić skarżącemu zwrócenie się ze sprawą do innego właściwego organu (Trybunał Sprawiedliwości, Rzecznik Praw Obywatelskich, krajowe organy ochrony danych itp.).

Skargi dotyczące faktów, które są **w oczywisty sposób nieznaczące** lub wymagające **niewspółmiernych nakładów** przy ich badaniu, nie są badane. EIOD może badać jedynie skargi dotyczące **rzeczywistego lub potencjalnego**, nie zaś czysto hipotetycznego naruszenia stosownych zasad odnoszących się do przetwarzania danych osobowych. Obejmuje to analizę dostępnych możliwości zaradzenia danemu problemowi przez skarżącego lub przez EIOD. EIOD może na przykład wszcząć dochodzenie z własnej inicjatywy w związku z ogólnym problemem, a także wszczynać dochodzenie w konkretnej sprawie przedłożonej przez skarżącego. W takich przypadkach skarżący jest informowany o wszystkich dostępnych środkach działania.

Osoba zwróciła się do EIOD z zapytaniem, czy mogłaby uzyskać dostęp do danych osobowych innych kandydatów w procedurze rekrutacyjnej, czy też można jej tego odmówić na podstawie ochrony danych. EIOD nie zajął stanowiska, ponieważ pytanie było na daną chwilę hipotetyczne, biorąc pod uwagę, że odnośny organ UE nie odmówił jeszcze dostępu do żądanych informacji, a tym samym nie wykorzystał ochrony danych jako podstawy odmowy.

Skarga jest z zasady **niedopuszczalna**, jeżeli skarżący **nie skontaktował się w pierwszej kolejności z daną instytucją** w celu rozwiązania problemu. Jeżeli skarżący nie skontaktował się z instytucją, powinien przedstawić EIOD wystarczające powody, dla których tego nie uczynił.

Jeżeli sprawę badają już organy administracji – tj. trwa wewnętrzne dochodzenie w danej instytucji – skarga jest z zasady dopuszczalna. EIOD może jednak na podstawie okoliczności konkretnej sprawy zadecydować o odłożeniu dochodzenia do chwili poznania wyniku tych procedur administracyjnych. Jeżeli jednak ta sama sprawa (w tych samych okolicznościach faktycznych) jest już badana przez sąd, skarga jest uznawana za niedopuszczalną.

W celu zapewnienia jednolitego podejścia do skarg dotyczących ochrony danych oraz uniknięcia niepotrzebnego powielania zadań **Europejski Rzecznik Praw Obywatelskich** i EIOD podpisali w listopadzie 2006 r. protokół ustaleń. Stwierdza się w nim między innymi, że skarga, która została już wniesiona, nie powinna być ponownie rozpatrywana przez drugą instytucję, chyba że przedstawiono istotne nowe dowody.

Co się tyczy **ograniczeń czasowych**, jeżeli fakty kierowane do EIOD zostają przedstawione po okresie dwóch lat, skarga jest z zasady niedopuszczalna. Dwuletni okres biegnie od dnia, w którym skarżący dowiedział się o tych faktach.

Jeżeli skarga jest dopuszczalna, EIOD przeprowadza **dochodzenie.** Dochodzenie to obejmuje wezwanie do danej instytucji do udzielenia informacji, przegląd stosownych dokumentów, spotkanie z administratorem danych, kontrolę na miejscu itp. EIOD ma uprawnienia, by zażądać od danej instytucji lub organu dostępu do wszystkich danych osobowych i wszystkich informacji niezbędnych do przeprowadzenia dochodzenia. Może również uzyskać dostęp do wszelkich pomieszczeń, w których administrator danych, instytucja lub organ prowadzi działalność.

Na zakończenie dochodzenia skarżącemu oraz administratorowi odpowiedzialnemu za przetwarzanie danych przesyłana jest **decyzja**. W decyzji EIOD określa swoje stanowisko dotyczące ewentualnego naruszenia zasad ochrony danych przez daną instytucję. **Uprawnienia EIOD** są szerokie: od udzielania porad osobom, których dane dotyczą, przez ostrzeżenia lub upomnienia dla

administratora danych, po nałożenie zakazu przetwarzania danych lub skierowanie sprawy do Trybunału Sprawiedliwości.

Każda zainteresowana strona może zwrócić się do EIOD o **zmianę** decyzji w terminie miesiąca od jej wydania. Zainteresowane strony mogą również odwołać się bezpośrednio do Trybunału Sprawiedliwości.

W 2009 r. skarżący odwołali się w dwóch przypadkach od decyzji EIOD do Sądu (sprawy T-164/09 i T-193/09). Jeśli chodzi o pierwszą sprawę, Sąd postanowił, że nie ma już potrzeby orzekania w sprawie działania EIOD, ponieważ postępowanie to stało się bezprzedmiotowe. W przypadku drugiej sprawy wniosek o przyznanie pomocy w zakresie kosztów postępowania przedłożony przez stronę skarżącą został oddalony przez Sąd. Przedmiot sprawy nie został omówiony przez Sąd.

2.4.3. Gwarancja poufności dla skarżących

*EIOD zdaje sobie sprawę z faktu, że niektórzy skarżący narażają swoją karierę zawodową, ujawniając naruszenie zasad ochrony danych, w związku z czym skarżącym i wnioskującym o to informatorom powinna być zagwarantowana **poufność**. Jednocześnie zasadą EIOD jest **przejrzystość** jego pracy oraz publikowanie co najmniej merytorycznej treści decyzji. Procedury wewnętrzne EIOD odzwierciedlają konieczność zachowania równowagi w tej delikatnej kwestii.*

Zasadą jest, że skargi są traktowane jako poufne. **Poufne traktowanie** implikuje nieujawnianie danych osobowych osobom spoza EIOD. Do prawidłowego przeprowadzenia dochodzenia niezbędne może być jednak poinformowanie właściwych służb danej instytucji oraz osób trzecich związanych ze sprawą o treści skargi i tożsamości skarżącego. EIOD przekazuje również kopię całej korespondencji między EIOD a daną instytucją inspektorowi ochrony danych tej instytucji.

Jeżeli skarżący wnioskuje o **anonimowość** przed instytucją, inspektorem ochrony danych lub osobami trzecimi związanymi ze sprawą, jest wzywany do wyjaśnienia powodów takiego wniosku. Następnie EIOD analizuje argumenty skarżącego i bada konsekwencje wniosku dla wykonalności dalszego dochodzenia EIOD. Jeżeli EIOD zadecyduje o niezagwarantowaniu anonimowości skarżącemu, wyjaśnia powód takiej decyzji i pyta skarżącego, czy zgadza się na zbadanie skargi przez EIOD bez zagwarantowania mu anonimowości, czy też woli wycofać skargę. Jeżeli skarżący zadecyduje o wycofaniu skargi, dana instytucja nie zostanie poinformowana o jej wniesieniu. W takim przypadku EIOD może podjąć w tej sprawie inne działania bez ujawniania danej instytucji faktu wniesienia skargi, tj. wszcząć dochodzenie z własnej inicjatywy lub skierować wniosek o powiadomienie o operacji przetwarzania danych.

Po zakończeniu dochodzenia wszystkie **dokumenty związane ze skargą**, w tym ostateczna decyzja, pozostają co do zasady poufne. Nie są one publikowane w całości ani przekazywane osobom trzecim. EIOD może jednak opublikować anonimowe podsumowanie skargi na swojej stronie internetowej oraz w sprawozdaniu rocznym EIOD w formie, która nie pozwala na zidentyfikowanie skarżącego ani osób trzecich. W ważnych sprawach EIOD może również podjąć decyzję o publikacji ostatecznej decyzji *in extenso*. Należy to uczynić w formie, która uwzględnia wniosek skarżącego o zachowanie poufności, a zatem nie pozwala na zidentyfikowanie skarżącego ani innych zainteresowanych osób.

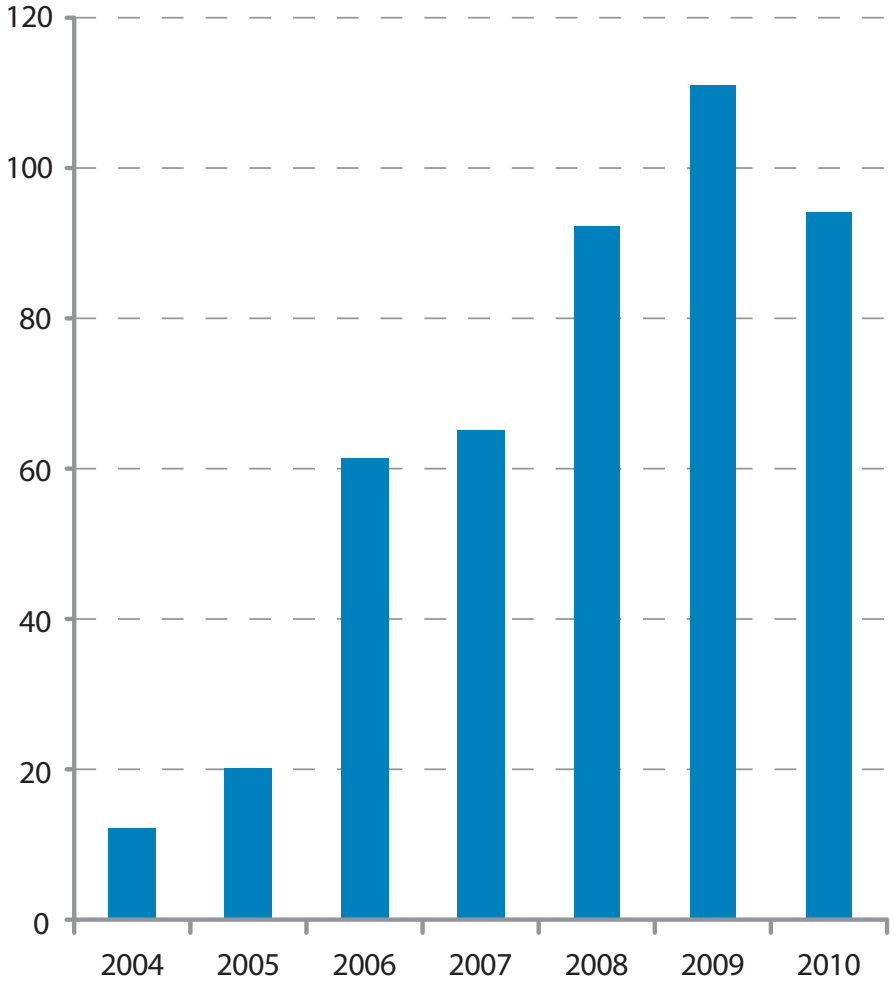
2.4.4. Skargi rozpatrzone w 2010 r.

2.4.4.1. Liczba skarg

*Złożoność skarg otrzymanych przez EIOD wzrosła w 2010 r., natomiast liczba skarg spadła. **W 2010 r. EIOD otrzymał 94 skargi** (o 15% mniej niż w 2009 r.). **69 spośród tych skarg było niedopuszczalnych**, gdyż w większości odnosiły się one do przetwarzania na szczeblu krajowym, nie zaś przez instytucję lub organ UE.*

Pozostałe 25 skarg wymagało wnikliwszego zbadania (o 41% mniej niż w 2009 r.). Ponadto 18 dopuszczalnych skarg przedłożonych w latach poprzednich (16 w 2009 r. i 2 w 2008 r.) pozostawało na etapie dochodzenia lub przeglądu w 2010 r.

Liczba otrzymanych skarg (zmiany w latach 2004–2010)



2.4.4.2. Skarżący

Spośród 94 otrzymanych skarg 17 (18%) pochodziło od pracowników instytucji lub organów UE, w tym byłych pracowników i kandydatów do pracy. W przypadku pozostałych 77 skarg skarżący, jak się wydaje, nie pozostawali w stosunku pracy z administracją UE.

2.4.4.3. Instytucje, których dotyczyły skargi

Spośród dopuszczalnych skarg przedłożonych w 2010 r. większość (ponad 80%) dotyczyła Komisji Europejskiej, w tym OLAFu i EPSO. Nie jest to zaskakujące, ponieważ Komisja przetwarza dane osobowe na większą skalę niż inne instytucje i organy UE. Znaczną liczbę skarg dotyczących OLAFu i EPSO można wyjaśnić charakterem działań podejmowanych przez te organy.

2.4.4.4. Język skarg

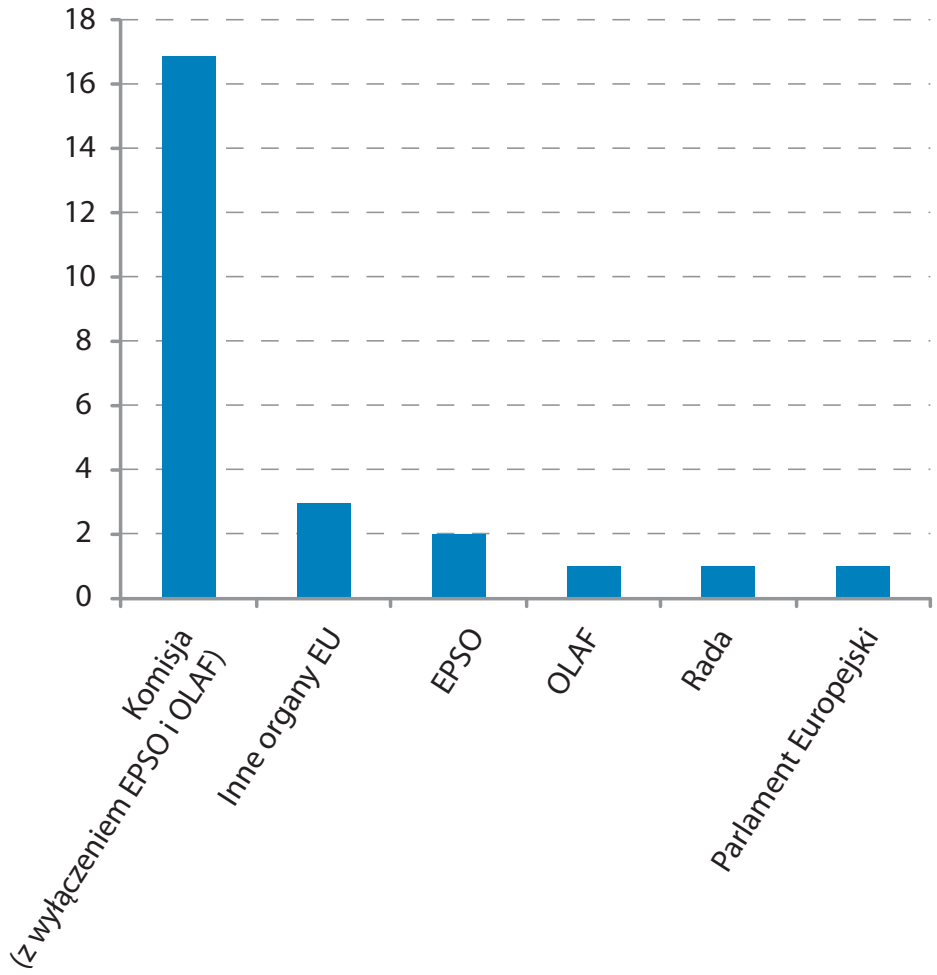
Większość skarg przedłożono w języku angielskim (44%) lub niemieckim (33%), rzadziej wykorzystywany był francuski (15%). Skargi w innych językach są względnie rzadkie (8%).

2.4.4.5. Rodzaje zarzucanych naruszeń

Najważniejszymi rodzajami naruszeń zasad ochrony danych zarzucanymi przez skarżących w 2010 r. były:

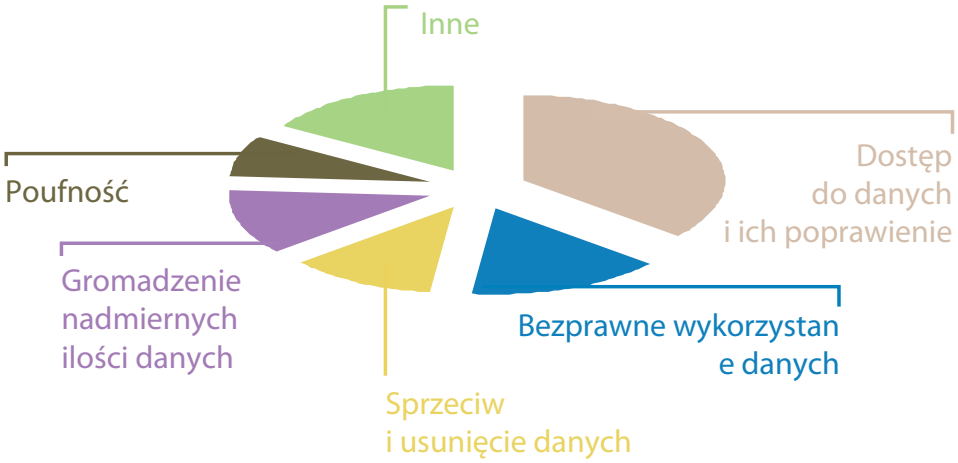
- złamanie praw osób, których dane dotyczą, takich jak prawo dostępu i prawo do poprawiania danych (36%) lub sprzeciwu i usuwania danych (12%);
- nieuprawnione wykorzystanie danych (16%), nadmierne gromadzenie danych osobowych (12%), naruszenie poufności (8%).

Skargi według instytucji i organów UE



Inne, mniej powszechne domniemane naruszenia dotyczyły bezpieczeństwa danych (4%), kradzieży tożsamości (4%), jakości danych i informacji dla osób, których dane dotyczą (4%).

Rozdzaje zarzucanych naruszeń

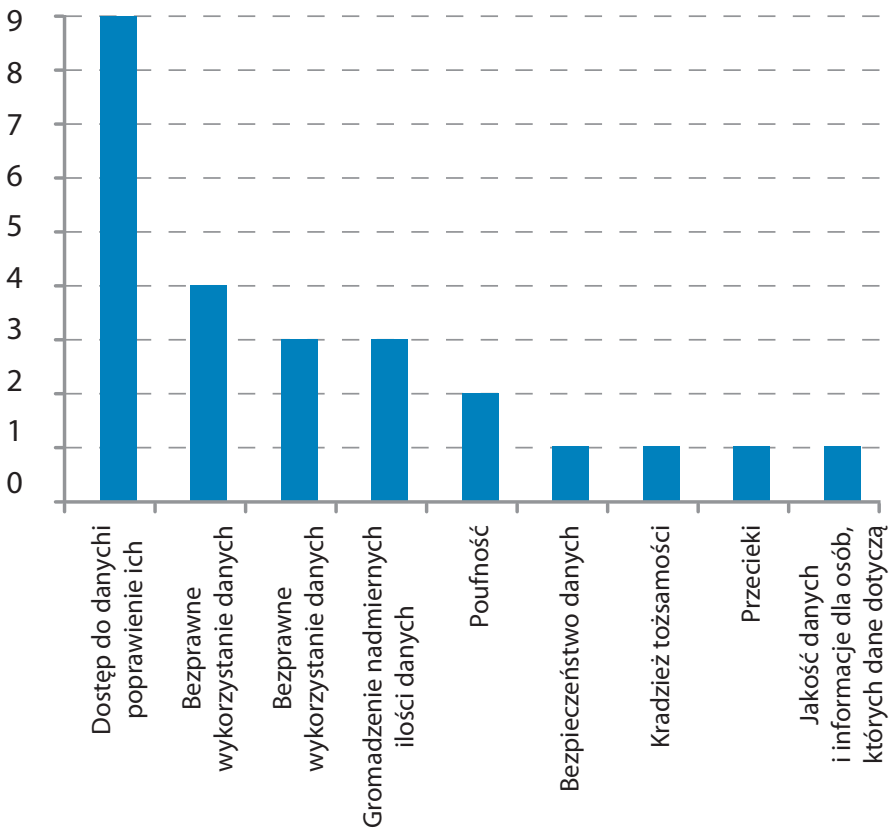


2.4.4.6. Wyniki dochodzeń EIOD

W 11 sprawach rozstrzygniętych w 2010 r. EIOD nie stwierdził naruszenia zasad ochrony danych.

Z kolei w 10 przypadkach doszło do naruszenia zasad ochrony danych i skierowano zalecenia do administratora danych.

Wyniki dochodzeń EIOD



EIOD otrzymał skargę odnoszącą się do dostępu do własnej dokumentacji medycznej, prowadzonej przez instytucję służby medycznej. EIOD potwierdził, że zgodnie z zasadami ochrony danych, dostęp do danych osobowych nie zobowiązuje administratora danych do przesłania oryginalnej dokumentacji medycznej, ale że wynika z nich w praktyce prawo do zapoznania się z nimi (osobiście lub w niektórych przypadkach za pośrednictwem doktora) lub prawo do uzyskania kopii dokumentacji. W odniesieniu do prawa do poprawienia niedokładnych lub niekompletnych danych EIOD podkreślił, że obowiązek poprawienia danych w kontekście dokumentacji medycznej odnosi się wyłącznie do danych faktycznych, ale nie do ocen związanych ze stanem zdrowia. Administrator danych nie jest tym samym zobowiązany na podstawie zasad ochrony danych do zmiany wniosków w danym orzeczeniu lekarskim. W tym kontekście prawo do poprawienia danych może skutkować możliwością zawarcia innego orzeczenia od innego lekarza, zawierającego inną ocenę. EIOD uznał tym samym, że w tym przypadku nie doszło do naruszenia zasad ochrony danych.

Otrzymano skargę dotyczącą publikacji danych osobowych wyjątkowo szczególnie chronionych w Dzienniku Urzędowym Unii Europejskiej i w protokole sesji Parlamentu Europejskiego. Po dochodzeniu w tej sprawie EIOD ustalił, że opinia posła do Parlamentu mogła zostać wyrażona, a przesłanie polityczne oświadczenia pisemnego mogło zostać skutecznie przekazane bez ujawniania tożsamości zaangażowanych osób. EIOD zażądał usunięcia nazwisk osób określonych przez posła w oświadczeniu pisemnym i w jakichkolwiek innych środkach. Zażądał on również wprowadzenia formalnej, skutecznej procedury w celu dopilnowania, by ostateczne wersje dokumentów publikowanych w Dzienniku Urzędowym i na stronach internetowych Parlamentu uwzględniały zmiany wdrożone przez służby odpowiedzialne za przygotowanie dokumentów.

Otrzymano skargę dotyczącą przekazania numerów pracowniczych członków personelu pewnej agencji wszystkim użytkownikom za pośrednictwem wewnętrznego adresu e-mail tej agencji. Celem tej operacji przetwarzania danych było zaproszenie wszystkich członków personelu na spotkanie z sekcją bezpieczeństwa agencji w celu zrobienia im zdjęć. EIOD uznał, że w tym celu wystarczyłoby wysłać listę zawierającą tylko nazwisko i imię wszystkich odnośnych osób. Numer pracowniczy na tej liście był niestosowny i zbędny w odniesieniu do wskazanego celu, co naruszało art. 4 rozporządzenia. EIOD zachęcił agencję do formalnego poinstruowania personelu pracującego z danymi osobowymi o ostrożności w wyborze danych i zapewnianiu szczególnej staranności przy wewnętrznym lub zewnętrznym przesyłaniu masowych informacji mailowych zawierających dane osobowe, aby e-maile zawierały tylko niezbędne dane z punktu widzenia celu wiadomości.

Członek personelu wniósł skargę przeciwko niejawnemu nadzorowi wideo w instytucji. W szczególności zakwestionował on zgodność z prawem użycia kamer wideo, które nagrywały go bez jego wiedzy, gdy wchodził on do biura przełożonego podczas jego nieobecności. EIOD stwierdził, że instytucja nie przedstawiła podstawy prawnej, która dopuszczałaby w wyraźny sposób możliwość takich mocno inwazyjnych działań oraz przewidywała szczególne warunki i zabezpieczenia. Bez przejrzystych ram prawnych i uporządkowanego podejścia proporcjonalność niejawnego nadzoru wideo budziła wątpliwości. EIOD wezwał tym samym instytucję do ponownego zbadania, czy jej intencją jest utrzymanie niejawnego nadzoru w przyszłości, a jeśli tak, do złożenia planów do EIOD do kontroli wstępnej.

2.4.5. Dalsze prace w dziedzinie skarg

Celem EIOD jest usprawnienie procesu składania skarg i przyspieszenie przetwarzania skarg przez służby EIOD poprzez wprowadzenie **formularza on-line do składania skarg** na stronie EIOD (zob. pkt 5.6.1). Tymczasowa wersja takiego formularza jest dostępna na stronie EIOD od początku 2010 r. Wersja ostateczna będzie bardziej interaktywna. EIOD oczekuje, że upowszechnienie użycia aplikacji pomoże skarżącym ocenić dopuszczalność ich skarg i tym samym wnioskować tylko w sprawach właściwych dla EIOD. Ponadto EIOD ma nadzieję uzyskać bardziej kompletne i właściwe informacje do bardziej wydajnego rozpatrywania skarg i ograniczenia liczby wyraźnie niedopuszczalnych skarg.

EIOD zamierza również przejrzeć podręcznik wewnętrznych procedur rozpatrywania skarg, przyjęty w 2009 r. Zmienione procedury wpisałyby się w nową strukturę organizacyjną EIOD i objaśniłyby wewnętrzny przepływ prac w zakresie skarg.

2.5. Monitorowanie przestrzegania przepisów

*EIOD jest odpowiedzialny za monitorowanie i **zapewnienie stosowania rozporządzenia (WE) nr 45/2001**. Monitorowanie prowadzono w szczególności w ramach **operacji sprawozdawczej**, zwanej „Wiosna 2009". Oprócz tego ogólnego monitorowania prowadzono działania w zakresie ukierunkowanego monitorowania w przypadkach, gdy w wyniku działań nadzorczych EIOD był zaniepokojony poziomem zgodności z przepisami w konkretnych instytucjach lub organach. Część z nich jest oparta na korespondencji, podczas gdy inne przybierają formę jednodniowej **wizyty** w odpowiednim organie w celu omówienia niezgodności z przepisami. Wreszcie przeprowadzono **kontrole** w niektórych instytucjach i organach w celu sprawdzenia przestrzegania przepisów w konkretnych dziedzinach.*

2.5.1. Ukierunkowane monitorowanie i sprawozdawczość

EIOD inicjował oparte na korespondencji ukierunkowane działania monitorujące w przypadkach, gdy miał obawy co do kwestii związanej z przestrzeganiem przepisów rozporządzenia w danej

instytucji lub agencji. Tak było przykładowo w przypadku EBC w zakresie wewnętrznych dochodzeń administracyjnych lub w przypadku operacji przetwarzania danych przez DG RELEX.

Wewnętrzne dochodzenia administracyjne – Europejski Bank Centralny

W styczniu 2010 r. EIOD wszczął dochodzenie w zakresie ochrony danych osobowych w trakcie wewnętrznych dochodzeń administracyjnych w Europejskim Banku Centralnym (EBC). Decyzja ta została podjęta na podstawie art. 46 lit. b) rozporządzenia, jako działanie następcze wobec opinii EIOD z dnia 22 grudnia 2005 r. w sprawie takich dochodzeń w EBC. Dochodzenie skoncentrowane było na ewentualnym dostępie do dokumentacji elektronicznej i przechwytywaniu rozmów telefonicznych. Przesłano do EBC liczne pytania dotyczące zastosowania okólnika administracyjnego EBC 01/2006 dotyczącego wewnętrznych dochodzeń administracyjnych i ich zasad. Obejmowały one między innymi pytania o sposób dokumentowania procedury, istnienie lub brak komputerowego protokołu oficjalnych dochodzeń, a także o roczną statystykę przechwyceń rozmów telefonicznych oraz dostęp do dokumentacji elektronicznej i danych o ruchu. Dochodzenie nie zostało jeszcze zamknięte.

Wykaz DG RELEX

W związku z licznymi skargami EIOD miał obawy, że wykaz operacji przetwarzania danych pod kontrolą DG RELEX niedokładnie odzwierciedlał operacje przetwarzania danych zawierające dane osobowe delegacji UE. EIOD chciał też potwierdzić, że DG RELEX powiadomiła inspektora ochrony danych Komisji o wszystkich operacjach przetwarzania danych delegacji UE zgodnie z art. 25. DG RELEX udostępniła następnie uaktualnienia i wydała odpowiednie zapewnienia w obu kwestiach, a sprawa została zamknięta.

Wizyta w Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji

Dnia 17 września 2010 r. EIOD odwiedził Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) w celu zweryfikowania i omówienia niskiego poziomu zgodności z rozporządzeniem (WE) 45/2001. Do wizyty tej skłoniły go dowody zebrane w toku działań nadzorczych EIOD, w formie skargi, konsultacji oraz braku działań następczych w odniesieniu do opinii dotyczącej kontroli wstępnej.

Wizyta pozwoliła inspektorowi ochrony danych poinformować EIOD o postępach ENISA w zakresie e-rejestru, działań następczych i nowego wykazu. IOD podkreślił problemy z niezależnością w wykonywaniu obowiązków inspektora danych, a zastępca Inspektora wskazał na dokument o standardach zawodowych inspektorów danych osobowych (przyjęty w październiku 2010 r.), który powinien pomóc inspektorowi wzmocnić i wyjaśnić jego rolę wewnętrznie.

Podczas spotkania zamykającego, na podstawie wymogów EIOD, przez obie strony został przyjęty plan nadzoru (zawierający szczegółowe terminy), kładący nacisk na istotność trzech głównych narzędzi dla przestrzegania przepisów rozporządzenia: wykaz, rejestr i powiadomienia do EIOD zgodnie z art. 27. EIOD będzie ściśle kontrolował dalsze postępy poczynione przez ENISA zgodnie z planem w celu zapewnienia osiągnięcia zgodności z przepisami rozporządzenia.

Wizyta w Europejskiej Agencji Środowiska

Dnia 10 grudnia 2010 r. EIOD odwiedził Europejską Agencję Środowiska (EEA) w celu zweryfikowania i omówienia poziomu zgodności z przepisami rozporządzenia w Agencji.

Wizyta obejmowała spotkanie pomiędzy EIOD i dyrektorem EEA oraz dalsze spotkania z udziałem inspektora ochrony danych i administratorów operacji przetwarzania danych. Stanowiło to okazję dla EIOD przedstawienia obaw dotyczących obecnego poziomu zgodności z przepisami rozporządzenia w EEA i pozwoliło Agencji na przekazanie nowych informacji o postępie w celu osiągnięcia pełnej zgodności. W tym kontekście EIOD z zadowoleniem zauważył znaczące wysiłki Agencji w ostatnim okresie i jej zaangażowanie w usuwanie uchybień.

Przez obie strony został przyjęty plan nadzoru (zawierający szczegółowe terminy), który będzie ściśle kontrolowany przez EIOD.

2.5.2. Ogólne monitorowanie i sprawozdawczość: operacja „Wiosna 2009”

W nawiązaniu do ogólnej inspekcji dotyczącej monitorowania, rozpoczętej na wiosnę 2009 r., EIOD kontynuował monitorowanie wdrożenia zasad i reguł ochrony danych przez odpowiednie instytucje i organy.

Instytucje UE nadal czynią **znaczące postępy** w spełnianiu wymogów ochrony danych i mimo że niektóre inne organy również poczyniły postępy, zidentyfikowano ogólnie **niższy poziom zgodności z przepisami** w **agencjach**.

Jeśli zdaniem EIOD postęp w kierunku zgodności z przepisami był niezadowalający, wyznaczono odpowiednie cele. Niestety, w niektórych przypadkach cele nie zostały osiągnięte i w rezultacie EIOD zażądał dalszego informowania. Gdy takie informacje nie były przesyłane lub gdy postęp był zbyt mały, EIOD uruchamiał bardziej ukierunkowane działania monitorujące (zob. powyżej).

Uaktualnienia w odniesieniu do operacji „Wiosna 2009"

- **Powiadomienia o operacjach przetwarzania danych od administratorów danych do inspektora danych osobowych:** ogólny poziom powiadomień wzrósł i podczas gdy EIOD będzie nadal oczekiwał informacji o postępach, będzie on również pracował ze słabiej funkcjonującymi instytucjami i organami zgodnie z ostatnio opublikowanym dokumentem strategicznym w sprawie monitorowania i zapewniania zgodności z przepisami.
- **Powiadomienia EIOD o operacjach przetwarzania danych do celów kontroli wstępnej:** większość instytucji poczyniła znaczące postępy w tym zakresie, ponownie jednak poziom zgodności z przepisami pozostaje niższy w agencjach i EIOD będzie z tego względu pracował nad rozwiązaniem tego problemu w najbliższych latach.

2.5.3. Następne kroki

EIOD będzie wspierać i uważnie monitorować dalsze postępy, w szczególności w tych instytucjach i agencjach, w których poziom przestrzegania przepisów dotyczących kontroli wstępnych EIOD oraz powiadamiania IOD należy poprawić. Będzie on również w dalszym ciągu kładł nacisk na **wykazy** i na **wewnętrzne procedury działań następczych wobec jego zaleceń**, w zapewnianiu przestrzegania rozporządzenia.

Następna operacja dotycząca ogólnego monitorowania (**Wiosna 2011**) rozpocznie się na początku 2011 r., w oparciu o dowody zgromadzone już w trakcie poprzednich takich działań prawdopodobnie podejmowane będą jednak w dalszym ciągu dodatkowe ukierunkowane inicjatywy w zakresie zgodności z przepisami.

2.5.4. Kontrole

Kontrole są podstawowym narzędziem umożliwiającym EIOD monitorowanie i zapewnienie stosowania rozporządzenia; są one przeprowadzane na podstawie art. 41 ust. 2, art. 46 lit. c) i art. 47 ust. 2.

W celu zapewnienia mu wystarczających narzędzi do wykonywania funkcji, EIOD przyznano szerokie uprawnienia do dostępu do wszelkich informacji i danych osobowych niezbędnych do prowadzonych przez niego dochodzeń oraz do uzyskania dostępu do pomieszczeń, w których administrator danych lub instytucja, lub organ UE prowadzi działalność. Kontrole mogą być uruchamiane na podstawie skargi lub z własnej inicjatywy EIOD.

Art. 30 rozporządzenia nakłada na instytucje i organy UE obowiązek współpracy z EIOD w wykonywaniu jego obowiązków oraz dostarczenia mu wymaganych informacji i udzielenia dostępu.

Podczas kontroli EIOD **weryfikuje fakty na miejscu** w celu zapewnienia przestrzegania przepisów. Kontrolowanej instytucji lub organowi przekazywane są po kontroli odpowiednie informacje zwrotne.

W 2010 r. EIOD kontynuował działania następcze w odniesieniu do wcześniejszych kontroli. Dodatkowo, w grudniu 2010 r. EIOD przeprowadził kontrolę we Wspólnym Centrum Badawczym (JRC) Komisji w Isprze.

Działania następcze wobec kontroli w Europejskim Urzędzie Doboru Kadr

W marcu 2009 r. EIOD przeprowadził kontrolę w Europejskim Urzędzie Doboru Kadr (EPSO). Celem kontroli było zbadanie okoliczności

Kontrole to podstawowe narzędzie monitorowania i zapewnienia wdrożenia rozporządzenia o ochronie danych.

operacji przetwarzania danych osobowych w związku z kilkoma kontrolami wstępnymi w zakresie doboru urzędników, personelu zatrudnionego na czasu określony i personelu kontraktowego, jak również wszelkich związanych z tym operacji przetwarzania danych osobowych. EIOD wydał szereg wniosków, głównie w zakresie przejrzystości procedur EPSO i zatrzymywania danych, które następnie zostały wzięte pod uwagę przez EPSO.

Celem kontroli była również weryfikacja zgodności z przepisami **wybranych baz danych EPSO i narzędzi informatycznych** wykorzystywanych podczas procedur selekcyjnych. EIOD wciąż oczekuje na dalsze informacje zwrotne na temat postępów w planie wdrożenia jego zaleceń. Z tego względu EIOD opatrzył zastrzeżeniami ostateczne wnioski z kontroli w oczekiwaniu na te informacje.

Działania następcze w odniesieniu do kontroli Europejskiego Trybunału Obrachunkowego

Po kontroli EIOD przeprowadzonej w Europejskim Trybunale Obrachunkowym (ETO) w marcu 2009 r., w odniesieniu do **personelu monitorującego** (sprawozdanie dotyczące narzędzia służącego do monitorowania Internetu i audytu), bieżąca współpraca z Trybunałem była owocna i EIOD odnotował postępy w przestrzeganiu przepisów w zbadanych obszarach.

W **sprawie dotyczącej monitorowania Internetu** (sprawa 2008-0284) EIOD wydał szczególne zalecenia w swoim sprawozdaniu, dotyczące działań następczych w związku z przyjętą opinią. Wciąż mają miejsce dalsze dyskusje w celu zapewnienia pełnej zgodności z ogólnymi ramami analizy tego zagadnienia w kontekście instytucjonalnym.

W odniesieniu do konsultacji w zakresie procedury dostępu do prywatnych dysków/e-maili członków personelu, EIOD stwierdził, że konieczne jest złożenie do niego formalnego powiadomienia o kontroli wstępnej w odniesieniu do tych operacji przetwarzania danych, ponieważ stwarza ona konkretne zagrożenie zgodnie z art. 27 ust. 1 rozporządzenia. W styczniu 2010 r. EIOD wydał opinię (sprawa 2009-0620), zezwalając na operacje przetwarzania danych przy pewnych zaleceniach, które następnie zostały wdrożone przez ETO. Tym samym EIOD zamknął sprawę.

Działania następcze po kontroli s-TESTA

Sieć s-TESTA (bezpieczne transeuropejskie usługi telematyczne między administracjami) zapewnia ogólną infrastrukturę służącą zaspokojeniu potrzeb biznesowych i wymogom w zakresie wymiany informacji administracji europejskiej oraz administracji krajowych. Obecnie z tej bezpiecznej sieci udostępnianej przez Komisję Europejską korzysta ponad 30 aplikacji.

W styczniu 2010 r. EIOD przyjął sprawozdanie z 22 zaleceniami odnoszącymi się do kontroli przeprowadzonej wcześniej w Centrum Usługowo-Operacyjnym e-TESTA. W grudniu 2010 r. Komisja przesłała do EIOD sprawozdanie z wdrożenia odnoszące się do tych zaleceń i wskazujące, że 12 z nich już zostało wdrożonych. Pozostałych 10, które wymagały bardziej znaczących inwestycji, zostało zawartych w planie ciągłego udoskonalania systemu i zostaną one zakończone w 2011 r. EIOD sprawdzi pozostałe te elementy w ramach nowych działań następczych planowanych w połowie 2011 r.

Kontrola we Wspólnym Centrum Badawczym

W grudniu 2010 r. EIOD przeprowadził kontrolę na miejscu we Wspólnym Centrum Badawczym w Isprze. Ogólny brak współpracy ze strony Centrum wraz z potrzebą sprawdzenia faktów i weryfikacji wdrożenia zaleceń na miejscu zaowocował decyzją o przeprowadzeniu kontroli.

Badane były dwa główne obszary: wybór i rekrutacja personelu JRC oraz procedury wdrożone przez służbę bezpieczeństwa (kontrola bezpieczeństwa przed zatrudnieniem, dochodzenia w zakresie bezpieczeństwa, kontrola dostępu i nagrywanie połączeń alarmowych). We wszystkich tych sprawach informacje o stanie faktycznym zostały uzyskane z analiz kontroli wstępnych.

Podczas kontroli współpraca pomiędzy EIOD a odpowiednimi jednostkami Centrum była produktywna i pozwoliła kontrolującym stwierdzić między innymi, że problemy komunikacyjne były główną przyczyną wcześniejszego braku współpracy. Na podstawie tych ustaleń EIOD wyda sprawozdanie z kontroli z nowymi zaleceniami dla zapewnienia lepszego przestrzegania rozporządzenia.

2.6. Konsultacje w sprawie środków administracyjnych

2.6.1. Konsultacje na mocy art. 28 ust. 1 i art. 46 lit. d)

Rozporządzenie (WE) nr 45/2001 stwierdza, że EIOD ma prawo do uzyskiwania informacji o środkach administracyjnych, które dotyczą przetwarzania danych osobowych (art. 28 ust. 1). EIOD może wydać opinię **na wniosek** *danej instytucji lub organu albo* **z własnej inicjatywy**.

Termin „środki administracyjne" należy rozumieć jako wydaną przez administrację decyzję o charakterze ogólnym dotyczącą przetwarzania danych osobowych przez daną instytucję lub organ (np. środki wykonawcze do rozporządzenia lub ogólne wewnętrzne przepisy i zasady oraz decyzje przyjęte przez administrację w związku z przetwarzaniem danych osobowych).

Ponadto art. 46 lit. d) rozporządzenia przewiduje bardzo szeroki zakres przedmiotowy konsultacji, rozszerzając go na „wszystkie kwestie dotyczące przetwarzania danych osobowych". Na tej podstawie EIOD doradza instytucjom i organom w konkretnych przypadkach związanych z przetwarzaniem danych lub w kwestiach ogólnych dotyczących wykładni rozporządzenia.

W ramach konsultacji w sprawie środków administracyjnych planowanych przez instytucje lub organy poruszano rozmaite zagadnienia; część z nich przedstawiono poniżej.

2.6.2. Żądanie dostępu do tożsamości informującego – Europejski Rzecznik Praw Obywatelskich

Europejski Rzecznik Praw Obywatelskich konsultował się z EIOD w kwestii poruszonej w skardze wniesionej przeciwko OLAF. Konsultacje obejmowały szereg pytań, takich jak:

- czy tożsamość osób, które przekazują OLAF informacje, takich jak informatorzy i osoby zgłaszające przypadki naruszenia, nie powinna być ujawniana nikomu poza organami sądowymi;

- czy ochrona informatorów i osób zgłaszających przypadki naruszenia musi być gwarantowana po zamknięciu dochodzenia, kiedy brak działań następczych, a jeśli tak, to w jaki sposób i w jakim zakresie.

EIOD wydał uwagi na poziomie regulacyjnym czy strategicznym, a nie w odniesieniu do konkretnej skargi przeciwko OLAF. EIOD przyjął stanowisko, że co do zasady tożsamość osób zgłaszających przypadki naruszenia czy informatorów nie powinna być ujawniana, z wyłączeniem przypadków, w których naruszałoby to krajowe zasady postępowania sądowego lub gdy osoby takie w złej wierze podały fałszywe zeznania. W takich przypadkach te dane osobowe mogą zostać ujawnione wyłącznie organom sądowym.

W odniesieniu do drugiego pytania EIOD stwierdził, iż istnieją uzasadnione powody, aby uznać, że ochrona osób zgłaszających przypadki naruszenia czy informatorów powinna być taka sama po zamknięciu dochodzenia, niezależnie od tego, czy podjęto działania następcze, czy też nie. Szczególny charakter roli osoby zgłaszającej przypadki naruszenia czy informatora, a więc i zagrożenie dla jego prywatności i integralności nie zmieniają się w zależności od tego, czy dochodzenie jest otwarte czy zamknięte bez działań następczych.

W praktyce podejście takie nie wyklucza oczywiście sytuacji, w których ochrona osoby zgłaszającej przypadki naruszenia czy informatora powinna być wyłączona przez uzasadnione roszczenia innych osób. Upływ czasu może być istotnym czynnikiem, ale oczywiście trudno jest abstrakcyjnie spekulować na ten temat.

2.6.3. Międzynarodowe przekazywanie danych osobowych – Europejska Agencja Bezpieczeństwa Lotniczego

Europejska Agencja Bezpieczeństwa Lotniczego (EASA) wykonuje określone zadania (np. usługi w zakresie certyfikacji), które wiążą się z uiszczaniem opłat i należności przez wnioskodawców. Część z tych działań certyfikacyjnych może być wykonywana w całości lub częściowo poza terytorium państw członkowskich. W niektórych przypadkach wnioskodawcy zwracają się do Agencji o przekazanie im nazwisk i dat podróży ekspertów w celu umożliwienia im zapłaty faktury.

Inspektor ochrony danych EASA wystąpił o poradę do EIOD w zakresie zastosowania art. 9 rozporządzenia do rozważanej sprawy.

Zgodnie z art. 9 ust. 1 dane osobowe mogą być przekazywane odbiorcom innym niż instytucje i organy UE, które nie podlegają prawu krajowemu przyjętemu zgodnie z dyrektywą 95/46/WE, jeśli **zapewniony jest wystarczający poziom ochrony** w państwie odbiorcy.

EIOD podkreślił, że jeśli państwo trzecie, o którym mowa, spoza EOG nie zapewnia wystarczającego poziomu ochrony, należy uwzględnić pozostałe warunki wymienione w art. 9. Art. 9 ust. 6 wskazuje, że „W drodze odstępstwa od ust. 1 i 2 instytucja lub organ Wspólnoty może przekazać dane osobowe, jeżeli:(...) d) przekazanie danych jest konieczne lub wymagane przez prawo z ważnych względów publicznych (...)".

Jako że wykonywanie tych usług stanowi jeden z kluczowych obszarów działalności EASA, przekazanie danych w związku z płatnościami za te usługi może być uznane, co do zasady, za **konieczne dla funkcjonowania tego organu**, a więc kwalifikujące się do odstępstwa na podstawie art. 9 ust. 6 lit. d).

EIOD zauważył również że w tej sprawie wydawało się, że przekazanie danych nie będzie „powtarzalne, masowe lub strukturalne", a że będzie mieć miejsce jako „jednorazowe" przekazanie danych różnym odbiorcom w różnych krajach. Jeśli chodzi o zagrożenia dla osób, których dane dotyczą, trudno wskazać na szczególne ryzyka. Kategorie danych do przekazania (nazwisko i data podróży danego eksperta) wydają się również nie budzić szczególnych obaw.

EIOD wskazał jednakże, że nie ustanowiono zabezpieczeń w tych przypadkach, gdzie zastosowano wyjątek. Z tego względu zalecił on uwzględnienie klauzuli, która wskazywałaby, że odbiorca jest prawnie upoważniony do żądania tych danych, i ograniczałaby użycie tych danych tylko do celów uzasadniających przekazanie danych.

2.6.4. Polityka w zakresie wewnętrznego wykorzystania e-maili – Komisja Europejska

Komisja Europejska konsultowała się z EIOD w odniesieniu do swojej polityki w zakresie wewnętrznego wykorzystania e-maili. EIOD

przeanalizował wybrane punkty polityki pod kątem ochrony danych osobowych i zasad prywatności, a także środków bezpieczeństwa.

W tym kontekście Komisja poinformowała EIOD, że nie będzie przeprowadzać na dużą skalę monitorowania na poziomie indywidualnym. W piśmie przesłanym do EIOD stwierdzono że „[j]edyna forma rutynowego monitoringu, który ma miejsce w ramach służby ds. e-maili Komisji (DG DIGIT), ma miejsce na poziomie DG/usługi, a nie na poziomie indywidualnych skrzynek e-mail lub indywidualnych danych o ruchu. DG DIGIT monitoruje korzystanie z usług w celu ograniczenia zagrożeń operacyjnych, ale nie sporządza się rutynowych sprawozdań z monitorowania indywidualnej działalności w poczcie lub indywidualnych danych o ruchu, które mogłyby być wykorzystane do analizy indywidualnych naruszeń".

To powoduje, że jakiekolwiek monitorowanie indywidualnych skrzynek e-mail może mieć miejsce **tylko w ramach toczącego się dochodzenia**. EIOD z zadowoleniem przyjął to podejście, które uznaje za najlepszą praktykę.

2.6.5. Prawa administratora IT – Europejski Bank Inwestycyjny

Dnia 26 marca 2010 r. EIOD odpowiedział na konsultację z Europejskiego Banku Inwestycyjnego (EBI) z zaleceniami dotyczącymi zarządzania dostępem administratorów IT do danych osobowych przechowywanych w systemach informatycznych i aplikacjach. EIOD podkreślił potrzebę zastosowania **zasady podziału obowiązków**. Poziom podziału powinien zostać określony w świetle poziomu ryzyka zidentyfikowanego dla odpowiednich procesów.

Zarządzanie prawami dostępu administratorów IT powinno być rozwiązywane poprzez zrównoważone podejście między środkami organizacyjnymi i technicznymi. EIOD zalecił również, aby środki te zostały odpowiednio udokumentowane w szczegółowej polityce bezpieczeństwa ustanowionej dla instytucji.

2.6.6. Monitorowanie komunikacji telefonicznej

Skonsultowano się z EIOD w kwestii projektu monitorowania komunikacji telefonicznej, która przekroczyła określony wstępnie próg.

Planowany system byłyby oparty na uzgodnionym progu (tolerowana liczba godzin lub tolerowany koszt komunikacji telefonicznej), który byłby zaoferowany personelowi. Na koniec miesiąca menedżerowie otrzymywaliby listę użytkowników będących ich pracownikami, których komunikacja związana z rozmowami zagranicznymi i rozmowami z telefonów komórkowych (prywatna i zawodowa) przekraczałaby progi w ostatnim miesiącu.

EIOD stwierdził, że zgodność z prawem przetwarzania takich danych wynika z uzasadnionego wykonywania urzędowego uprawnienia instytucji czy organu do wydajnego zarządzania wykorzystaniem narzędzi telekomunikacyjnych w obrębie instytucji czy organu (art. 5a rozporządzenia w powiązaniu z przepisami art. 37 ust. 2). EIOD uznał jednak, że takie ogólne monitorowanie, w odróżnieniu od bardziej selektywnego monitorowania, nie jest zawsze konieczne.

Mimo że EIOD zaakceptował jako uzasadniony cel zarządzania budżetem, wskazał on również, że monitorowanie użycia telefonów do celów prywatnych, nawet bez przekazania szczegółów wykonanych rozmów, mogłoby być potencjalnie uznane za naruszenie prawa do prywatności członków personelu.

W tym zakresie EIOD zażądał, aby instytucje lub organy dopilnowały, by wartość progu, która prowadziłaby do wysłania listy do kierownictwa, była odpowiednio wysoka, by uniknąć nieuzasadnionego monitorowania i zapewnić identyfikację tylko tych przypadków, w których dochodzi do wyraźnego lub powtarzającego się nadużywania systemu. Instytucja lub organ został również wezwany do zbadania, w jakim zakresie inne wskaźniki mogłyby być użyte do identyfikacji możliwych nadużyć.

EIOD zwrócił się w związku z tym do instytucji o ponowną ocenę proponowanego systemu i zbadania, czy mogą być zastosowane inne, mniej inwazyjne metody.

2.6.7. Dalsze przetwarzanie danych w celu ich przekazania do AMEX – Europejski Urząd ds. Bezpieczeństwa Żywności

Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA) przetwarza coroczną deklarację o braku konfliktu interesów dla niektórych osób zaangażowanych w działalność EFSA w celu weryfikacji,

Monitorowanie wykorzystania telefonów do prywatnych rozmów można co do zasady uznać za naruszenie prawa do prywatności pracowników.

czy u takich osób nie występuje konflikt interesów, który mógłby wpływać na działania wykonywane dla EFSA.

W trakcie kontroli wstępnej tej operacji przetwarzania danych (sprawa 2008-0737) inspektor danych osobowych EFSA wystąpił do EIOD o poradę w zakresie dalszego użycia bazy danych deklaracji o braku konfliktu interesów w celu przekazania do biura podróży, AMEX, danych identyfikujących zewnętrznych ekspertów.

Inspektor danych osobowych EFSA zapytał EIOD, czy dalsze przetwarzanie danych zawartych w bazie danych w celu ich przekazania do biura podróży wraz z danymi identyfikującymi zewnętrznych ekspertów jest zgodne z art. 4 ust. 1 lit. b) rozporządzenia.

Zgodnie z tym przepisem dane osobowe powinny być gromadzone do konkretnych, bezpośrednich i zgodnych z prawem celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

W opinii EIOD stwierdził, że jakiekolwiek dalsze przetwarzanie przez EFSA danych przetwarzanych w bazie deklaracji, do celów dostarczenia danych identyfikujących osoby, które mogą korzystać z usług turystycznych AMEX, stanowiłoby **zupełnie inny cel** i nie mogłoby zostać uznane za zgodne z pierwotnym celem gromadzenia i przetwarzania danych. Tym samym jakiekolwiek dalsze przetwarzanie danych przez EFSA nie jest zgodne z art. 4 ust. 1 lit. b) rozporządzenia.

EIOD wskazał dalej, że rola i odpowiedzialność AMEX w odniesieniu do danych nie była dostatecznie jasno określona w umowie w sprawie przekazania danych podpisanej pomiędzy stronami, w szczególności nie określono dostatecznie jasno, z jakich przyczyn i w jakich okolicznościach AMEX działa jako podmiot przetwarzający lub administrator danych. Należy wprowadzić odpowiednie gwarancje zapewniające prawa osób, których dane dotyczą, i zabezpieczyć dalsze przekazania danych przez AMEX do innych odbiorców, zgodnie z odpowiednimi przepisami o ochronie danych.

2.6.8. Okres zatrzymywania dokumentów medycznych - Rada Szefów Administracji

W listopadzie 2006 r. przewodniczący Rady Szefów Administracji (Rady) wystąpił o opinię EIOD na temat pisma przygotowanego przez Komisję dotyczącego okresu zatrzymywania niektórych dokumentów medycznych. EIOD wydał opinię w dniu 26 lutego 2007 r. podkreślającą, że 30-letni okres wskazany w piśmie nie powinien stanowić

minimalnego okresu zatrzymywania dokumentów medycznych. Przeciwnie, z pewnymi ograniczonymi wyjątkami, powinien być on uznany za *maksymalny* okres zatrzymywania dokumentów. Ponadto EIOD stwierdził, że zastosowanie zasady z art. 4 rozporządzenia oznacza, iż charakter dokumentów medycznych powinien zostać zbadany w celu określenia, jakie okresy zatrzymywania danych byłyby odpowiednie dla każdego typu dokumentu.

Zagadnienie zatrzymywania dokumentów medycznych zostało ponownie podniesione we wrześniu 2010 r., kiedy to *Comité de Préparation pour les Affaires Sociales* (CPAS), odpowiedni podkomitet Rady, przygotował sprawozdanie na temat różnych przypadków z poszczególnymi okresami zatrzymywania dokumentacji medycznej. W październiku 2010 r. Rada konsultowała się w sprawie sprawozdania z EIOD. EIOD obecnie bada zagadnienie i przedstawi swoje stanowisko w zakresie konsultacji, biorąc pod uwagę opinię z lutego 2007 r. i swoje stanowisko wyrażone w poprzednich opiniach dotyczących kontroli wstępnych.

2.6.9. Przepisy wykonawcze dotyczące Inspektora Ochrony Danych

*Rozporządzenie o ochronie danych wymaga, aby szczegółowe **przepisy wykonawcze w zakresie zadań, obowiązków i uprawnień inspektorów ochrony danych** zostały przyjęte przez każdą instytucję i organ UE. W lipcu 2010 r. EIOD wydał **wytyczne** w celu usprawnienia przygotowania przepisów wykonawczych, tam gdzie nie zostały one jeszcze przyjęte lub gdzie wymagają zmian.*

W maju 2010 r. Agencja Wykonawcza Europejskiej Rady ds. Badań Naukowych (ERCEA) przesłała do konsultacji EIOD przepisy wykonawcze dotyczące funkcji inspektora ochrony danych. Przepisy te obejmowały również rolę administratorów danych i zasady, zgodnie z którymi osoby, których dane dotyczą, mogą wykonywać swoje prawa. EIOD z zadowoleniem przyjął to globalne podejście, szczególnie biorąc pod uwagę, że ERCEA przyjęła najlepsze praktyki sugerowane przez lata przez EIOD, takie jak:

- utrzymywanie anonimowego wykazu pisemnych wniosków od osób, których dane dotyczą, w zakresie wykonania praw (dostęp, poprawianie, blokowanie itp.);

30-letni okres zatrzymywania dokumentacji medycznej należy uznać za maksymalnych okres zatrzymywania danych.

- współpraca ze służbami IT i bezpieczeństwa informacji Agencji w celu uzupełnienia źródeł informacji inspektora ochrony danych.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) i Trybunał Obrachunkowy również przedłożyły do konsultacji EIOD zmienione wersje przepisów wykonawczych. Konsultacje były zgodne z wytycznymi wydanymi przez EIOD.

2.7. Wytyczne tematyczne

Doświadczenia zebrane w trakcie stosowania rozporządzenia o ochronie danych pozwoliły personelowi EIOD przełożyć swoją wiedzę na ogólne wytyczne dla instytucji i organów w zakresie rekrutacji, danych dotyczących zdrowia, dochodzeń administracyjnych i postępowań dyscyplinarnych oraz nadzoru wideo. Obecnie EIOD pracuje nad wytycznymi dotyczącymi oceny personelu i przetwarzania danych osobowych w postępowaniach dotyczących nękania.

2.7.1. Wytyczne dotyczące dochodzeń administracyjnych i postępowań dyscyplinarnych

W kwietniu 2010 r. EIOD wydał wytyczne w zakresie przetwarzania danych osobowych w dochodzeniach administracyjnych i postępowaniach dyscyplinarnych przez instytucje i organy UE.

Celem wytycznych jest ujednolicenie dobrej praktyki w tej dziedzinie i ułatwienie przestrzegania przepisów rozporządzenia. Wytyczne w jasny i zwięzły sposób prezentują podsumowanie stanowisk EIOD po przeanalizowaniu ich w opiniach dotyczących kontroli wstępnych. Określają również kilka zaleceń w odniesieniu do każdej podstawowej zasady rozporządzenia.

Jedno ważne zalecenie dotyczy **prawa dostępu i prawa do poprawiania** dla osoby, której dane dotyczą. Prawa te mogą co prawda niekiedy zostać ograniczone, administrator danych powinien jednak dopilnować, by takie ograniczenia były konieczne i były wprowadzane indywidualnie. Ponadto administrator danych powinien dopilnować, by prawo dostępu i prawo do poprawiania oraz prawo do informacji były gwarantowane za pomocą innych środków.

EIOD wskazuje również na brak jednolitego podejścia do **okresu zatrzymywania danych dotyczących postępowań dyscyplinarnych**, co prowadzi do naruszeń zasad ochrony danych i innych podstawowych praw osób, który dane dotyczą. Wynika to z pewnych poważnych luk w załączniku IX do regulaminu pracowniczego i braku wspólnej polityki wśród instytucji i organów UE w zakresie zatrzymywania takich danych.

W końcu EIOD podkreśla konieczność bardziej szczegółowego uwzględnienia specyficznej kwestii **przechwytywania wiadomości**, ze szczególnym naciskiem na podstawę prawną podsłuchiwania wiadomości głosowych i możliwość takiego podsłuchiwania bez nakazu sądowego lub upoważnienia.

Wytyczne mają być wykorzystywane przez agencję w powiadomieniach EIOD o postępowaniach w tym zakresie do celów kontroli wstępnej, ale powinny także służyć jako praktyczny przewodnik dla wszystkich instytucji i organów. Kolejnym krokiem EIOD będzie wydanie wspólnej opinii dotyczącej powiadomień przedłożonych przez agencje do celów kontroli wstępnej w świetle wspomnianych wytycznych.

2.7.2. Wytyczne w zakresie nadzoru wideo

W marcu 2010 r. EIOD wydał praktyczny zestaw wytycznych dla instytucji i organów UE, w jaki sposób wykorzystywać nadzór wideo w sposób odpowiedzialny i z zastosowaniem skutecznych zabezpieczeń. Wytyczne określają zasady oceny konieczności uciekania się do nadzoru wideo i podpowiadają, jak wprowadzać taki nadzór w sposób minimalizujący jego wpływ na prywatność i inne prawa podstawowe.

Projekt wersji do konsultacji opublikowano w lipcu 2009 r., jak podano w sprawozdaniu rocznym EIOD za 2009 r. Proces konsultacji pozwolił uzyskać informację zwrotną o potrzebie poprawy projektu wytycznych i zwiększeniu współpracy zainteresowanych stron.

Wytyczne wskazywały, że decyzje o zamontowaniu kamer i sposobie ich wykorzystania nie powinny być oparte wyłącznie na potrzebach w zakresie bezpieczeństwa. Należy raczej **szukać równowagi**

pomiędzy potrzebami w zakresie bezpieczeństwa a prawami podstawowymi jednostki. Niezależnie od powyższego prawa podstawowe i bezpieczeństwo nie muszą się wzajemnie wykluczać. Dzięki pragmatycznemu podejściu opartemu na zasadach selektywności i proporcjonalności systemy nadzoru wideo mogą zaspokajać potrzeby w zakresie bezpieczeństwa przy jednoczesnym poszanowaniu prywatności.

W ramach ograniczeń ustanowionych w przepisach z zakresu ochrony danych każda instytucja i organ dysponuje swobodą uznania w zakresie opracowania własnego systemu. Wytyczne mają umożliwić indywidualne dostosowanie systemu. Ta elastyczność powinna nie dopuszczać, by sztywna i biurokratyczna interpretacja kwestii ochrony danych szkodziła uzasadnionym potrzebom bezpieczeństwa lub innym uzasadnionym celom.

Jednocześnie każda instytucja musi również **wykazać, że wdrożono procedury zapewniające zgodność** z wymogami ochrony danych. Zalecane praktyki organizacyjne obejmują przyjęcie zestawu gwarancji ochrony danych, które powinny być określone w polityce nadzoru wideo instytucji, oraz okresowe audyty w celu weryfikacji zgodności. Zaleca się wykonanie przez instytucje oceny skutków, podczas gdy kontrole wstępne EIOD będą wciąż wymagane dla nadzoru wideo, z którym nieodłącznie wiążą się zagrożenia (takie jak niejawny nadzór lub złożone dynamiczne systemy nadzoru prewencyjnego).

Okres przejściowy

Wytyczne odnoszą się do istniejących i przyszłych systemów: każda instytucja do 1 stycznia 2011 r. musi zapewnić zgodność jej istniejących praktyk z przepisami. EIOD będzie w dalszym ciągu dostępny, jeśli wystąpi potrzeba dalszego doradztwa w konkretnych sprawach.

EIOD będzie również wspierać te instytucje, które już złożyły powiadomienia dotyczące kontroli wstępnych przed wydaniem wytycznych. Było dziewięć takich spraw. W lipcu 2010 r. EIOD wydał wstępne zalecenia w tych sprawach, przy założeniu, że zgodności z tymi zaleceniami nie można uznać za odpowiednik dogłębnej, wewnętrznej analizy wytycznych, własnych praktyk i statusu zgodności, przez samą instytucję. Uwagi EIOD miały na celu pomoc omawianym instytucjom w skupieniu uwagi na kluczowych zagadnieniach, które wymagają rozwiązania. Kwestie wymagające szczególnej uwagi obejmowały niejawny nadzór i okres zatrzymywania dokumentów.

W podobnym duchu EIOD wydał również wstępne wskazówki dla OLAF, którego system nadzoru wideo jako jedyny podlegał kontroli wstępnej EIOD przed wydaniem wytycznych (ponieważ było to faktyczne powiadomienie o kontroli wstępnej nowego systemu, które z tego względu musiało zostać potraktowane priorytetowo).

EIOD w dalszym ciągu udzielał wskazówek dla innych instytucji w odniesieniu do wykładni

Instytucje UE mają czas do 1 stycznia 2011 r. na wykazanie zgodności z wytycznymi EIOD.

i wdrożenia wytycznych oraz kontynuował przyjmowanie skarg i konsultacji, w tym skarg przeciwko praktykom niejawnego nadzoru w jednej z instytucji oraz dochodzeniu administracyjnemu dotyczącemu ograniczeń w użyciu materiału z nadzoru wideo jako dowodu, jeśli został on uzyskany w sposób naruszający zasady ochrony danych.

2.8. Polityka przestrzegania i egzekwowania prawa EIOD

W grudniu 2010 r. EIOD przyjął dokument strategiczny „Monitorowanie i zapewnianie zgodności z rozporządzeniem (WE) nr 45/2001".

Dokument ten jest znakiem nowej ery w egzekwowaniu rozporządzenia. Do tej pory EIOD preferował wydawanie zaleceń i zachęcanie do przestrzegania przepisów od ostrzegania i wydawania upomnień administratorom danych czy wydawania prawnie wiążących nakazów. Po pięciu latach takich działań EIOD uważa, że nadszedł czas na przyjęcie bardziej **zdecydowanego podejścia do egzekwowania przepisów**, szczególnie w przypadkach poważnego, umyślnego lub powtarzającego się nieprzestrzegania zasad ochrony danych. Tym samym dokument wprowadza zestaw kryteriów, które zapewnią proaktywne, spójne i przejrzyste zastosowanie uprawnień do egzekwowania przepisów.

Dokument określa ramy, w których EIOD monitoruje, ocenia i zapewnia przestrzeganie zasad ochrony danych przez administrację UE. Wyjaśnia on charakter różnych uprawnień do egzekwowania prawa dostępnych dla EIOD oraz określa czynniki i warunki wszczynania formalnych działań, które może podjąć.

Dokument ma na celu **zachęcanie do dobrowolnego przestrzegania i wprowadzania najlepszych praktyk** oraz wprowadza odpowiednie zachęty do przestrzegania poprzez:

- podkreślanie, gdzie leży odpowiedzialność za przestrzeganie przepisów;
- wyjaśnianie, jak EIOD może wspierać to przestrzeganie przepisów;
- wyjaśnianie, co zrobi EIOD w przypadku nieprzestrzegania przepisów.

Dokument kładzie również silny nacisk na **zasadę „rozliczalności"**, która ma zachęcać do przestrzegania przepisów i przyjęcia najlepszych praktyk przez administrację UE. Rozliczalność wymaga od instytucji i organów UE oraz administratorów

EIOD uważa, że nadszedł czas na przyjęcie bardziej zdecydowanego podejścia do egzekwowania przepisów.

danych działania we własnym imieniu, wprowadzenia odpowiednich i skutecznych środków dla zapewnienia przestrzegania obowiązków z zakresu ochrony danych oraz późniejszego wykazania EIOD tej zgodności.

Wreszcie dokument określa podejście EIOD do **przejrzystości i publikacji** działań egzekwujących, kładąc nacisk na to, że są to ważne narzędzia dla zainteresowanych stron, a także z punktu widzenia dobrej administracji. Tym samym, w przyszłości EIOD będzie co do zasady publikować informacje dotyczące wszelkich oficjalnych wniosków do Parlamentu, Rady, Komisji lub Trybunału Sprawiedliwości. Ponadto rozważy on również, dla każdego przypadku z osobna, czy należy upublicznić którekolwiek z jego innych działań egzekwujących.

EIOD ma nadzieję, że umożliwiając mu skoncentrowanie się na jego odpowiedzialności za monitorowanie i zapewnianie zgodności z rozporządzeniem poprzez selektywne, ukierunkowane, oparte na ocenie ryzyka podejście do egzekwowania prawa, omawiany dokument strategiczny zapewni bardziej skuteczne i efektywne wykorzystanie zasobów EIOD.

3 KONSULTACJE

3.1. Wprowadzenie: przegląd roku i główne tendencje

W 2010 r. Komisja poczyniła znaczne postępy w zakresie nowych, **zmodernizowanych ram prawnych ochrony danych w Europie**. Zakończono konsultację społeczną rozpoczętą w 2009 r. i uzupełniono ją o bardziej ukierunkowane konsultacje z kilkami kluczowymi zainteresowanymi stronami.

W listopadzie 2010 r. Komisja wydała komunikat ustanawiający całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej, określający priorytety i zasadnicze cele przeglądu obecnych zasad.

Projekt ten zajmował ważne miejsce w harmonogramie prac EIOD na 2010 r. i będzie to jeden z jego ścisłych priorytetów na nadchodzące lata.

W 2010 r. Komisja i Rada poczyniły również znaczące wysiłki w celu **wdrożenia programu sztokholmskiego** – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli, przyjętego przez Radę Europejską w grudniu 2009 r. Program określa strategiczne wytyczne na potrzeby planowania ustawodawczego i operacyjnego w obszarze wolności, bezpieczeństwa i sprawiedliwości oraz koncentruje się na interesach i potrzebach obywateli.

*W programie sztokholmskim podkreślono, że **środki bezpieczeństwa i egzekwowania prawa oraz przestrzeganie praw podstawowych, w tym ochrona danych, muszą iść ze sobą w parze**. Uznaje on również potrzebę ochrony danych osobowych w globalnym społeczeństwie, które charakteryzuje się szybkim postępem technicznym i nieograniczoną wymianą informacji.*

Kilka inicjatyw bezpośrednio związanych z wdrażaniem programu sztokholmskiego było ściśle monitorowanych przez EIOD. Między innymi EIOD zajmował się kluczowymi kwestiami ochrony danych związanymi ze strategią bezpieczeństwa wewnętrznego UE, z zarządzaniem informacją w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz polityką zwalczania terroryzmu UE. Ogólnie rzecz biorąc, postępy w zakresie programu sztokholmskiego były głównymi punktami w harmonogramie prac EIOD i będą dalej dominować na przestrzeni kilku kolejnych lat.

Związek pomiędzy prywatnością a postępem technicznym był również obszarem znaczących działań EIOD. W maju 2010 r. Komisja opublikowała komunikat dotyczący europejskiej agendy cyfrowej w celu ustanowienia priorytetów UE w zakresie technologii internetowych i cyfrowych. Kilka z tych inicjatyw ma duże znaczenie dla ochrony danych i jest skrzętnie monitorowanych przez EIOD. EIOD jest także przekonany, że nowe technologie nie tylko wiążą się z nowymi wyzwaniami dla prywatności i ochrony danych, ale także niosą ze sobą nowe możliwości w zakresie ochrony danych.

Bardzo ważne więc, by wymogi prywatności były uwzględniane przy projektowaniu i funkcjonowaniu systemów TIK oraz przy zarządzaniu nimi, przez cały cykl życia informacji. EIOD zaleca więc usilnie włączenie zasady „wbudowanej ochrony prywatności" do ram prawnych.

Z EIOD skonsultowano się również w kwestii inicjatyw w dziedzinie **współpracy międzynarodowej z zakresu bezpieczeństwa i egzekwowania prawa**, takich jak ogólna umowa UE-USA w sprawie wymiany danych w celu egzekwowania prawa oraz umowa w sprawie wymiany danych finansowych do celów programu śledzenia środków finansowych należących do terrorystów (TFTP). Wypowiedział się także na temat umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA) i kilku umów w sprawie wymiany danych dotyczących przelotu pasażera (PNR).

EIOD działał także w innych obszarach, takich jak wielkoskalowa wymiana danych w kontekście systemu wymiany informacji na rynku wewnętrznym, użytkowanie skanerów ciała w portach lotniczych i współpraca w zakresie opodatkowania.

Ogromna różnorodność obszarów polityki, w sprawie których konsultowano się z EIOD, jest kolejnym dowodem na to, że przetwarzanie danych coraz częściej staje się zasadniczym elementem licznych inicjatyw ustawodawczych. Inicjatywy te wiążą się często z ważnymi kwestiami ochrony danych, a tym samym ponownie uzasadniają rolę EIOD jako doradcy instytucji UE.

3.2. Ramy polityki i priorytety

3.2.1. Realizacja polityki konsultacyjnej

Chociaż metody pracy EIOD w dziedzinie konsultacji rozwijały się na przestrzeni lat, podstawowe podejście do konsultacji nie uległo zmianie. Dokument przyjęty w marcu 2005 r. zatytułowany „The EDPS as an advisor to the Community institutions on proposals for legislation and related documents"[8] („EIOD jako doradca instytucji wspólnotowych w sprawie wniosków ustawodawczych i pokrewnych dokumentów") pozostaje aktualny, chociaż należy go teraz interpretować w świetle traktatu lizbońskiego.

Oficjalne opinie EIOD – wydawane na podstawie art. 28 ust. 2 lub art. 41 rozporządzenia (WE) nr 45/2001 – stanowią podstawowe instrumenty zawierające pełną analizę wszystkich aspektów wniosku Komisji lub innego stosownego instrumentu związanych z ochroną danych.

Co do zasady EIOD wydaje opinie w sprawie aktów o charakterze nieustawodawczym (takich jak dokumenty robocze, komunikaty lub zalecenia Komisji), jeśli ochrona danych jest ich kluczowym elementem. Od czasu do czasu wydawane są też uwagi na piśmie o bardziej ograniczonym zakresie, których celem jest zwięzłe przedstawienie podstawowych kwestii politycznych lub skupienie się na jednym lub na większej liczbie aspektów technicznych, lub też podsumowanie lub powtórzenie wcześniej poczynionych uwag.

Można także wykorzystać inne instrumenty, takie jak prezentacje ustne, pisma wyjaśniające, konferencje prasowe lub komunikaty prasowe. Dla przykładu, w 2010 r. EIOD odbył konferencję prasową zatytułowaną „Przyszłość ram prawnych ochrony danych UE" w połączeniu z prezentacją sprawozdania rocznego z 2009 r.

Z EIOD można się konsultować we wszystkich fazach opracowywania polityki i prawodawstwa; wykorzystuje on także szereg innych instrumentów wywierania wpływu. Może to wymagać ścisłej współpracy z instytucjami UE, najważniejszą kwestią pozostaje jednak ochrona jego niezależności.

Kontakty z Komisją mają miejsce na różnych etapach opracowywania wniosków, a ich intensywność jest zależna od przedmiotu wniosku, a także podejścia służb Komisji. Dotyczy to w szczególności długoterminowych projektów, takich jak inicjatywa e-sprawiedliwość lub przegląd ram ochrony danych, w których EIOD uczestniczył na różnych etapach.

Regularne kontakty z odpowiednimi służbami instytucji miały też miejsce w fazie monitorowania dalszych działań. W niektórych przypadkach EIOD i jego pracownicy byli ściśle zaangażowani w dyskusje i negocjacje w Parlamencie i Radzie. W innych przypadkach Komisja była głównym rozmówcą na etapie monitorowania dalszych działań. Proces prawodawczy dotyczący rozporządzenia Frontex,

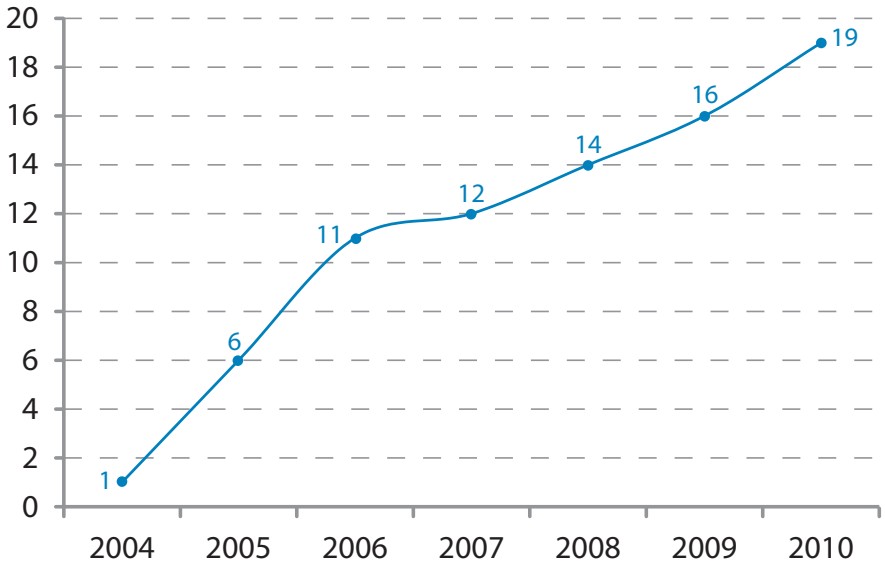
[8] Dostępny na stronie internetowej EIOD w zakładce Publications > Papers.

monitorowania agendy cyfrowej (na przykład w kwestii neutralności sieci) oraz systemu wymiany informacji na rynku wewnętrznym to kolejne przykłady intensywnego zaangażowania prowadzącego do kolejnych uwag EIOD w 2010 r.

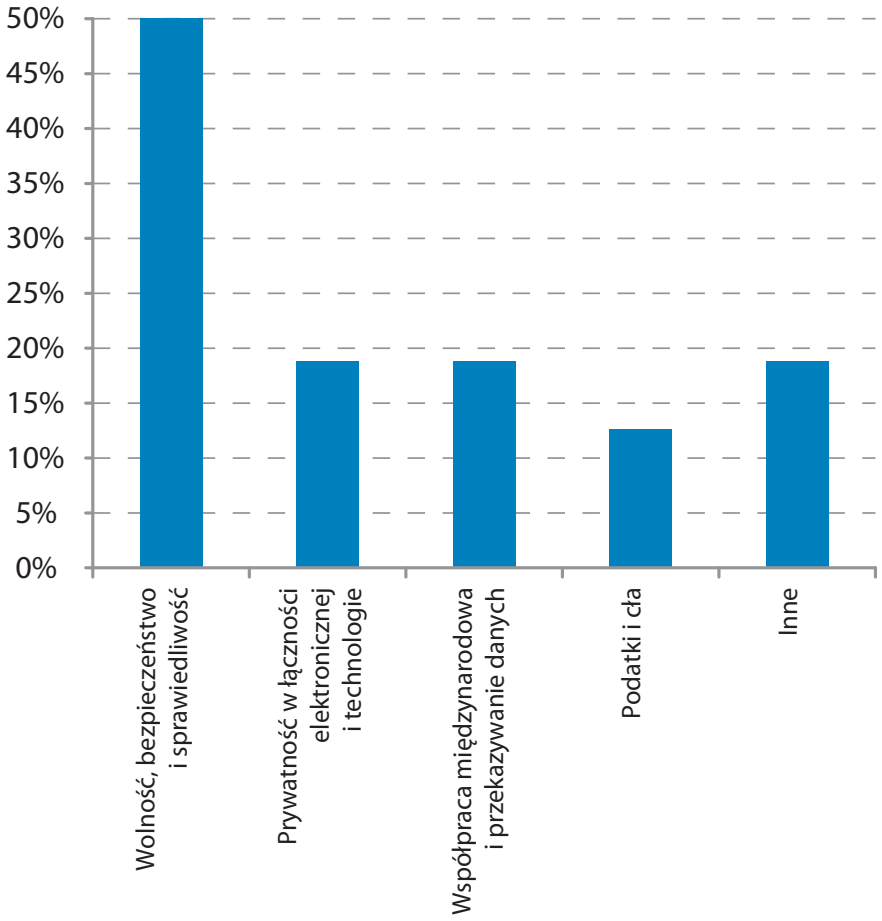
3.2.2. Wyniki w 2010 r.

W 2010 r. utrzymywał się systematyczny wzrost liczby opinii. EIOD wydał 19 opinii dotyczących różnorodnych kwestii.

Rozwój opinii w sprawie wniosków ustawodawczych w latach 2004–2010



Główne obszary polityki opinii w sprawie wniosków legislacyjnych w 2010 r.



Opinie te i inne instrumenty interwencyjne stanowiły realizację priorytetów EIOD na 2010 r. zgodnie z jego spisem. 19 wydanych opinii dotyczyło różnych obszarów polityki UE.

Spis na 2010 r. określał cztery główne obszary zainteresowania:

- nowe ramy prawne ochrony danych;
- wolność, bezpieczeństwo i sprawiedliwość;
- współpraca międzynarodowa i przekazywanie danych;
- postęp techniczny.

EIOD skoncentrował się w znacznym stopniu na tych wszystkich obszarach w 2010 r. Realizując spis na 2010 r., EIOD skupił się głównie na tych inicjatywach, którym przypisano bezwzględne pierwszeństwo w spisie (tj. na czerwonych inicjatywach): EIOD wydał opinię lub zareagował w inny sposób w 13 z 15 ściśle priorytetowych wniosków[9], które przyjęto na przestrzeni 2010 r.

Treść opinii EIOD i inne środki z zakresu konsultacji opisano szczegółowo poniżej.

3.3. Przegląd ram ochrony danych UE

Przegląd ram prawnych ochrony danych UE był już jednym z głównych priorytetów EIOD w 2009 r., gdy to rozpoczęto oficjalną debatę nad reformą. W 2010 r. zainteresowanie reformą znacznie wzrosło za sprawą publikacji komunikatu ustanawiającego całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej w listopadzie 2010 r. EIOD ze szczególną uwagą podchodził do tego zagadnienia przez cały 2010 r. i wypowiadał się w tej kwestii na różne sposoby.

EIOD zorganizował specjalną **konferencję prasową** tuż po publikacji komunikatu w celu publicznego wyrażenia swojego poglądu na temat nowych ram prawnych. Przy tej okazji podkreślił ważność przeglądu, który w jego ocenie ma miejsce w odpowiednim momencie i wyraził opinię na temat głównych elementów nowych ram.

[9] W dwóch z tych spraw (przegląd rozporządzenia (WE) nr 831/2002 dotyczącego dostępu do poufnych danych do celów naukowych oraz decyzji ramowej Rady w sprawie ataków na systemy informatyczne) opinii nie uznano za konieczną na tym etapie.

Nowe ramy ochrony danych muszą być ambitne, muszą także faktycznie zwiększać skuteczność instrumentów ochrony danych w zglobalizowanym i pełnym technologii świecie.

*EIOD podkreślił potrzebę **mocnej i skutecznej ochrony danych** w społeczeństwie, w którym dane osobowe są wykorzystywane w przeogromnych ilościach, bardzo często bez świadomości osób, których dane dotyczą. EIOD z zadowoleniem przyjął komunikat Komisji, ostrzegł jednak, że **nie ma miejsca na błędy**: wyzwania są ogromne, zaproponowane rozwiązanie muszą więc być równie **ambitne** i muszą zwiększać skuteczność instrumentów ochrony danych.*

EIOD przedstawił również swoją opinię na temat głównych elementów nowych ram. W szczególności podkreślił:

- swoje poparcie dla **dalszego ujednolicania** krajowych przepisów dotyczących ochrony danych;
- potrzebę **technicznie neutralnego** podejścia;
- uwzględnienie zasad **wbudowanej ochrony prywatności i rozliczalności**;
- wprowadzenie **obowiązkowego powiadamiania o naruszeniu bezpieczeństwa**, obejmującego wszystkie właściwe sektory;
- **włączenie** obszarów **policji i wymiaru sprawiedliwości** do ogólnych ram.

EIOD opracował szczegółowo te poglądy w całościowej opinii przyjętej w styczniu 2011 r.

Oczekuje się, że Komisja przyjmie pełny wniosek ustawodawczy na przestrzeni 2011 r. EIOD będzie kontynuował ścisłe monitorowanie procesu ustawodawczego w 2011 r. i będzie wydawał, odpowiednio do sytuacji, nowe dokumenty.

3.4. Przestrzeń wolności, bezpieczeństwa i sprawiedliwości

W 2010 r. EIOD śledził ze szczególnym zainteresowaniem postępy we wdrażaniu **programu sztokholmskiego** i wydał zalecenia dotyczące kilku inicjatyw o charakterze ustawodawczym i nieustawodawczym, bezpośrednio lub pośrednio związanych z przestrzenią wolności, bezpieczeństwa i sprawiedliwości.

3.4.1. Strategia bezpieczeństwa wewnętrznego UE

Strategia bezpieczeństwa wewnętrznego UE (ISS) przedstawia europejski model bezpieczeństwa mający na celu zintegrowanie działań w zakresie egzekwowania prawa i współpracy sądowej, zarządzania granicami i ochroną ludności. Po ISS, zatwierdzonej przez Radę w lutym 2010 r. i potwierdzonej przez Radę Europejską miesiąc później, pojawił się komunikat Komisji w listopadzie 2010 r. odnoszący się do najpilniejszych zagrożeń dla bezpieczeństwa, przed którymi stoi UE, takich jak przestępczość zorganizowana, terroryzm, cyberprzestępczość, zarządzanie granicami zewnętrznymi UE i klęski żywiołowe.

EIOD wezwał do opracowania skutecznej strategii bezpieczeństwa wewnętrznego, wspieranej solidnym systemem ochrony danych uzupełniającym tę strategię.

Ze względu na **potencjalne inwazyjny** charakter środków, jakie mają zostać podjęte w ramach strategii, EIOD ściśle przyglądał się dyskusjom na temat ISS i działaniom planowanym w ramach wdrażania tej strategii. W swojej opinii przyjętej w grudniu 2010 r. EIOD podkreślił potrzebę zapewnienia **właściwej równowagi** pomiędzy celem, jakim jest zapewnienie bezpieczeństwa obywatelom, a skuteczną ochroną ich prywatności i danych osobowych. EIOD zwrócił także uwagę na fakt, że ISS jest w oczywisty sposób **politycznie powiązana z innymi strategiami UE**, które są obecnie opracowywane na poziomie UE, takimi jak strategia w zakresie zarządzania informacjami i przegląd ram prawnych ochrony danych UE.

EIOD wzywa do **pełniejszego i bardziej zintegrowanego podejścia do ISS**, zapewniającego wyraźne powiązania i interakcje pomiędzy poszczególnymi odnośnymi inicjatywami. Uważa on, że skuteczna ISS nie może zostać wprowadzona bez wsparcia w postaci trwałego systemu ochrony danych, który będzie ją uzupełniał.

3.4.2. Zarządzanie informacjami

Program sztokholmski zachęcił Komisję do oceny potrzeby opracowania **europejskiego modelu wymiany informacji** w oparciu o ocenę obecnych instrumentów wymiany informacji. Program odnosił się również do **silnego systemu ochrony danych** jako do głównego warunku wstępnego strategii UE w zakresie zarządzania informacjami. W lipcu 2010 r. Komisja przyjęła **komunikat – Przegląd zarządzania informacjami** w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w sprawie którego EIOD wydał opinię we wrześniu 2010 r.

EIDO w pełni poparł trwające prace nad oceną wszystkich instrumentów odnoszących się do zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Podkreślił fakt, że inicjatywa jest **pierwszym krokiem w procesie oceny** i wezwał do **obiektywnej, całościowej i wnikliwej oceny** wszystkich istniejących instrumentów, które mają zostać wykorzystane w ramach strategii w zakresie zarządzania informacjami, przed zaproponowaniem nowych instrumentów.

EIOD zasugerował również zgłaszanie i uwzględnianie uchybień i słabych stron systemów w przyszłej pracy nad zarządzaniem informacjami.

3.4.3. FRONTEX

W lutym 2010 r. Komisja zaproponowała **wniosek zmieniający ramy prawne regulujące FRONTEX** w celu wzmocnienia zdolności operacyjnych agencji. W opinii wydanej w maju 2010 r. EIOD skoncentrował się na coraz liczniejszych zadaniach agencji i ich konsekwencjach dla ochrony danych.

EIOD był szczególnie krytycznie nastawiony wobec faktu, że wniosek nie określał, czy i w jakim zakresie FRONTEX będzie miał prawo przetwarzać dane osobowe. EIOD wezwał również prawodawcę do określenia jasnych zasad ochrony danych oraz wyjaśnienia warunków i okoliczności, w jakich przetwarzanie danych przez FRONTEX może mieć miejsce.

Ponadto EIOD monitorował ściśle dyskusje nad tą sprawą w Parlamencie Europejskim. W piśmie skierowanym do sprawozdawcy Parlamentu Europejskiego poczynił on konkretne zalecenia mające na celu wprowadzenie **specjalnej podstawy prawnej** dla tej kwestii, która będzie przedmiotem **mocnych gwarancji ochrony danych** i będzie zgodna z zasadami proporcjonalność i konieczności.

3.4.4. Polityka zwalczania terroryzmu

Zwalczanie terroryzmu jest obszarem, gdzie dane osobowe są często przetwarzane w szeroki i prewencyjny sposób.

W swojej opinii o polityce zwalczania terroryzmu UE EIOD wezwał do **konkretnych inicjatyw** wspierających poszanowanie praw podstawowych w tym obszarze, w szczególności prawa do ochrony danych osobowych. EIOD położył nacisk na potrzebę zapewnienia **spójności** i jasnych relacji między strategiami a inicjatywami w obszarze spraw wewnętrznych i bezpieczeństwa wewnętrznego. Zalecił on również, aby prawodawca UE **zwiększył rolę ochrony danych w tym obszarze**. W szczególności **zasada konieczności** powinna znaleźć bezpośrednie odniesienie w każdym wniosku. Powinno to tym samym zapobiec ewentualnemu powielaniu istniejących instrumentów; ponadto wymiana danych osobowych powinna być ograniczona do zakresu, który jest rzeczywiście konieczny z punktu widzenia obranego celu.

Dodatkowo całościowe i globalne podejście, mające na uwadze zarówno skuteczność egzekwowania prawa, jak i poszanowanie praw podstawowych powinno być zaproponowane w odniesieniu do **środków zamrażających aktywa** skierowanych przeciwko wybranym krajom podejrzanym o terroryzm. W odniesieniu do współpracy międzynarodowej EIOD wskazał ponownie na potrzebę zapewnienia odpowiednich zabezpieczeń w przypadkach, gdy dane osobowe są wymieniane z państwami trzecimi i organizacjami międzynarodowymi, by prawo do ochrony danych obywateli w tym kontekście było odpowiednio przestrzegane.

3.4.5. Wprowadzanie do obrotu i używanie prekursorów materiałów wybuchowych

Z perspektywy ochrony danych gromadzenie danych o podejrzanych transakcjach dotyczących wybranych środków chemicznych jest najdelikatniejszą kwestią we wniosku rozporządzenia Komisji w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych. Głównym celem wniosku jest ograniczenie ryzyka ataków terrorystycznych lub innych przestępców za pomocą wytworzonych domowym sposobem urządzeń wybuchowych. EIOD wezwał do wyjaśnienia odpowiednich zapisów w celu dopilnowania, **by ochrona danych pozostała proporcjonalna i by zapobiegano nadużyciom**.

Zapewnienie wysokiego poziomu ochrony danych przyczynia się również do walki z rasizmem, ksenofobią i dyskryminacją, co z kolei może przyczyniać się do zapobiegania radykalizacji i rekrutacji do terroryzmu.

Główne zalecenia EIOD były następujące:

- **danych nie powinno się wykorzystywać do żadnego innego celu** niż zwalczanie terroryzmu (i innych przestępstw związanych z niewłaściwym używaniem substancji chemicznych do wytwarzanych domowym sposobem materiałów wybuchowych);
- **danych nie powinno się również zatrzymywać w dłuższych okresach**, szczególnie jeśli liczba potencjalnych i faktycznych odbiorców miałaby być duża lub jeśli dane miałyby być wykorzystane do eksploracji danych. Jest to szczególnie ważne w sprawach, gdzie da się

Dane osobowe powiązane z niepotwierdzonymi podejrzeniami o działalność terrorystyczną nie powinny być przechowywane bez końca.

wykazać, że wstępne podejrzenia okazały się nieuzasadnione. EIOD wezwał, aby rozporządzenie określało maksymalny okres zatrzymywania (*prima facie* nieprzekraczający dwóch lat) dla wszystkich danych osobowych odnoszących się do zgłaszanych podejrzanych transakcji;

- **przetwarzanie szczególnych kategorii danych powinno być wyraźnie zakazane**, w celu uniknięcia praktyk dyskryminujących, takich jak profilowanie na podstawie rasy lub religii.

3.4.6. Rozporządzenie Eurodac

W swojej opinii opublikowanej w grudniu 2010 r. EIOD skupił się na problemie „**niepowodzenia rejestracji**" (który w tym konkretnym kontekście oznacza brak możliwości ze strony osoby ubiegającej się o azyl podania czytelnych odcisków palców). EIOD naciskał na zasadę, aby brak możliwości rejestracji nie powodował sam z siebie odmowy praw osobie ubiegającej się o azyl. W szczególności odrzucił on zdecydowanie założenie, że osoba, która ma nieczytelne odciski palców – *ipso facto* – podjęła próbę zakłócenia procedury identyfikacji, na przykład przez samookaleczenie.

W opinii z zadowoleniem przyjęto również fakt, że możliwość przyznania **organom ścigania dostępu do EURODAC została usunięta z obecnego wniosku**.

EIOD wydał zalecenia dotyczące informowania osoby, której dane dotyczą: niepewna pozycja osób ubiegających się o azyl lub nielegalnych imigrantów jest sama w sobie uzasadnieniem dostarczenia dokładnych i pomocnych informacji o ich prawach. Opinia obejmowała również wykorzystanie najlepszych dostępnych technik jako środka wdrożenia „wbudowanej ochrony prywatności" i konsekwencji podzlecania (części) tworzenia systemu lub zarządzania nim stronom trzecim.

EIOD do tej pory wydał kilka opinii w tym obszarze. Zalecenia w tej opinii były albo oparte na nowych działaniach, albo na wcześniejszych zaleceniach, które nie zostały jeszcze wzięte pod uwagę.

3.4.7. Niegodziwe traktowanie dzieci w celach seksualnych i pornografia dziecięca

W maju 2010 r. EIOD przyjął opinię na temat wniosku Komisji dotyczącego dyrektywy w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej.

W opinii EIOD naciskał na potrzebę zapewnienia **pewności prawnej** wszystkim zaangażowanym stronom, w tym dostawcom usług internetowych, ofiarom i osobom fizycznym korzystającym z sieci.

Mimo że wniosek wspominał o potrzebie wzięcia pod uwagę praw podstawowych użytkowników końcowych, EIOD uznał, że we wniosku powinien być uwzględniony obowiązek państw członkowskich zapewnienia **zharmonizowanych, jasnych i dokładnych procedur** pod **nadzorem niezależnych organów publicznych** w przypadku walki z nielegalnymi treściami.

EIOD nie kwestionował potrzeby wprowadzenia lepszych ram zapewniających odpowiednie środki ochrony dzieci przed nadużyciami. Położył jednak nacisk na **wpływ** niektórych środków, takich jak blokowanie stron czy tworzenie linii zaufania, **na podstawowe prawa jednostek do prywatności i ochrony danych**. Zagadnienie to nie jest charakterystyczne dla walki z nadużyciami wobec dzieci, ale dla każdej inicjatywy wymagającej współpracy sektora prywatnego przy egzekwowaniu prawa.

3.4.8. Europejski nakaz ochrony i europejski nakaz dochodzeniowy

Inicjatywa licznych państw członkowskich dotycząca dyrektywy w sprawie europejskiego nakazu ochrony (EPO) i europejskiego nakazu

dochodzeniowego (EIO) ma swoje korzenie w programie sztokholmskim i zakłada wymianę danych osobowych pomiędzy odpowiednimi państwami członkowskimi. Podczas gdy celem EPO jest zwiększenie ochrony ofiar przestępstw (szczególnie kobiet), celem EIO jest stworzenie jednego, skutecznego i elastycznego instrumentu pozyskiwania dowodów zlokalizowanych w innym państwie członkowskim UE.

W swojej opinii EIOD podkreślił, że przetwarzanie danych osobowych, szczególnie w delikatnym obszarze wolności, bezpieczeństwa i sprawiedliwości, musi być zgodne z zasadami UE o ochronie danych.

Skuteczna ochrona danych osobowych jest nie tylko ważna dla osób, których dane dotyczą, ale również przyczynia się do sukcesów samej współpracy sądowej, opartej na wzajemnym uznawaniu i lepszej jakości danych w przypadkach wymiany informacji.

Wśród różnych zaleceń EIOD wezwał do wprowadzenia odpowiednich zabezpieczeń dla zapewnienia ochrony osób w odniesieniu do przetwarzania danych osobowych, sprawiedliwości proceduralnej i właściwego nadzoru przepisów dotyczących poufności i tajemnicy służbowej. W szczególności EIOD podkreślił konieczność a) dopilnowania, by systemy uwierzytelniania umożliwiały dostęp do danych osobowych wyłącznie upoważnionym osobom, 2) zapewnienia śledzenia dostępu i prowadzenia operacji i 3) zapewnienia wykonania kontroli wewnętrznych.

Opinia ta była również ważną okazją dla EIOD do podkreślenia potrzeby ustanowienia **specyficznych procedur** zapewniających **konsultację EIOD także** w przypadkach, w których inicjatywa ze strony państwa członkowskiego odnosi się do przetwarzania danych osobowych.

3.5. Prywatność w kontekście łączności elektronicznej i technologie

3.5.1. Wspieranie zaufania w społeczeństwie informacyjnym

W maju 2010 r. Komisja Europejska przyjęła agendę cyfrową, strategię zawierającą zestaw zasad i działań mających ożywić gospodarkę cyfrową do 2020 r. EIOD przyjął w marcu 2010 r. opinię w sprawie wspierania zaufania w społeczeństwie informacyjnym poprzez działanie na rzecz ochrony danych i prywatności jako wkład do tej strategii.

Opinia podkreśla, że zaufanie konsumentów jest kluczowym czynnikiem pojawiania się i udanego rozwoju technologii informacyjno-komunikacyjnych (TIK), takiej jak identyfikacja radiowa (RFID), sieci społecznościowe, e-zdrowie i e-transport i wiele innych.

Zaufanie będzie rosło jedynie wtedy, gdy TIK będą niezawodne, bezpieczne, pozostające pod kontrolą jednostek i gdy gwarantowana będzie ochrona ich danych osobowych i prywatności.

UE ma silne ramy regulujące ochronę danych, które zasadniczo powinny zapewniać ochronę danych osobowych jednostek. W wielu przypadkach TIK budzą jednak nowe wątpliwości, które nie są uwzględnione w istniejących ramach. Opinia omawia środki, które UE może podjąć lub promować w celu wzmocnienia tych ram. W szczególności EIOD wzywa Komisję Europejską do obrania następujących kierunków działań:

- włączenia zasady **„wbudowanej ochrony prywatności”** jako **ogólnej wiążącej zasady** do istniejących ram prawnych ochrony danych. Wbudowana ochrona prywatności powinna zostać w pełni zatwierdzona przez europejską agendę cyfrową i stać się wiążącą zasadą w przyszłych strategiach UE, na przykład w e-transporcie, e-administracji itp.;

- wdrożenia zasady wbudowanej ochrony prywatności zgodnie ze specjalnym podejściem w trzech **obszarach** TIK **stanowiących szczególne zagrożenie** dla prywatności i ochrony danych: a) **RFID**: zaproponowanie środków ustawodawczych regulujących główne kwestie stosowania RFID, gdyby samoistna regulacja nie zapewniała oczekiwanych wyników (np. zapewnienie zasady wyrażania zgody w punkcie sprzedaży), b) **sieci społecznościowe**: zapewnienie obowiązkowych ustawień domyślnej ochrony prywatności; c) **ukierunkowana reklama**: gdy przeglądarki mają ustawienia domyślnej ochrony prywatności w celu ułatwienia uzyskania zgody odbiorców na odbieranie reklam.

3.5.2. Internet i neutralność sieci

W czerwcu 2010 r. DG INSFO rozpoczęła konsultację społeczną na temat otwartego Internetu i neutralności sieci w Europie. Konsultacja poruszała wiele kwestii odnoszących się do strategii zarządzania ruchem, które umożliwiają operatorom sieci i dostawcom usług internetowych obsługiwanie ruchu w szczególny sposób.

W odpowiedzi na konsultację EIOD przedstawił uwagi, by zwrócić szczególną uwagę DG INFSO na kwestie ochrony danych i prywatności, które pojawiają się, gdy dostawcy usług internetowych i operatorzy sieci angażują się w działania z zakresu zarządzania ruchem.

EIOD podkreślił dwa aspekty odnoszące się do wdrażania mechanizmów zarządzania ruchem: po pierwsze, umożliwia ono dostawcom analizowanie treści wiadomości lub komunikatów, a po drugie, daje im możliwość przypisywania tych informacji do konkretnego użytkownika. EIOD podkreślił potrzebę należytego uwzględnienia ram UE regulujących ochronę danych przy podejmowaniu takich działań. W szczególności przypomniał, że ramy ochrony danych UE wymagają od użytkowników **dobrowolnej świadomej zgody** i podał praktyczne wskazówki dotyczące wymogów w zakresie uzyskiwania takiej zgody.

3.5.3. Dyrektywa w sprawie zatrzymywania danych

W trakcie konferencji zorganizowanej przez Komisję w grudniu 2010 r. EIOD wygłosił przemówienie – odnosząc się do „chwili prawdy" dla dyrektywy w sprawie zatrzymywania danych – w której wzywał do wykorzystania okazji do **wyraźnego wykazania konieczności i uzasadnienia** dyrektywy.

Dyrektywa w sprawie zatrzymywania danych prowadzi do obowiązku nakładanego na dostawców łączności elektronicznej (firmy telekomunikacyjne, dostawcy telefonii ruchomej i usług internetowych) zachowywania danych o ruchu, lokalizacji i abonentach do celów prowadzenia dochodzeń w sprawie poważnych przestępstw, ich wykrywania i ścigania.

EIOD podkreślił, że to masowe naruszenie prywatności wymaga głębokiego uzasadnienia. Dlatego EIOD wezwał Komisję Europejską do wykorzystania procesu oceny do **wykazania konieczności** dyrektywy. Konkretne fakty i liczby powinny umożliwić określenie, czy wyniki przedstawione w ocenie mogłyby zostać osiągnięte za pomocą mniej inwazyjnych środków.

Nowy lub zmieniony instrument UE w zakresie zatrzymywania danych powinien mieć wyraźny zakres i zapewniać pewność prawa dla obywateli. Oznacza to, że powinien on również regulować możliwości dostępu organów ścigania do danych i ich dalszego wykorzystania przez nie oraz pozostawić miejsce dla państw członkowskich na wykorzystanie ich do dodatkowych celów.

Orzeczenie niemieckiego Trybunału Konstytucyjnego

W dniu 2 marca 2010 r. niemiecki Trybunał Konstytucji **orzekł na niekorzyść niemieckiego prawa wdrażającego dyrektywę w sprawie zatrzymywania danych**. Niemiecki Trybunał uznał, że wykorzystanie przechowywanych danych powinno być przedmiotem bardziej rygorystycznych wymogów niż te określone przez niemieckiego ustawodawcę. W swoim orzeczeniu Trybunał przedstawił następnie kryteria bardziej ograniczonego dostępu do danych i ich wykorzystania. Kryteria te należałoby włączyć do niemieckiego ustawodawca w celu dopilnowania, by obowiązek zatrzymywania danych mógł być przestrzegany bez naruszania praw podstawowych zawartych w niemieckiej Konstytucji.

W swoim oświadczeniu dla prasy EIOD podkreślił, że orzeczenie należy postrzegać jako wiarygodne źródło inspiracji dla innych państw członkowskich UE i jako wartościowy wkład w ocenę dyrektywy w sprawie zatrzymywania danych, w szczególności w świetle nowych ram prawnych ustanowionych w traktacie lizbońskim.

3.5.4. E-odpady

Prywatność i ochrona danych są nierozłącznie związane ze środkami bezpieczeństwa odnoszącymi się do urządzeń mogących przechowywać coraz większe ilości danych osobowych. EIOD podkreślił ten aspekt w swojej opinii z kwietnia

EIOD zwrócił się do Komisji o wykazanie konieczności zatrzymywania danych z komunikacji na tak szeroką skalę.

2010 r. w sprawie wniosku Komisji zmieniającego dyrektywę w sprawie zużytego sprzętu elektrotechnicznego i elektronicznego (określanego również jako e-odpady).

Popierając cel wniosku, jakim jest poprawa przyjaznych dla środowiska strategii w dziedzinie e-odpadów, EIOD zauważa jednocześnie, że inicjatywa ta koncentruje się jedynie na środowiskowych zagrożeniach związanych z usuwaniem e-odpadów i nie uwzględnia **zagrożeń dla ochrony danych**, które mogą powstać w wyniku **niewłaściwego usuwania, ponownego użycia lub recyclingu** zużytego sprzętu elektrotechnicznego i elektronicznego.

Większe ryzyko utraty lub rozproszenia danych osobowych występuje, gdy dane osobowe odnoszące się do użytkowników urządzeń lub stron trzecich są w chwili usuwania przechowywane na urządzeniach informatycznych i telekomunikacyjnych (np. komputerach osobistych, laptopach i urządzenia łączności elektronicznej).

W obliczu takich zagrożeń EIOD podkreśla znaczenie przyjęcia właściwych **środków bezpieczeństwa** na każdym etapie przetwarzania danych osobowych, w tym na etapie usuwania urządzeń zawierających dane osobowe (od początku do końca).

Ponadto zasada „**wbudowanej ochrony danych**" oraz, w tej dziedzinie, „**wbudowanego bezpieczeństwa**" powinny zostać odpowiednio uwzględnione i włączone do wniosku w celu dopilnowania, by prywatność i gwarancje bezpieczeństwa zostały domyślnie wbudowane w urządzenia elektrotechnicznego i elektroniczne.

Dane osobowe przechowywane w elektronicznych odpadach powinny być odpowiednio chronione.

3.5.5. Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA)

W opinii opublikowanej w grudniu 2010 r. EIOD z zadowoleniem przyjął przedłużenie mandatu ENISA i poszerzenie jej obecnych zadań zgodnie z wnioskiem Komisji Europejskiej oraz podkreślił, że **bezpieczeństwo** przetwarzania **danych** jest **zasadniczym elementem ochrony danych**. W tym względzie poparł cel wniosku, jakim jest wzmocnienie kompetencji Agencji poprzez dołączenie organów **ochrony danych** i **organów ścigania** jako **pełnoprawnych stron zainteresowanych**.

EIOD zalecił większą precyzję w odniesieniu do poszerzenia zadań Agencji w celu uniknięcia niepewności prawa oraz wskazał na potrzebę utworzenia solidnych kanałów współpracy ze stronami zainteresowanymi Agencji w celu zapewnienia spójności i ścisłej współpracy.

EIOD podkreślił także potrzebę włączenia **zaleceń i najlepszych praktyk** w zakresie bezpieczeństwa do wewnętrznych operacji Agencji. To umożliwi ENISA lepsze testowanie i promowanie tych technik w innych organach i agencjach.

Nowe rozporządzenie w sprawie agencji ENISA przedłuży jej mandat o pięć lat i wzmocni jej kompetencje.

3.5.6. E-sprawiedliwość

EIOD ściśle współpracuje z zespołami Komisji i Rady zaangażowanymi w opracowanie i funkcjonowanie planu działania e-sprawiedliwość. Inicjatywa ta ma na celu zmodernizowanie i usprawnienie sposobu, w jaki społeczeństwo odbiera informacje prawne, tak by mogło ono skorzystać z „wielojęzykowego punktu kompleksowej obsługi cybernetycznej w zakresie informacji prawnych".

Strona została uruchomiona w lipcu 2009 r. z ograniczonymi funkcjami i ma zawierać więcej usług zgodnie z ambitnym planem dziania określonym przez Radę, który obejmuje między innymi następujące funkcje: usługi informacyjne, e-płatność, europejski nakaz zapłaty, drobne roszczenia, wyszukiwarka specjalistów i wyniki wyszukiwania we wzajemnie połączonych publicznych rejestrach.

Ponieważ niektóre z tych usług mogą obejmować przetwarzanie znacznej ilości danych osobowych, EIOD zaleca włączenie od początku odpowiednich **gwarancji ochrony danych** do instrumentów prawnych stanowiących podstawę prawną oraz do infrastruktury IT służącej do świadczenia usługi.

3.5.7. Siódmy program ramowy Wspólnoty Europejskiej w zakresie badań, rozwoju technologicznego i demonstracji, w tym projekt TURBINE

EIOD, zastosowując możliwe opcje interakcji wyszczególnione w swoim dokumencie strategicznym z kwietnia 2008 r. „The EDPS and EU Research and Technological Development" („EIOD a badania i rozwój technologiczny UE")[10], ułatwił kontakty i współpracę pomiędzy krajowymi organami ochrony danych a konsorcjami projektów badawczych w 2010 r.

Sprawa TURBINE[11]

W 2008 r., po przeanalizowaniu elementów projektu UE „TrUsted Revocable Biometric IdeNtitiEs" (TURBINE, „Pewne odwołalne tożsamości biometryczne"), którego celem jest prowadzenie badań z zakresu **odwołalnych danych biometrycznych**, EIOD postanowił przychylnie odpowiedzieć na wniosek konsorcjum o przedstawienie opinii w sprawie tego projektu UE[12]. EIOD z zadowoleniem przyjął silne powiązanie projektu z kwestią ochrony danych i uznał, że odzwierciedla on priorytety określone w jego rocznym sprawozdaniu.

Pomiędzy majem a październikiem 2010 r. konsorcjum projektu przekazało EIOD wszystkie właściwe dokumenty dotyczące kwestii ochrony danych

[10] Dostępny na stronie internetowej EIOD w zakładce Publications > Papers.

[11] www.turbine-project.eu

[12] Zob. sprawozdanie roczne 2008, s. 70.

badań prowadzonych w ramach projektu TURBINE. EIOD odbył również szereg dyskusji z przedstawicielami konsorcjum, szukając bardziej szczegółowych wyjaśnień i dalszych dokumentów, jeśli tego wymagała sytuacja. Demonstratory opracowane przez TURBINE i wdrożone latem 2010 r. zostały uznane za ważny element analizy. Kluczowe punkty opinii EIOD zostały przedstawione na końcowej konferencji projektu, która miała miejsce w Brukseli w styczniu 2011 r.

Siódmy program ramowy: punkt wyjścia dla zasady wbudowanej ochrony bezpieczeństwa.

3.6. Współpraca międzynarodowa i przekazywanie danych

3.6.1. Dane dotyczące przelotu pasażera

W 2010 r., tak jak w poprzednich latach, przetwarzanie danych dotyczących przelotu pasażera (PNR) przez organy ścigania wiązało się z kwestami ochrony danych postrzeganymi z perspektywy europejskiej.

W odniesieniu do **umowy z USA w sprawie PNR** EIOD powrócił do kilku obaw, które wyraził, występując przed Trybunałem Sprawiedliwości, a także w opiniach przyjętych z Grupą Roboczą Art. 29, a które nie zostały odpowiednio uwzględnione w ostatecznej wersji umowy. W szczególności EIOD podkreślił, że umowa nie koncentruje się na osobach stanowiących zagrożenie, a raczej planuje masowe gromadzenie danych osobowych i ocenę ryzyka stosowaną wobec wszystkich jednostek. Natomiast umowa w sprawie PNR z Australią budzi mniej zastrzeżeń w zakresie prywatności.

EIOD zajął również stanowisko w kwestii wniosku Komisji o określenie jej **zewnętrznej strategii w zakresie PNR**. Wniosek przedstawia ogólne zasady, w tym zestaw gwarancji ochrony danych, na których powinna być oparta każda umowa w sprawie PNR z państwem trzecim. W swojej opinii EIOD pochwalił horyzontalne podejście przyjęte przez Komisję i silnie poparł cel, jakim jest osiągnięcie wysokiego i ujednoliconego poziomu ochrony danych dla wszystkich istniejących i przewidywanych systemów PNR.

Warunki gromadzenia i przetwarzania PNR, aby były dopuszczalne, powinny jednak zostać **znacznie ograniczone**. W przypadku umowy z USA w sprawie PNR EIOD był szczególnie zaniepokojony **wykorzystaniem systemów PNR do oceny ryzyka lub profilowania**. Miał duże wątpliwości co do **konieczności i uzasadnienia** niektórych istotnych aspektów zaproponowanych systemów. W jego opinii proaktywne wykorzystanie danych PNR wszystkich pasażerów do celów oceny ryzyka wymaga bardziej bezpośredniego uzasadnienia i gwarancji.

Jeśli chodzi o treść zaproponowanych gwarancji ochrony danych, EIOD wezwał o większą precyzję w odniesieniu do **minimalnych gwarancji** mających zastosowanie do wszystkich umów w sprawie PNR. Ściślejsze warunki powinny mieć w szczególności zastosowanie do przetwarzania danych szczególnie chronionych, warunków dalszego przekazywania i zatrzymywania danych. EIOD podkreślił również konieczność zawarcia w umowie w sprawie PNR odrębnego przepisu dla jednostek o **bezpośrednio wykonywalnych prawach**.

Dane osobowe wszystkich pasażerów są wykorzystywane do oceny ryzyka. Budzi to poważne obawy co do konieczności i proporcjonalności takich operacji.

3.6.2. Program śledzenia środków finansowych należących do terrorystów

EIOD miał znaczne obawy co do projektu umowy Komisji Europejskiej ze Stanami Zjednoczonymi w sprawie **programu śledzenia środków finansowych należących do terrorystów (TFTP)**. Umowa umożliwia organom USA dostęp do danych finansowych pochodzących z Europy, zarządzanych przez belgijską firmę **SWIFT** w dochodzeniach w ramach zwalczania terroryzmu. Po decyzji Parlamentu Europejskiego o zawetowaniu umowy przejściowej w połowie lutego nowy projekt miał uwzględniać obawy dotyczące prywatności i ochrony danych.

*EIOD uznał, że **nie** przedstawiono dotąd **dostatecznych dowodów uzasadniających konieczność i proporcjonalność** takiej umowy naruszającej prywatność, która na wiele sposobów pokrywa się z istniejącymi wcześniej unijnymi i międzynarodowymi instrumentami w tym obszarze.*

EIOD podkreślił, że **konieczność** zaproponowanej umowy powinno się wykazać w sposób jednoznaczny, z uwzględnieniem innych istniejących instrumentów w mniejszym stopniu naruszających prywatność (np. porozumienie między Unią Europejską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej). EIOD wyraził szczególne obawy co do planu umożliwienia **zbiorowego przekazywania ilości danych bankowych** organom USA (masowe przekazywanie danych).

Ponadto opinia wskazywała kluczowe elementy wymagające poprawy z perspektywy ochrony danych, w tym:

- zapewnienie zastąpienia **masowego przekazywania danych** mechanizmami umożliwiającymi filtrowanie danych finansowych w UE i gwarantującymi przesyłanie organom USA wyłącznie właściwych i niezbędnych danych;
- znaczne skrócenie **okresu przechowywania** dla nieusuniętych danych, których organy nie pobrały do celów dochodzeń związanych z terroryzmem;
- powierzenie zadania oceny wniosków Departamentu Skarbu USA **publicznemu organowi sądowemu**, zgodnie z mandatem negocjacyjnym i obecnymi ramami prawnymi UE w zakresie ochrony danych;
- zapewnienie **faktycznej wykonalności praw** osób, których dane dotyczą, **z zakresu ochrony danych**, w szczególności na terytorium USA;
- poprawa mechanizmów **niezależnego nadzoru i monitorowania**.

Niektóre z tych punktów zostały uwzględnione przez Komisję Europejską, Parlament Europejski i Radę w końcowej procedurze. Nieznacznie zmieniona umowa weszła w życie w dniu 1 sierpnia 2010 r.

EIOD wyraził szczególne obawy co do planu umożliwienia przekazywania masowych ilości danych bankowych organom USA.

3.6.3. Międzynarodowa umowa pomiędzy UE a USA w sprawie wymiany informacji i ochrony danych osobowych

EIOD brał udział w dyskusjach nad projektem międzynarodowej umowy w sprawie ochrony danych pomiędzy UE a USA. Umowa ta zapewniłaby **wysokiego poziomu gwarancje**, które obowiązywałby w stosunku do wymiany danych osobowych w dziedzinie **współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych**.

Od 2007 r. EIOD ściśle przyglądał się pracy grupy kontaktowej wysokiego szczebla obejmującej przedstawicieli UE i USA i brał udział w poszczególnych etapach prac przygotowawczych. Wydał opinię w listopadzie 2008 r. i brał udział w spotkaniach i konsultacji społecznej zorganizowanej przez Komisję. W zakresie mandatu negocjacyjnego przygotowanego przez Komisję EIOD poparł włączenie podstawowych wymogów w zakresie ochrony danych do projektu, takich jak wyraźny cel i zakres zastosowania, przepisy dotyczące wykonalnych praw osób, których dane dotyczą i niezależny nadzór.

3.6.4. Umowa handlowa dotycząca zwalczania obrotu towarami podrobionymi

W ciągu całego 2010 r. Unia Europejska była zaangażowana w negocjacje prowadzone w celu sfinalizowania międzynarodowej umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA). Umowa, która została przyjęta w grudniu 2010 r., miała na celu wzmocnienie egzekwowania praw własności intelektualnej, również w Internecie.

W trakcie negocjacji, które były przedmiotem mocnej krytyki ze względu na brak przejrzystości, okazało się, że niektóre przepisy projektu umowy mogą naruszać prawa jednostek do prywatności i ochrony danych.

EIOD, z którym nie skonsultowano się w żadnym momencie w tej sprawie, był szczególnie zaniepokojony potencjalnymi przepisami ACTA uzasadniającymi ***monitorowanie użytkowników Internetu na szeroką skalę*** *oraz nałożeniem obowiązku na dostawców usług internetowych przyjęcia* ***„polityki odłączania od Internetu po trzech ostrzeżeniach”***[13]

W celu omówienia tych kwestii EIOD przyjął opinię w lutym 2010 r., zawierającą następujące zalecenia:

- **przeanalizowanie mniej inwazyjnych środków walki z piractwem w Internecie:** EIOD był zadania, że polityka odłączania Internetu po trzech ostrzeżeniach nie jest konieczna dla osiągnięcia celu, jakim jest egzekwowanie praw własności intelektualnej. Zwrócił się o rozważnie mniej inwazyjnych rozwiązań lub przynajmniej ograniczenie zakresu rozważanego monitorowania i rozważenie ukierunkowanego doraźnego monitorowania;

- **zastosowanie odpowiednich gwarancji do wszystkich operacji przekazywania danych w kontekście ACTA:** ponieważ ACTA wiąże się z międzynarodową wymianą danych osobowych pomiędzy organami lub prywatnymi organizacjami z siedzibą w państwach-sygnatariuszach, EIOD wzywa UE do wdrożenia odpowiednich gwarancji w stosunku do wszystkich operacji przekazywania danych w kontekście ACTA. Takie gwarancje powinny przyjąć formę wiążących umów pomiędzy nadawcami z UE a odbiorcami z państw trzecich.

[13] Polityka ta zazwyczaj wiązałaby się z odłączeniem dostępu do Internetu po wcześniejszych ostrzeżeniach o domniemanej niezgodnej z prawem wymianie lub pobieraniu materiału chronionego prawami autorskimi.

EIOD był szczególnie zaniepokojony ewentualnymi postanowieniami umowy ACTA dającymi prawo do monitorowania użytkowników Internetu na szeroka skalę.

3.7. Podatki i cła

3.7.1 Współpraca w dziedzinie opodatkowania

Pierwsza opinia EIOD z 2010 r. dotyczyła wniosku Komisji mającego wzmocnić administracyjną współpracę pomiędzy państwami członkowskimi w dziedzinie opodatkowania. Wniosek dotyczył podatków pośrednich, ale nie obejmował podatku VAT i podatku akcyzowego, o których mowa w innych instrumentach prawnych.

Jednym z głównych celów wniosku było udoskonalenie wymiany informacji pomiędzy państwami członkowskimi. W większości przypadków dotyczyło to informacji o osobach fizycznych. Zasady ochrony danych miały więc zastosowanie.

W swojej opinii, opublikowanej w styczniu 2010 r., EIOD stwierdził, że wniosek Komisji był typowym przykładem **braku świadomości ochrony danych**, kwestia ta została bowiem niemal całkowicie w nim pominięta. W konsekwencji wniosek zawierał kilka elementów niezgodnych z wymogami z zakresu ochrony danych. W opinii podkreślono i omówiono te uchybienia.

EIOD wezwał prawodawcę między innymi do bardziej precyzyjnego określenia odpowiedzialności Komisji za **utrzymanie i bezpieczeństwo** sieci, której zamierzano użyć do wymiany informacji. Zwrócił się także do prawodawcy o uściślenie, jaki rodzaj danych osobowych można wymieniać, dokładniejsze określenie celów, w jakich można wymieniać dane osobowe, oraz dokonanie oceny konieczności takiego przekazania danych lub przynajmniej zapewnienie przestrzegania zasady konieczności.

3.7.2. Wspólny Komitet Współpracy Celnej UE-Japonia

W lutym 2010 r. Komisja przyjęła wniosek dotyczący decyzji Rady w sprawie stanowiska Unii w ramach Wspólnego Komitetu Współpracy Celnej UE-Japonia dotyczącego wzajemnego uznawania programów upoważnionego przedsiębiorcy w Unii Europejskiej i w Japonii[14]. Artykuł IV załącznika do wniosku dotyczy **wymiany informacji i komunikacji**. Znajduje się w nim zapis, że informacje i związane z nimi dane, w szczególności dotyczące podmiotów objętych programem, wymieniane są w sposób systematyczny w formie elektronicznej.

Zarówno dyrektywa 95/46/WE, jak i rozporządzenie (WE) 45/2001 zawiera analogiczne przepisy, odpowiednio w art. 25–26 i art. 9, w odniesieniu do transgranicznych przepływów danych osobowych. Zasada tam ustanowiona zakłada, że **dane osobowe nie mogą być przekazywane** z państwa członkowskiego do państwa trzeciego, chyba że państwo trzecie zapewni **odpowiedni poziom ochrony** (lub zostaną przyjęte odpowiednie gwarancje albo zastosowanie będzie miał jeden z przewidzianych wyjątków).

Mimo projektu uzasadnienia wniosku, które stwierdza, że japoński system ochrony danych jest odpowiedni, nie została zastosowana procedura ustalania, że państwo trzecie zapewnia odpowiedni poziom ochrony, określona w dyrektywie. W konsekwencji stwierdzenie w projekcie uzasadnienia stanowiło naruszenie dyrektywy.

EIOD zaleca więc usunięcie stwierdzenia o odpowiednim poziomie ochrony japońskiego systemu, które znajduje się w pkt 5.1 projektu uzasadnienia, ponieważ stwierdzenie to jest niezgodne z wymogami rozporządzenia (WE) 45/2001 i dyrektywy 95/46/WE. EIOD ponadto zalecił rozważenie różnych możliwości oferowanych przez rozporządzenie i dyrektywę w celu zapewnienia przestrzegania przepisów dotyczących międzynarodowych operacji przekazywania danych.

3.8. Dostęp publiczny, łącznie ze sprawami Trybunału

3.8.1. Publiczny dostęp do dokumentów zawierających dane osobowe

Od początku swojej działalności EIOD stale spotykał się z niekiedy skomplikowaną relacją pomiędzy unijnymi przepisami dotyczącymi **publicznego dostępu do dokumentów** a unijnymi przepisami w zakresie **ochrony danych**. EIOD po raz pierwszy zmierzył się z tą kwestią, wydając wytyczne dla instytucji UE. Dla przykładu, w 2005 r., EIOD opublikował dokument bazowy dotyczący tej kwestii zatytułowany „Public access to documents and data protection" („Dostęp publiczny do dokumentów a ochrona danych"), który zawierał wytyczne dla instytucji i organów UE.

[14] COM(2010)55 wersja ostateczna.

EIOD bronił także swojego podejścia jako interwenient w głównej sprawie Trybunału dotyczącej tej kwestii: *Bavarian Lager przeciwko Komisji*. W tej sprawie poproszono o publiczny dostęp do protokołu posiedzenia Komisji, wraz z nazwiskami uczestników. Odmówiono dostępu do tych nazwisk, powołując się na zasady ochrony danych. Sąd zgodził się ze stanowiskiem bronionym przez EIOD, jednak Trybunał Sprawiedliwości w ramach odwołania, w swoim wyroku z dnia 29 czerwca 2010 r., uchylił decyzję Sądu i nadał inną wykładnię mającym zastosowanie przepisom unijnym.

Część analizy przedstawionej w dokumencie bazowym z 2005 r. nie ma odtąd zastosowania w świetle wyroku Trybunału. EIOD przygotował zatem krótki dodatkowy dokument na ten temat, który został ukończony i opublikowany na początku 2011 r.

W tym dodatkowym dokumencie EIOD podkreślił konieczność **proaktywnego podejścia** w tej sprawie. W skrócie rzecz ujmując, oznacza to, że instytucje powinny wyraźnie informować osoby, których dane dotyczą – przed lub przynajmniej w chwili gromadzenia ich danych osobowych – o zakresie, w jakim przetwarzanie takich danych obejmuje lub może obejmować publicznie ujawnienie. EIOD uznał, że instytucje są zobowiązane są do tego w ramach dobrej praktyki.

Proaktywne podejście ogranicza liczbę sytuacji, w których instytucje muszą decydować o publicznym ujawnieniu na wniosek o publiczne udostępnienie danych, tak jak w sprawie Bavarian Lager. Dokument radzi, jak uzyskać właściwą równowagę w sytuacjach, w których należy wykazać inicjatywę i sytuacjach, w których należy reagować.

Kilka toczących się spraw przed Trybunałem zawieszono w oczekiwaniu na wyrok w sprawie Bavarian Lager. Wszystkie te sprawy zostały ponownie rozpatrzone po wyroku Trybunału w czerwcu 2010 r. EIOD był interwenientem w kilku tych sprawach. W stosownych przypadkach EIOD skorzystał z możliwości przedstawienia swoich poglądów na temat zastosowania wyroku Trybunału w sprawie *Bavarian Lager* do tych innych sytuacji. EIOD przedstawił także swoje stanowisko w nowo wszczętej sprawie w tej dziedzinie.

Wyrok w sprawie Bavarian Lager spowodował również, że pierwsza sprawa złożona przeciwko EIOD do Sądu została oddalona.

3.8.2. Inne sprawy sądowe

Inny wyrok z udziałem EIOD został wydany przez Sąd do spraw Służby Publicznej w dniu 15 czerwca 2010 r. w sprawie *Pachtitis przeciwko Komisji*. Jedną z kwestii poruszanych w tej sprawie była odmowa Komisji udostępnienia skarżącemu pytań z testu kwalifikacyjnego, w którym uczestniczył. Ponieważ powołano się tutaj na zasady ochrony danych, a sprawa poruszała interesującą kwestię zakresu prawa dostępu do danych osobowych określonej osoby, EIOD postanowił zająć stanowisko. Opowiedział się po stronie skarżącego. Skarżący wygrał sprawę, ale kwestia ochrony danych nie została rozwiązana. Z tego powodu EIOD wycofał się z późniejszego odwołania złożonego przez Komisję do Sądu.

W lipcu 2010 r. Sąd do spraw Służby Publicznej zwrócił się do EIOD o udział w charakterze interwenienta w sprawie, która dotyczyła przekazywania danych medycznych między dwiema instytucjami UE. Po raz pierwszy EIOD został wezwany przez Sąd do udziału w sprawie. EIDO przyjął zaproszenie i przygotował uwagi interwenienta, w których wyjaśnił obowiązujące przepisy rozporządzenia o ochronie danych.

3.9. Różne inne kwestie

3.9.1. System wymiany informacji na rynku wewnętrznym

W lipcu 2010 r. EIOD zwrócił się z pismem do Dyrekcji Generalnej ds. Rynku Wewnętrznego i Usług (DG MARKT), w którym podsumował, co zostało osiągnięte i jakie dalsze postępy są konieczne w zakresie kwestii poruszonych w sprawozdaniu Komisji w sprawie stanu ochrony danych w Systemie Wymiany Informacji na Rynku Wewnętrznym (IMI).

IMI to aplikacja on-line, która umożliwia państwom członkowskim wzajemną współpracę mającą na celu poprawę wdrażania przepisów rynku wewnętrznego. Odnosi się to również do rejestrowania i wymiany właściwych danych osobowych. IMI umożliwia w szczególności krajowym, regionalnym i lokalnym organom w państwach członkowskich UE szybką i łatwą komunikację z ich odpowiednikami w innych europejskich krajach, IMI pomaga odnaleźć użytkownikom odpowiedni organ, z którym należy się skontaktować i skomunikować w innym kraju za pomocą wcześniej przetłumaczonych standardowych pytań i odpowiedzi. IMI zaprojektowano jako elastyczny system, który

można wykorzystać do wielu podzbiorów przepisów jednolitego rynku.

EIOD z zadowoleniem przyjął dotąd poczynione postępy i zachęcił Komisję do wdrażania **dalszych gwarancji**, poprzez zastosowanie zasad **wbudowanej ochrony prywatności**, i w stosownych przypadkach – do kontynuowania współpracy z organami ochrony danych w państwach członkowskich. Co ważniejsze EIOD wezwał Komisję do przyjęcia nowego instrumentu prawnego, najlepiej w ramach zwykłej procedury ustawodawczej, w celu ustanowienia pełniejszych ram ochrony danych dla IMI oraz zapewnienia pewności prawa i wyższego poziomu ochrony danych.

IMI czeka rozbudowa, potrzebna jest zatem silna podstawa prawna i szczegółowe gwarancje ochrony danych.

3.9.2. Skanery ciała

W lutym 2010 r. przedstawiciel EIOD wziął udział w próbie zastosowania skanera ciała wprowadzonego w porcie lotniczym Schiphol w Holandii. Celem wizyty było uzyskanie dodatkowych informacji na temat tzw. „drugiej generacji systemów", której celem jest poprawa ochrony danych i wdrożenie zasady „wbudowanej ochrony prywatności".

W lipcu 2010 r. EIDO wydał uwagi[15] do komunikatu w sprawie użytkowania skanerów ciała w portach lotniczych, przyjętego przez Komisję w czerwcu[16].

W tych uwagach EIOD podkreślił, że **zgoda nie** powinna być wykorzystywana jako uzasadnienie przetwarzania danych osobowych, jeśli brak podstawy prawnej do takiego przetwarzania.

Podkreślił także, że w przypadku skanerów ciała „**najlepsza dostępna technika**" oznaczałyby najwydajniejszy i najbardziej zaawansowany etap

Od skanera ciała do skanera bezpieczeństwa, rozwiązaniem jest wbudowana ochrona prywatności.

rozwoju technologii oraz metody ich stosowania, który wskazuje na praktyczną przydatność poszczególnych technik z punktu widzenia zdefiniowanej granicy wykrywalności, zgodnie z unijnymi ramami ochrony prywatności i danych.

EIOD nadal będzie ściśle obserwował prawodawcze i techniczne postępy w zakresie skanerów ciała i odpowiednio zareaguje na dalsze kroki, które Komisja Europejska zamierza powziąć.

3.9.3. Systemy gwarantowania depozytów

Systemy gwarantowania depozytów zwracają depozyty deponentom do kwoty 100 000 EUR w razie bankructwa instytucji kredytowej. Europejskie przepisy dotyczące takich systemów istnieją od 1994 r. Tuż po wystąpieniu kryzysu finansowego w 2008 r. instrument ten został wzmocniony.

[15] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-07-01_Security_scanners_EN.pdf

[16] Komunikat COM (2010) 311 wersja ostateczna

W lipcu 2010 r. Komisja przedstawiła kolejny wniosek mający na celu uproszczenie i ujednolicenie właściwych przepisów krajowych w tym zakresie.

Zwrot depozytów w ramach takich systemów gwarantowania depozytów wymaga przetwarzania danych deponentów. Zasady ochrony danych mają zatem zastosowanie, o ile deponenci ci są osobami fizycznymi. Dane są wymieniane pomiędzy instytucją kredytową a systemem gwarantowania depozytów, a także pomiędzy samymi systemami gwarantowania depozytów, zarówno w obrębie danego państwa członkowskiego, jak i pomiędzy poszczególnymi państwami członkowskimi.

EIOD wydał we wrześniu 2010 r. krótką opinię w sprawie tego wniosku, w której stwierdzał, że zasadniczo był zadowolony ze sposobu, w jaki aspekty ochrony danych zostały uwzględnione we wniosku. Wniosek dopilnowuje na przykład, by właściwe dane osobowe były wykorzystywane wyłączenie do celów, dla których były wymieniane, tj. w celu zwrotu depozytów.

EIOD ze szczególnym zadowoleniem przyjmuje fakt, że dane mogą być wykorzystywane wyłącznie w anonimowym formacie do przeprowadzania tzw. „testów warunków skrajnych". Na etapie opracowywania wniosku EIOD kwestionował bowiem konieczność korzystania z danych osobowych przy przeprowadzaniu takich testów.

3.9.4. Inicjatywa obywatelska

Inicjatywa obywatelska jest jedną z innowacji wprowadzonych w traktacie lizbońskim. Umożliwia ona minimum milionowi obywateli UE, którzy są obywatelami znaczącej liczby państw członkowskich, zwrócenia się do Komisji o przedłożenie wniosku ustawodawczego na interesujący ich temat. Zebranie co najmniej miliona głosów poparcia wiąże się z gromadzeniem danych osobowych.

W swojej opinii z kwietnia 2010 r. EIOD podkreślił, że pełne poszanowanie zasad ochrony danych znacznie przyczyni się do wiarygodności, mocy i powodzenia tego ważnego nowego instrumentu.

Jedno z zalecenie dotyczyło obowiązku organizatora inicjatywy, który zamierza wykorzystać system gromadzenia głosów on-line, zwrócenia się do właściwego organu o potwierdzenie bezpieczeństwa takiego systemu. Jeśli chodzi o czas składania takiego wniosku, EIOD zasugerował zobowiązanie organizatorów do złożenia go przed rozpoczęciem zebrania głosów poparcia, a nie po zebraniu ich. EIOD również zasugerował, by prawodawca dopilnował, by:

- dane osobowe gromadzone przez organizatora nie mogły zostać użyte do żadnego innego celu niż wskazane poparcie dla danej inicjatywy obywatelskiej;
- dane otrzymane przez właściwy organ mogły zostać wykorzystane wyłączenie do celu weryfikacji autentyczność głosów poparcia dla danej inicjatywy obywatelskiej.

3.9.5. Badanie wypadków i incydentów w lotnictwie cywilnym oraz zapobieganie im

Opinia EIOD koncentrowała się na tych aspektach wniosku, które mają wpływ na ochronę danych osobowych, w szczególności **przetwarzanie danych z list pasażerów, danych dotyczących ofiar, ich rodzin i świadków**, podczas różnych etapów badania oraz w kontekście wymiany informacji między organami ds. badania wypadków i incydentów w lotnictwie.

EIOD z zadowoleniem przyjął fakt, że aspekty ochrony danych zostały uwzględnione we wniosku. Jednakże, biorąc pod uwagę **szczególny kontekst** przetwarzania danych osobowych – badanie wypadków w celu zwiększenia bezpieczeństwa lotnictwa – **należy wprowadzić większe gwarancje w celu zapewnienia poufności danych**. Powinno to obejmować przepisy wymagające niezwłocznego usuwania lub anonimizacji danych osobowych, gdy przestają one być potrzebne do celów badania zdarzeń.

W opinii EIOD bardziej kategoryczne gwarancje są niezbędne dla ochrony jednostek, które doświadczają bezpośrednio lub pośrednio poważnego wypadku lub utraty krewnych.

Zalecenia EIOD obejmują m. in.:

- co do zasady zachowanie poufności list pasażerów przy jednoczesnym oferowaniu państwom członkowskim możliwości podjęcia innej decyzji w poszczególnych sprawach i na uzasadnionej podstawie, w tym za zgodą krewnych;

- wyznaczenie ograniczonego okresu przechowywania danych osobowych;

- uzależnienie przekazania danych osobowych państwom trzecim od tego, czy zapewniają one właściwy poziom ochrony;

- uściślenie roli i zakresu obowiązków Komisji Europejskiej i Europejskiej Agencji Bezpieczeństwa Lotniczego w zakresie stosowania przepisów dotyczących ochrony danych.

3.10. Spojrzenie w przyszłość

3.10.1. Postęp techniczny

Już w poprzednich sprawozdaniach rocznych[17] EIOD podkreślał **coraz większą zbieżność** w **społeczeństwie informacyjnym** pomiędzy „**światem realnym**" a „światem internetowym/cyfrowym". W konsekwencji rozróżnienie pomiędzy światem fizycznym a cyfrowym zaczęło się zacierać. W 2010 r. tendencja ta przyspieszyła, zbieżność była bowiem zwiększana przez nowe, innowacyjne narzędzia wprowadzane na szeroką skalę. Jak dotąd jednostki mogły żyć w równoległych światach, w których były w stanie odseparować wirtualnych siebie od swoich realnych wersji. Staje się to coraz mniej możliwie i czy tego chcemy, czy nie, jednostka wchodzi w ciągłe środowisko obejmujące świat elektroniczny i rzeczywisty, ale światy te są nadal przedmiotem innych ram regulacyjnych.

Tendencja ta urzeczywistniła się w szczególności w postaci **sieci społecznościowych**, które ciągle się rozwijają. Świat wydaje obecnie ponad 110 miliardów minut rocznie przy ich użyciu[18] i po raz pierwszy strona sieci społecznościowe stała się najczęściej odwiedzaną stroną w USA[19], wyprzedzając wyszukiwarki.

Następujące zmiany jeszcze mocniej przyspieszyły to zjawisko:

- **Urządzenia mobilne typu smart**[20] stanowią jeden z głównych filarów nowych pomostów pomiędzy fizycznym a cyfrowym światem. Są one zawsze włączone, wszechobecne i gotowe do wymiany, zmiany i przetwarzania informacji w czasie rzeczywistym. Ich moc przetwarzania danych jest imponująca i mogą je wprowadzać do niemal nieograniczonej infrastruktury, jaka jest dostępna w modelu przetwarzania zwanym „chmurą". Są w stanie rejestrować obrazy i filmy wysokiej rozdzielczości, indywidualnie oznaczać przedmioty i jednostki oraz linkować geograficzne współrzędne do materiału multimedialnego obejmującego miejsca, zdarzenia i ludzi. Użytkownicy są stale podłączeni do sieci, przy tym przetwarzają oni dane osobowe lub ich dane są przetwarzane.

- **Technologia rozpoznawania twarzy**, która również dotąd ograniczała się do mocno kontrolowanych środowisk, przeżywa nowy rozkwit i zaczyna być wykorzystywana w sieciach społecznościowych i smartfonach. Kombinacja ślepej siły milionów użytkowników sieci społecznościowej „uzbrojonych" w urządzenia mobilne typu smart, za pomocą których zamieszczają oni zdjęcia, na których oznaczają twarze jednostek, gwałtowanie rozszerza zakres technologii rozpoznawania twarzy i nawet przyczynia się do jej udoskonalania. Ten nowo powstały trend może również umożliwić utworzenie bezprecedensowej olbrzymiej biometrycznej bazy danych z platform sieci społecznościowej.

Pojęcie **poszerzonej rzeczywistości**, rozwijanej przez takie platformy jak smartfony, umożliwi wprowadzenie dodatkowych informacji on-line do rzeczywistości danej jednostki. Już teraz można odwiedzić miasto lub uzyskać dodatkowe informacje o zabytkach, które są „zidentyfikowane" przez urządzenia mobilne typu smart. Łącząc to z rozpoznawaniem twarzy i sieciami społecznościowymi, jak opisano powyżej, w niedalekiej przyszłości będzie możliwe zrobienie zdjęcia komuś na ulicy i uzyskanie szczegółowych informacji o tej osobie w czasie rzeczywistym.

W przyszłości „**technologia do ubrania"** będzie również stanowić pomost sprzyjający łączeniu fizycznego codziennego życia jednostki z cyfrowymi obrazami, które niekonieczne podlegają regulacjom w tych samych ramach. Będzie łączyć dane szczególnie chronione osób (temperatura, ciśnienie krwi, praca serca, poziom cukru itp.) z aplikacjami i usługami on-line.

Te ciągłe, nierozerwalnie związane światy otwierają niespotykane dotąd możliwości dla

[17] Sprawozdanie roczne 2007, s. 56 i sprawozdanie roczne 2009, s. 64.

[18] http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/#

[19] http://www.hitwise.com/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/

[20] http://www.enisa.europa.eu/media/news-pictures/smartphones-video-clip

obywateli, przedsiębiorców i polityków, jednocześnie niosąc ze sobą **niespotykane dotąd zagrożenia**, którym należy odpowiednio stawić czoła. W szczególności **kradzież tożsamości w wirtualnym świecie** będzie wkrótce mieć podobne skutki jak kradzież tożsamości w realnym świecie. W świetle powyższych rozważań dostępność masowych ilości danych osobowych w sieci, niezwracanie uwagi na naruszenia danych osobowych (z których wiele ma miejsce bez naszej świadomości) oraz większa dostępność usług handlowych, rządowych i społecznych, do których wirtualne tożsamości dają dostęp w świecie on-line, potencjalnie stanowią niebezpieczną mieszankę. Tradycyjne tożsamości oparte na papierze nie stanowią odtąd satysfakcjonującego rozwiązania w postaci wsparcia/potwierdzenia, gdy tożsamość elektroniczna zostaje także naruszona, ponieważ obie te tożsamości są coraz mocniej ze sobą powiązane.

Mimo zacierania granic pomiędzy światem wirtualnym a realnym zasady mające zastosowanie w tych światach nie są podobne. Weźmy na przykład inteligentne opomiarowanie: produkcja, wprowadzanie do obrotu i korzystanie z elektrycznego opomiarowania jest przedmiotem szeregu szczegółowych zasad chroniących konsumenta, ale gdy tylko to samo opomiarowanie jest podłączone do sieci i zaczyna opisywać czyjeś zachowanie, stając się tym samym inteligentnym opomiarowaniem – na przykład poprzez zapisywanie i przechowywanie informacji, o której godzinie dana osoba zużywa energię elektryczną, można by wiedzieć czy jest ona w domu, czy nie – zasady te nie mogą mieć już zastosowania. **Przegląd ram ochrony danych** może być odpowiednim momentem na uwzględnienie tych kwestii. Ramy prawne musza przyczyniać się do wdrażania niezbędnych gwarancji, których obywatele oczekują w tym nowym środowisku wymagającym dogłębnej analizy.

3.10.2. Priorytety na 2011 r.

W grudniu 2010 r. EIOD opublikował swój piąty publiczny spis jako doradca ds. wniosków do prawodawstwa UE, określając swoje priorytety w zakresie konsultacji na przyszły rok. Jak w poprzednich latach EIOD stara się wydawać opinię na temat wszystkich wniosków ustawodawczych, które mają zasadnicze znaczenie dla ochrony danych. Może również przyglądać się środkom o charakterze nieustawodawczym, jeśli odnoszą się one do zasadniczych kwestii ochrony danych.

Oto główne priorytety EIOD, które można odnaleźć w jego spisie:

- ***Przegląd ram prawnych dotyczących ochrony danych**, który będzie jednym ze ścisłych priorytetów EIOD w 2011 r.*
- *Różne inicjatywy odnoszące się do dalszego **wdrażania programu sztokholmskiego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości**, takie jak ustanowienie systemu wjazdu/wyjazdu i program rejestrowania podróżnych, zaproponowana dyrektywa w sprawie wykorzystania danych PNR do celów egzekwowania prawa i wprowadzenie europejskiego TFTP. EIOD będzie także dokładnie przyglądał się negocjacjom umów w sprawie ochrony danych z państwami trzecimi. I ostatni priorytet, choć nie mniej ważny: EIOD będzie aktywnie uczestniczył w przeglądzie dyrektywy w sprawie zatrzymywania danych.*
- ***Inicjatywy w dziedzinie technologii**, które mogą mieć wpływ na prywatność i ochronę danych, będą starannie obserwowane. EIOD będzie nadal monitorował dalsze wdrażanie **agendy cyfrowej** dla Europy.*
- ***Wszystkie inne inicjatywy**, które mogą znacząco wpływać na ochronę danych, takie jak inicjatywy w dziedzinie **transportu** (np. wykorzystanie skanerów ciała w portach lotniczych, pakiety dotyczące e-mobilności) oraz wielkoskalowa wymiana danych, która może mieć miejsce w **systemie wymiany informacji na rynku wewnętrznym**.*

4 WSPÓŁPRACA

4.1. Grupa Robocza Art. 29

Grupę Roboczą Art. 29 powołano na mocy art. 29 dyrektywy o ochronie danych (95/46/WE) jako niezależne ciało doradcze. Zapewnia ona Komisji Europejskiej niezależne doradztwo w kwestiach ochrony danych i przyczynia się do tworzenia ujednoliconych zasad ochrony danych w państwach członkowskich UE[21].

Jej zadania zostały określone w art. 30 dyrektywy i można je podsumować w następujący sposób:

- przekazywanie opinii eksperckich w sprawach dotyczących ochrony danych z państw członkowskiego członkowskich do Komisji Europejskiej;
- wspieranie jednolitego stosowania ogólnych zasad dyrektywy we wszystkich państwach członkowskich poprzez współpracę pomiędzy organami nadzoru ochrony danych.
- doradztwo na rzecz Komisji w zakresie środków odnoszących się do praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych;
- opracowanie zaleceń dla ogółu społeczeństwa, a w szczególności dla instytucji UE, na temat kwestii odnoszących się do ochrony osób w zakresie przetwarzania danych osobowych w UE.

EIOD jest członkiem Grupy Roboczej Art. 29 od początku 2004 r. i uznaje ją za bardzo ważną platformę współpracy z krajowymi organami nadzorczymi. Oczywiste jest również, że Grupa Robocza powinna odgrywać centralną rolę w spójnym stosowaniu dyrektywy i nadawaniu wykładni jej ogólnym zasadom.

W 2010 r. Grupa Robocza skupiła swoją działalność na czterech głównych strategicznych zagadnieniach określonych w jej programie prac na lata 2010–2011, mianowicie:

- wdrożenie dyrektywy i przygotowanie przyszłych całościowych ram prawnych;
- zmierzenie się z globalizacją;
- reakcja na wyzwania technologiczne;
- zwiększenie skuteczności Grupy Roboczej i organów ochrony danych.

W tym celu Grupa Robocza przyjęła wiele dokumentów, w tym:

- opinię 2/2010 w sprawie **internetowej reklamy behawioralnej** (WP 171);

[21] Grupa Robocza składa się z przedstawicieli krajowych organów nadzorczych w poszczególnych państwach członkowskich, przedstawiciela organu ustanowionego dla instytucji i organów UE (tj. EIOD) oraz przedstawiciela Komisji. Komisja obsługuje również Sekretariat Grupy Roboczej. Krajowe organy nadzorcze Islandii, Norwegii i Liechtensteinu (jako partnerzy w ramach EOG) są reprezentowane w roli obserwatorów.

- opinię 5/2010 na temat propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w **zastosowaniach RFID** (WP 175);

- opinię 7/2010 dotycząca komunikatu Komisji w sprawie **globalnego podejścia do przekazywania danych dotyczących przelotu pasażera** (PNR) państwom trzecim (WP 178).

Grupa Robocza i EIOD ściśle współpracowały przy kwestiach odnoszących się do wdrażania dyrektywy 95/46/WE i wykładni niektórych jej kluczowych przepisów. EIOD aktywnie działał w wielu obszarach, na przykład:

- opinia 1/2010 w sprawie pojęć **„administrator danych" i „przetwarzający"** (WP 169);

- opinia 3/2010 **w sprawie zasady rozliczalności** (WP 173);

- opinia 8/2010 w sprawie **prawa właściwego** (WP 179).

EIOD współpracował również z krajowymi organami nadzorczymi w stopniu koniecznym dla wykonywania ich obowiązków, w szczególności poprzez wymianę wszystkich użytecznych informacji i wnioskowanie o wsparcie lub udzielanie wsparcia przy wykonywaniu ich zadań (art. 46 lit. f) ppkt i) rozporządzenia). Współpraca ta jest nawiązywana dla indywidualnych przypadków.

Bezpośrednia współpraca z krajowymi organami jest coraz ważniejszym elementem w kontekście powstawania wielkich międzynarodowych systemów, takich jak Eurodac, które wymagają skoordynowanego podejścia do nadzoru (zob. pkt 4.2 i 4.3).

4.2. Skoordynowany nadzór nad systemem Eurodac

Skuteczny nadzór nad systemem Eurodac opiera się na ścisłej współpracy pomiędzy krajowymi organami ochrony danych a EIOD.

Złożona z przedstawicieli krajowych organów ochrony danych oraz EIOD Grupa ds. Koordynowania Nadzoru nad Systemem Eurodac opiera swoją działalność na programie prac na lata 2010–2011 przyjętym na początku 2010 r.

Ten program prac porusza szereg kwestii, skupiając się na wspólnych lub delikatnych zagadnieniach, do których grupa może coś wnieść lub w których może coś zmienić. Kilka działań zależy jednak od przyjęcia nowych rozporządzeń Eurodac/Dublin. Zostaną one wdrożone w najbardziej odpowiednim momencie.

Działania grupy są obecnie zorganizowane zgodnie z harmonogramem, który umożliwia lepsze planowanie perspektywiczne. Praca na nadchodzące lata jest podzielona na działania, które mają zostać wykonane:

- co cztery lata: np. pełny audyt bezpieczeństwa ma zostać przeprowadzony przez organy ochrony danych na poziomie krajowym i unijnym; skoordynowane przez grupę przygotowania do tej kontroli pozwolą na większą wydajność i bardziej porównywalne wyniki;

- co dwa lata: np. skoordynowane kontrole. Wiąże się to z określeniem i wykonaniem skoordynowanych kontroli w równych odstępach czasu;

- co roku: krótsze rozpoznawcze działania, o mniejszym zasięgu niż skoordynowane kontrole, będą prowadzone odpowiednio do potrzeb zidentyfikowanych przez grupę;

- na co dzień: obejmuje to głównie działania następcze, które są niezbędne na poziomie strukturalnym, takie jak monitorowanie postępów w zakresie przepisów i polityki, specjalnych przeszukiwań i wcześniejszych zaleceń.

W obrębie tych kategorii wybrano kilka rodzajów działań i rozpoczęto je w 2010 r.

Grupa odbyła trzy posiedzenia w Brukseli w marcu, październiku i grudniu 2010 r. W trakcie marcowego posiedzenia grupa ponownie wybrała Petera Hustinksa (EIOD) na przewodniczącego i po raz pierwszy Elisabeth Wallin (ze szwedzkiego organu ochrony danych) na wiceprzewodniczącą.

Grupa rozpoczęła prace **nad przygotowaniami do pełnego audytu bezpieczeństwa**. Wybrano podgrupę i rozpoczęto prace nad określeniem głównych zadań, takich jak opracowanie wykazu celów bezpieczeństwa. Pracuje ona również nad wyzwaniami, jakie wiążą się z zapotrzebowaniem na porównywalne wyniki. Prace będą kontynuowane w 2011 r.

Nową skoordynowaną kontrolę rozpoczęto pod koniec 2010 r. Grupa wybrała kwestię wcześniejszego usuwania danych oraz omówiła kwestionariusz i metodologię. Wyników można spodziewać się w 2011 r. Zagadnienie wcześniejszego usuwania danych uznano za ważne w świetle jego wpływu na jakość danych w Eurodac i ochronę osób, które nie powinny być już zgłaszane do bazy danych.

Interakcja pomiędzy stronami zainteresowanymi została z powodzeniem rozpoczęta w trakcie grudniowego posiedzenia, w którym uczestniczyli przedstawiciele Wysokiego Komisarza Narodów Zjednoczonych ds. Uchodźców i Europejskiej Rady ds. Uchodźców i Wypędzonych. Zewnętrzne strony zainteresowane przedstawiły swoje prace i priorytety oraz wymieniły poglądy z grupą na temat takich kwestii, jaki przyszłość systemu dublińskiego, informacje, jakie należy przedstawił osobom ubiegającym się o azyl lub obrona ich praw. Strony zainteresowane wyjaśniły także swoje zastrzeżenia co do możliwości udostępnienia Eurodac organom ścigania. Ta wymiana poglądów okazała się niezwykle przydatna i należałoby ją regularnie powtarzać.

4.3. Nadzór nad systemem informacji celnej (CIS)

Celem systemu informacji celnej (CIS) jest stworzenie **systemu ostrzegania** w ramach **zwalczania nadużyć finansowych**, by umożliwić państwu członkowskiemu wprowadzającemu dane do systemu zwrócenie się do innego państwa członkowskiego o obserwację i wprowadzanie zgłoszeń, niejawny nadzór, kontrolę szczególną lub operacyjną i strategiczną analizę.

CIS przechowuje informacje na temat masowych towarów, środków transportu, osób i przedsiębiorstw oraz zatrzymanych, zajętych lub skonfiskowanych towarów i środków pieniężnych w celu wspierania działań z zakresu zapobiegania działaniom, które naruszają przepisy celne i rolnicze (wcześniej „pierwszy filar" UE"), lub poważnym naruszeniom przepisów krajowych (wcześniej „trzeci filar" UE), prowadzenia dochodzeń w ich sprawie i ich ścigania. Ostatnią część nadzoruje wspólny organ nadzorczy, w skład którego wchodzą przedstawiciele krajowych organów ochrony danych.

Skoordynowany nadzór nad systemem Eurodac jest kluczowy dla ochrony praw słabszych grup, takich jak osoby ubiegające się o azyl.

Grupę ds. Koordynowania Nadzoru nad Systemem SIC utworzono jako platformę, w ramach której organy ochrony danych, odpowiedzialne za nadzór nad CIS zgodnie z rozporządzeniem (WE) nr 766/2008[22], tj. EIOD i krajowe organy ochrony danych – współpracują zgodnie z ich zakresem obowiązków w celu zapewnienia skoordynowanego nadzoru nad CIS.

Grupa ds. koordynowania nadzoru:

a) analizuje trudności realizacyjne dotyczące operacji CIS;

b) analizuje trudności napotykane w trakcie kontroli prowadzonych przez organy nadzorcze;

c) analizuje trudności z przypisaniem wykładni rozporządzeniu w sprawie CIS lub jego stosowaniem;

d) opracowuje zalecenia w celu dostarczenia wspólnych rozwiązań dla istniejących problemów; oraz

e) stara się wzmocnić współpracę pomiędzy organami nadzorczymi.

W 2010 r. EIOD zwołał dwa posiedzenia Grupy ds. Koordynowania Nadzoru nad Systemem CIS (w marcu i grudniu). Posiedzenia zgromadziły przedstawicieli krajowych organów ochrony danych oraz przedstawicieli Wspólnego Celnego Organu Nadzorczego i Sekretariatu Ochrony Danych.

W trakcie grudniowego posiedzenia grupa przyjęła regulamin, który będzie regulował jej przyszłą pracę z CIS oraz omówiła możliwe działania, które mają zostać podjęte na przestrzeni 2011 i 2012 r. w celu zapewnienia całościowego nadzoru nad ochroną danych w systemie.

[22] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 766/2008 z dnia 9 lipca 2008 r. zmieniające 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.

4.4. Współpraca policyjna i wymiarów sprawiedliwości: współpraca z JSB/JSA oraz WPPJ

EIOD współpracuje także z organami odpowiedzialnymi za nadzór nad specjalnymi organami lub określonymi wielkoskalowymi systemami informatycznym UE, takimi jak wspólne organy nadzorcze (JSB) Europolu i Eurojustu oraz wspólne organy nadzorcze (JSA) ds. systemu informacyjnego Schengen (SIS) oraz aspektów „byłego trzeciego filaru" systemu informacji celnej (CIS). Współpraca ta przyjmuje formę wzajemnego informowania się o kwestiach leżących we wspólnym interesie, w takich sytuacjach, jak te, w których EIOD i JSB/JSA osobno nadzorują różne części tego samego systemu.

W 2010 r. współpraca dotyczyła głównie CIS. Ponieważ EIOD i JSA CIS dzielą między sobą rolę nadzorczą dla tego samego systemu, bardzo ważna jest maksymalna koordynacja ich działania. W tym duchu EIOD zwrócił się do przedstawicieli JSA o uczestnictwo w posiedzeniach zorganizowanych w związku z koordynowanym nadzorem nad CIS (zob. pkt 4.3).

EIOD brał także udział w posiedzeniach i działaniach Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości (WPPJ). WPPJ pracowała nad kilkoma kwestiami w 2010 r., takimi jak tworzenie wspólnej polityki nadzoru lub umowy „typu Prüm" (dwustronne umowy w sprawie wymiany danych). WPPJ pracowała także z Grupą Roboczą Art. 29 nad wydaniem „wspólnego głosu europejskich organów ochrony danych" reprezentowanych w tych grupach roboczych, w sprawie umowy pomiędzy UE a USA o ochronie danych. Jest to przykład, jak potrzebna jest szeroko zakrojona współpraca pomiędzy tymi dwiema grupami w sytuacji, gdy rozróżnienie między byłym pierwszym i trzecim filarem staje się coraz mniej istotne.

WPPJ poruszyła także temat własnej przyszłości w świetle powyższych zmian i w perspektywie coraz większego zaangażowania Grupy Roboczej Art. 29 w obszary, którymi tradycyjnie zajmowała się WPPJ.

4.5. Konferencja europejska

Organy ochrony danych z państw członkowskich Unii Europejskiej i Rady Europy spotykają się raz w roku na wiosennej konferencji w celu omówienia kwestii leżących we wspólnym interesie oraz wymiany różnego rodzaju informacji i doświadczeń.

Europejska Konferencja Rzeczników Ochrony Danych Osobowych odbyła się w **Pradze w dniach 29–30 kwietnia 2010 r.**, pod hasłem „Patrząc w przeszłość, myśląc o przyszłości" Konferencję poprowadził czeski organ ochrony danych.

Konferencja obejmowała sesje poświęcone różnym kwestiom, w tym: 1) Internet przedmiotów; wszechobecny nadzór w czasie i przestrzeni – z prezentacją zastępcy Inspektora; 2) Dzieci zaplątane w sieci; 3) Ochrona danych osobowych na rozdrożu – z prezentacją EIOD; 4) Sektor publiczny: szanowany partner czy uprzywilejowany przetwarzający?

Jaka można się było spodziewać, przyszłe ramy ochrony danych, obecnie przygotowywane przez Komisję Europejską, były głównym tematem dyskusji. Przyjęto szereg uchwał, w szczególności w sprawie:

- planowanej umowy pomiędzy UE a USA w sprawie norm ochrony danych w dziedzinie współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych;
- skanerów ciała;
- ochrony dzieci;
- przyszłości prywatności.

4.6. Konferencja międzynarodowa

Przedstawiciele organów ochrony danych oraz rzeczników ochrony prywatności z Europy i innych części świata, w tym Kanady, Ameryki Łacińskiej, Australii, Nowej Zelandii, Hongkongu, Japonii oraz innych państw regionu Azji i Pacyfiku od wielu lat spotykają się na corocznych jesiennych konferencjach.

W tym roku Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności została zorganizowana przez izraelski organ ochrony danych w **Jeruzalem w dniach 26–29 listopada 2010 r.** Jej temat przewodni brzmiał: „Prywatność: pokolenia".

Zorganizowano szereg sesji plenarnych, by omówić następujące kwestie:

- Gdzie jesteśmy obecnie? Zmiana między pokoleniami w postrzeganiu prywatności;
- Jakie są plany regulacyjne: słowo od regulujących;
- Wbudowana ochrona prywatności;
- Przyszłość prywatności: jak normy prywatności mogą przenikać do regulacji.

Konferencja analizowała następnie perspektywy prywatności i ochrony danych różnych pokoleń. Główny temat konferencji dotyczył tego, jak przepisy i mechanizmy samoregulujące wpływają na technologię i vice versa. Kluczowym tematem konferencji było również coraz częstsze korzystanie z sieci społecznościowych.

EIDO i jego zastępca przedstawili prezentacje i przewodniczyli poszczególnym sesjom na Konferencji.

Na zamkniętej sesji rzeczników przyjęto różne uchwały; najważniejsza była wezwaniem do zorganizowania konferencji międzyrządowej w celu utworzenia wiążącego międzynarodowego instrumentu w zakresie prywatności i ochrony danych osobowych.

33. Międzynarodowa Konferencja będzie miała miejsce w Meksyku w listopadzie 2011 r.

4.7. Organizacje międzynarodowe (warsztaty we Florencji)

EIOD we współpracy z Europejskim Instytutem Uniwersyteckim zorganizował trzecią edycję warsztatów na temat ochrony danych w organizacjach międzynarodowych. Odbyły się one we Florencji w dniach 27–28 maja 2010 r. i przyciągnęły czołowe organizacje międzynarodowe, takie jak UNHCR,

WCO, IOM, MTK i wiele innych. Dyskusje dotyczyły różnorodnych wyzwań stojących przed organizacjami międzynarodowymi, starającymi się zapewnić dobry poziom ochrony danych w niejednokrotnie trudnych warunkach i bez jasnych podstaw prawnych. Te organizacje, które już osiągnęły dobry poziom ochrony danych, podkreślały wiele korzyści, jakie płyną z tego dla ich podstawowej działalności (np. bezpieczeństwo danych i legitymizacja działań w szczególności).

Po warsztacie EIOD rozesłał kwestionariusz w celu zebrania informacji na temat sposobów ochrony danych (lub jej braku) w uczestniczących organizacjach międzynarodowych. Skupiono się na tym, jak zapewnić faktyczną i skuteczną ochronę danych, a nie na szczegółowych ustaleniach o charakterze ustawodawczym.

W konsekwencji kwestionariusz jest oparty na już wykonanej pracy na międzynarodowych forach dotyczących ochrony danych w zakresie pojęcia rozliczalności jako narzędzia do dalszego nakłaniania administratorów danych do zmniejszania ryzyka nieprzestrzegania przepisów poprzez praktyczne mechanizmy skutecznej ochrony danych. Pojęcie to jest szczególnie odpowiednie w kontekście organizacji międzynarodowych, ponieważ ma zastosowanie bez względu na kontekst prawny przetwarzania danych.

Odpowiedzi te posłużą za podstawę przyszłych działań w tym kontekście. Wielu uczestników chciałoby, by takie warsztaty regularnie organizowano w przyszłości.

5 KOMUNIKACJA

5.1. Wprowadzenie

Informacja oraz komunikacja odgrywają centralną rolę w **eksponowaniu** najważniejszych działań EIOD i **poszerzaniu wiedzy** zarówno o jego pracy, jak i o ochronie danych w ogólności. Jest to tym ważniejsze, że istnieje potrzeba zwiększania wiedzy na temat roli i zadań EIOD na poziomie UE, choć trzeba przyznać, że poczyniono znaczne postępy w tym kierunku. Wskaźniki, takie jak liczba wniosków o udzielenie informacji otrzymywanych od obywateli, zapytania od mediów i zaproszenia na wywiady, liczba osób otrzymujących biuletyn oraz zaproszenia do wystąpień na konferencjach i ruch na stronie internetowej, jednoznacznie wskazują, że EIOD stał się punktem odniesienia dla kwestii ochrony danych na poziomie UE.

Zwiększona widoczność EIOD w strukturze instytucjonalnej ma szczególne znaczenie z punktu widzenia pełnionych przez niego trzech głównych funkcji: funkcji nadzorczej w odniesieniu do wszystkich europejskich instytucji i organów biorących udział w przetwarzaniu danych osobowych; funkcji konsultacyjnej w stosunku do instytucji zaangażowanych w opracowywanie i przyjmowanie nowego prawodawstwa i polityki (Komisja, Rada i Parlament), które mogą mieć wpływ na ochronę danych osobowych; funkcji współpracy z krajowymi organami nadzorczymi, jak też różnymi organami nadzorczymi w dziedzinie bezpieczeństwa i wymiaru sprawiedliwości.

Działania w 2010 r. były nadal ukierunkowane na dalsze usprawnienie działań komunikacyjnych i narzędzi informacyjnych EIOD. Głównym postępem w tym względzie było wprowadzenie języka niemieckiego jako trzeciego języka, obok angielskiego i francuskiego, w działaniach prasowych i komunikacyjnych. Ma to tym większe znaczenie, że język niemiecki ma najwięcej użytkowników w UE. Ogólnym celem jest więc dotarcie do szerszego grona odbiorców i zapewnienie niemieckojęzycznej prasie i obywatelom możliwości śledzenia działalności EIOD w ich własnym języku.

5.2. Aspekty działań komunikacyjnych

Polityka komunikacyjna EIOD musi uwzględniać specyficzne aspekty, które mają znaczenie z racji okresu działania tej instytucji, jej rozmiaru i zakresu kompetencji. Wymaga to podejścia dostosowanego do potrzeb i wykorzystującego właściwe narzędzia, aby dotrzeć do odpowiednich odbiorców, a jednocześnie móc dostosować się do rozmaitych ograniczeń i wymogów.

5.2.1. Główni odbiorcy i grupy docelowe

W odróżnieniu od większości pozostałych instytucji i organów UE, których polityka oraz działania komunikacyjne mają charakter ogólny i skierowane są do wszystkich obywateli UE, bezpośredni zakres działań EIOD jest znacznie węższy. Obejmuje on głównie europejskie instytucje i organy, ogólnie osoby, których dane dotyczą, a w szczególności personel UE, zainteresowane podmioty polityczne

w obrębie UE, a także partnerów zajmujących się ochroną danych. Dlatego też polityka komunikacyjna EIOD nie musi opierać się na strategii „komunikacji masowej". Uświadamianie obywateli państw członkowskich UE w zakresie problematyki ochrony danych opiera się na podejściu bardziej pośrednim, bazującym na przykład na działaniu organów ochrony danych na szczeblu krajowym.

EIOD dba jednak o widoczność swojej instytucji w oczach społeczeństwa, w szczególności przez wykorzystanie różnych narzędzi komunikacyjnych (strona internetowa, biuletyn i inne materiały informacyjne), regularne kontakty z zainteresowanymi stronami (np. wizyty studentów w biurze EIOD) oraz udział w imprezach publicznych, spotkaniach i konferencjach.

5.2.2. Polityka językowa

Polityka komunikacyjna EIOD musi również uwzględniać szczególny charakter działalności jego instytucji. Problematyka ochrony danych może być postrzegana jako skomplikowana i niejasna dla laika, a zatem język używany w komunikatach EIOD powinien być dostosowany do potrzeb odbiorców. Jeżeli chodzi o narzędzia informacyjne i komunikacyjne skierowane do różnorodnych grup odbiorców, konieczne jest stosowanie jasnego i zrozumiałego stylu oraz unikanie zbędnego żargonu. W tym celu czynione są stałe wysiłki, w szczególności przy komunikowaniu się z ogółem społeczeństwa i niespecjalistyczną prasą, służące skorygowaniu nadmiernie „prawniczego" wizerunku zagadnienia ochrony danych.

W przypadku bardziej świadomych odbiorców (np. specjalistów z zakresu ochrony danych, strony zainteresowane UE) stosowanie bardziej specjalistycznych terminów jest bardziej celowe. Dlatego też może być konieczne przekazywanie tych samych wiadomości przy użyciu innej formy i stylu komunikacji.

5.3. Relacje z mediami

EIOD pragnie być w jak największym stopniu dostępny dla dziennikarzy, aby umożliwić ogółowi społeczeństwa śledzenie swoich działań. Regularnie informuje on media, głównie za pośrednictwem komunikatów prasowych, wywiadów, dyskusji wyjaśniających kontekst wydarzeń oraz konferencji prasowych. Odpowiadanie na pytania ze strony mediów sprzyja dodatkowym regularnym kontaktom z nimi.

5.3.1. Komunikaty prasowe

W 2010 r. służba prasowa wydała 19 komunikatów prasowych. Większość z nich odnosiła się do opinii EIOD, a w szczególności **nowych opinii w sprawie aktów prawnych** mających istotne znaczenie z punktu widzenia ogółu społeczeństwa. Wśród poruszanych kwestii była strategia reformy ochrony danych UE, negocjacje w sprawie Umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA), Umowa pomiędzy EU a USA w sprawie programu śledzenia środków finansowych należących do terrorystów (TFTP), zarządzanie informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, prywatność i zaufanie w społeczeństwie informacyjnym, zewnętrzna strategia UE w zakresie danych dotyczących przelotu pasażera, proces oceny dyrektywy w sprawie zatrzymywania danych i strategia bezpieczeństwa wewnętrznego UE. Właściwe orzeczenia Trybunału Sprawiedliwości były również przedmiotem komunikatów prasowych, jak np. orzeczenie w sprawie Bavarian Lager i orzeczenie dotyczące niezależności organów ochrony danych.

Pojawiły się także komunikaty prasowe dotyczące **głównych działań z zakresu nadzoru**, w szczególności odnoszące się do przyjęcia wytycznych w zakresie nadzoru wideo i do całościowej polityki w dziedzinie monitorowania przestrzegania i egzekwowania przepisów.

Komunikaty prasowe publikowane są w językach angielskim i francuskim na stronie internetowej EIOD oraz wprowadzonej przez Komisję Europejską międzyinstytucjonalnej bazie komunikatów prasowych (RAPID). Wersję niemiecką wprowadzono w 2010 r. w celu odzwierciedlenia wprowadzenia języka niemieckiego jako trzeciego języka w działaniach komunikacyjnych EIOD. Komunikaty prasowe są rozsyłane do regularnie aktualizowanej sieci dziennikarzy i zainteresowanych stron. Informacje dostarczane w postaci komunikatów prasowych są zazwyczaj obszernie wykorzystywane w mediach – ukazują się często 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, ruchów na rzecz wolności obywatelskich, instytucji uniwersyteckich oraz przedsiębiorstw z branży informatycznej.

5.3.2. Wywiady

W 2010 r. EIOD udzielił około 20 wywiadów dziennikarzom z całej Europy reprezentującym prasę, radio i telewizję oraz media elektroniczne; znaczna liczba

zapytań pochodziła od prasy niemieckiej, austriackiej, holenderskiej i amerykańskiej.

Zaowocowało to wieloma artykułami w prasie krajowej, międzynarodowej i unijnej, ogólnej i specjalizującej się w zagadnieniach technologii informacyjnych, jak również wywiadami w radiu i telewizji (np. dla austriackiej publicznej telewizji, holenderskiego i austriackiego radia).

Wywiady dotyczyły spraw ogólnych, takich jak tendencja w kierunku społeczeństwa nadzorowanego oraz obecne i nadchodzące wyzwania w dziedzinie ochrony prywatności i danych. Omawiano także kwestie bardziej szczegółowe, które pojawiały się na pierwszych stronach gazet w 2010 r., w tym umowę z USA w sprawie TFTP, przegląd ram prawnych ochrony danych UE, zagadnienia prywatności w kontekście stron sieci społecznościowych, aplikacje geolokalizacji oraz korzystanie ze skanerów ciała w portach lotniczych.

5.3.3. Konferencje prasowe

Konferencja prasowa na temat przeglądu zasad ochrony danych i prywatności UE została zorganizowana w Brukseli w dniu 15 listopada 2010 r.. Peter Hustinx i Giovanni Buttarelli omówili w szczególności komunikat Komisji dotyczący strategii wzmacniania zasad ochrony danych UE, który został opublikowany na początku listopada 2010 r. Konferencja prasowa była również okazją do zaprezentowania sprawozdania rocznego EIOD z 2009 r. oraz zakreślenia głównych elementów działań EIOD w 2009 r. w zakresie zadań nadzorczych, konsultacyjnych i współpracy (zob. pkt 5.7.1).

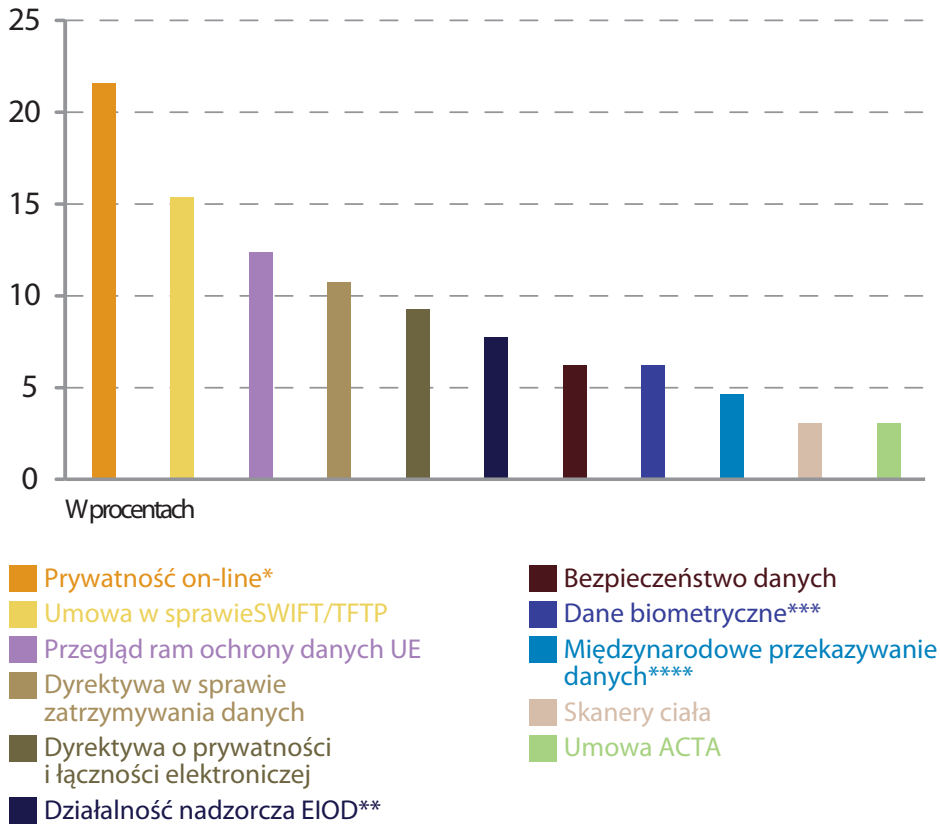
5.3.4. Pytania ze strony mediów

Media regularnie zadają EIOD pytania, prosząc zwykle o komentarze, wyjaśnienia lub informacje. W 2010 r. uwaga mediów skupiała się głównie na kwestii prywatności on-line, w szczególności w zakresie nowych aplikacji on-line, takich jak aplikacje geolokalizacji, wyszukiwarki i sieci społecznościowe – obszar, który zajmował pierwsze miejsce na liście zapytań. Umowa ze Stanami Zjednoczonymi o przetwarzaniu i przekazywaniu danych finansowych w ramach programu śledzenia środków finansowych należących do terrorystów (TFTP) cieszyła się również szczególnym zainteresowaniem ze strony prasy.

Pozostałe główne kwestie będące przedmiotem zainteresowania ze strony mediów obejmowały przegląd ram prawnych ochrony danych UE, dyrektywę w sprawie zatrzymywania danych, dyrektywę o prywatności i łączności elektronicznej i jej przepisy dotyczące naruszeń danych, działania nadzorcze EIOD, w tym jego wytyczne w zakresie nadzoru

Konferencja prasowa EIOD dotycząca przeglądu unijnych ram prawnych ochrony danych (Bruksela, 15 listopada 2010 r.).

Najważniejsze tematy pytań prasy w 2010 r.



* w tym nowe aplikacje on-line, wyszukiwarki i sieci społecznościowe

** w tym wytyczne w zakresie nadzoru wideo

*** w tym system informacyjny Schengen

**** w tym decyzje Komisji dotyczące odpowiedniego poziomu ochrony

wideo, kwestia bezpieczeństwa danych, dane biometryczne – w paszportach i systemie informacyjnym Schengen, międzynarodowe przekazywanie danych, w tym decyzje Komisji dotyczące odpowiedniego poziomu ochrony w odniesieniu do państw trzecich oraz korzystanie ze skanerów ciała w portach lotniczych.

5.4. Wnioski o udzielenie informacji i porad

Liczba wniosków o udzielenie informacji lub pomocy otrzymanych od obywateli nieco zmalała w 2010 r. (141 wniosków w porównaniu z 174 w 2009 r.). Wynika to głównie ze spadku liczby wniosków dotyczących kwestii ochrony danych na poziomie krajowym, wobec których EIOD nie jest właściwym organem. Taką zmianę można postrzegać jako wyniki wysiłków, jakie włożono w doprecyzowanie obszaru kompetencji EIOD za pomocą jego różnych narzędzi informacyjnych i komunikacyjnych.

Wnioski te pochodzą od wielu różnych osób i podmiotów – zainteresowanych stron funkcjonujących w ramach UE lub aktywnych w dziedzinie prywatności, ochrony danych i technologii informacyjnych (kancelarii prawnych, firm doradczych, lobbystów, organizacji pozarządowych, stowarzyszeń, uniwersytetów itp.), jak też obywateli proszących o dodatkowe informacje na temat zagadnień prywatności lub potrzebujących pomocy w związku z napotkanymi problemami z tej dziedziny.

Pierwsza kategoria wniosków otrzymanych w 2010 r. dotyczy skarg od obywateli UE, których EIOD nie jest władny rozpatrywać. Skargi te odnosiły się w większości do domniemanych naruszeń ochrony danych przez władze publiczne, państwowe lub prywatne przedsiębiorstwa oraz do usług i technologii on-line, takich jak gry komputerowe on-line, blogi, usługi geolokalizacji, serwisy społecznościowe i komunikatory. Inne kwestie obejmowały bezpieczeństwo danych bankowych, prawo dostępu do dokumentów przechowywanych przez krajowe organy administracyjne, rozpowszechniane danych osobowych wśród

osób trzecich bez zgody osób, których dane dotyczą i odwołania od decyzji krajowego organu ochrony danych. Ponieważ skargi tego rodzaju nie wchodzą w zakres kompetencji EIOD, w odpowiedzi precyzowano mandat EIOD oraz radzono, aby skarżący zwrócili się do właściwego krajowego organu, którym jest zazwyczaj krajowy organ ochrony danych właściwego państwa członkowskiego.

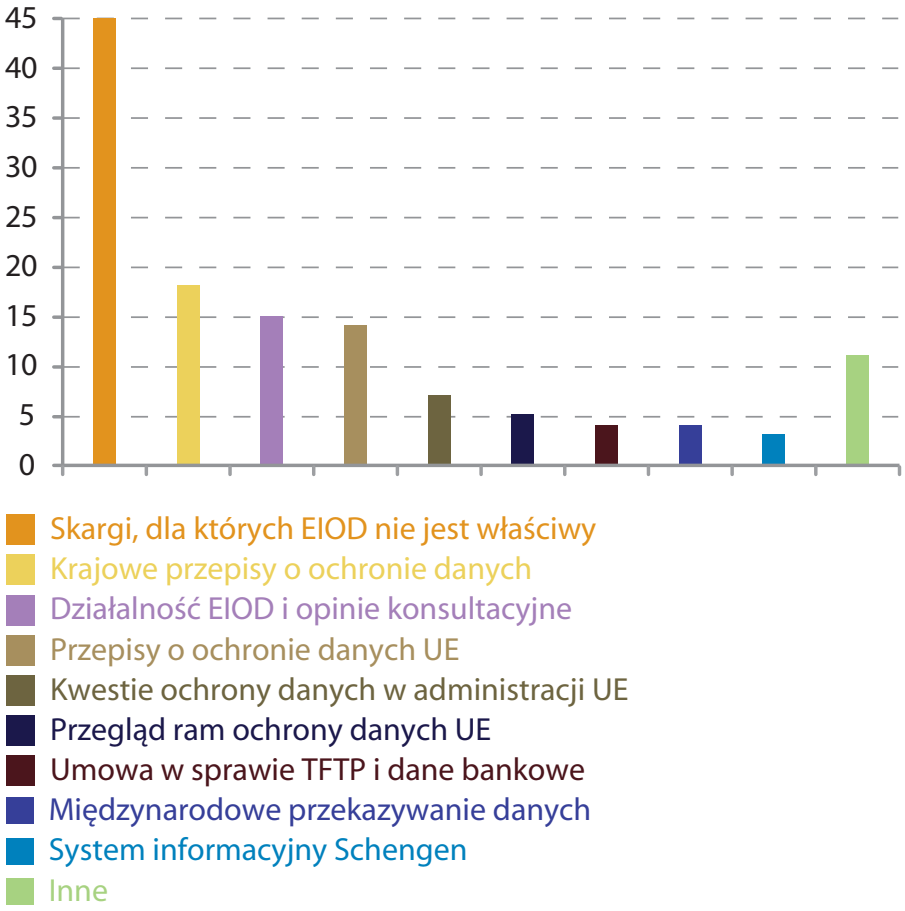
Druga kategoria wniosków otrzymanych w 2010 r. odnosiła się do ustawodawstwa dotyczącego ochrony danych w państwach członkowskich UE lub jego wdrożenia. W takich przypadkach EIOD radzi, aby wnioskujący skontaktował się z właściwym organem ochrony danych oraz w stosownych przypadkach – z działem ochrony danych Komisji Europejskiej.

Pozostałe kategorie wniosków o udzielenie informacji w większości mieściły się w kompetencjach EIOD, dlatego też w ich przypadku udzielano merytorycznych odpowiedzi. Obejmowały one pytania dotyczące działalności EIOD, w szczególności jego prac w zakresie polityki i konsultacji, prawodawstwa UE w zakresie ochrony danych, kwestii ochrony danych w administracji UE, przeglądu ram ochrony danych UE, umowy w sprawie TFPT i danych bankowych, międzynarodowego przekazywania danych i dostępu do systemu informacyjnego Schengen.

5.5. Wizyty szkoleniowe

W ramach wysiłków zmierzających do dalszego szerzenia wiedzy na temat ochrony danych oraz współdziałania z kręgami akademickimi EIOD regularnie gości grupy studentów specjalizujących się w dziedzinie prawa europejskiego, problematyce ochrony danych lub kwestiach związanych z bezpieczeństwem systemów informatycznych. W 2010 r. biuro EIOD odwiedziło siedem grup studentów z kilku europejskich krajów. Na przykład w październiku 2010 r. urząd EIOD odwiedziła grupa europejskich i pochodzących spoza Europy studentów prawa z niemieckiej Fundacji im. Friedricha Eberta; w trakcie wizyty przedstawiono rolę i działalność urzędu oraz omawiano zagadnienia ochrony danych w związku programem sztokholmskim. Wśród

Najważniejsze tematy wniosków o informacje od społeczeństwa w 2010 r.



innych grup należy wymienić austriackich słuchaczy studiów MBA w dziedzinie zarządzania instytucjami publicznymi i studentów z uniwersytetu w Tilburgu w Holandii, z Fundacji im. Róży Luksemburg i z francuskiego Uniwersytet Grenoble.

W celu dotarcia do młodszych odbiorców urząd EIOD zaprosił również grupę uczniów szkół średnich z Austrii, z którymi pracownicy omawiali szczególnie interesujące ich realne problemy w zakresie ochrony danych, takie jak problematyka prywatności w kontekście sieci społecznościowych on-line.

5.6. Narzędzia informacyjne on-line

5.6.1. Strona internetowa

Strona internetowa pozostaje najważniejszym kanałem komunikacji i narzędziem informacyjnym EIOD. Jest aktualizowana niemal codziennie. Stanowi też medium, za którego pośrednictwem użytkownicy mogą uzyskać dostęp do dokumentów sporządzonych w ramach działalności EIOD (np. opinie dotyczące kontroli wstępnych i wnioski odnoszące się do prawodawstwa UE, priorytety działań, przemówienia Inspektora i jego zastępcy, komunikaty prasowe, biuletyny oraz informacje na temat wydarzeń).

Rozwój strony

W 2010 r. najbardziej znaczącą zmianą na stronie internetowej było wprowadzenie jej niemieckiej wersji obok istniejącej angielskiej i francuskiej. Ta inicjatywa jest częścią decyzji o publikacji wszystkich zewnętrznych materiałów komunikacyjnych w – przynajmniej – tych trzech językach, by lepiej zaspokajać potrzeby informacyjne społeczeństwa i stron zainteresowanych.

Strona główna została również przeorganizowana w celu lepszego uwidocznienia najnowszych doniesień na temat działalności EIOD.

Planowane są dalsze udoskonalenia strony internetowej, w tym:

- wprowadzenie formularza skargi on-line w celu ułatwienia procesu składania skarg i przyspieszenia procesu ich rozpatrywania przez służby EIOD;
- przebudowa działu opinii dotyczących kontroli wstępnych w celu zwiększenia możliwości wyszukiwania i opcji nawigacyjnych w kategoriach tematycznych;
- usprawniona prezentacja rejestru powiadomień;
- wprowadzenie sekcji „zestaw dla prasy" w celu dostarczenia przedstawicielom mediów odpowiednich materiałów i zasobów, które można wykorzystać w najnowszych doniesieniach i wywiadach.

Ruch i nawigacja

W ramach bieżących wysiłków w kierunku usprawnienia strony internetowej w 2009 r. udoskonalono działanie wielu funkcji, z których nie wszystkie są widoczne na pierwszy rzut oka (np. narzędzie do wyszukiwania zaawansowanego).

Analiza danych dotyczących ruchu i nawigacji wskazuje, że na stronę weszło w 2010 r. łącznie 108 215 użytkowników, w tym ponad 12 000 miesięcznie w lutym i marcu. Stanowi to zdecydowany wzrost w porównaniu z 2009 r. Po stronie głównej najczęściej odwiedzano podstrony: kontakt, nadzór i konsultacje, chociaż popularne były też aktualności, publikacje i wydarzenia. Statystyki pokazują także, że większość odwiedzających uzyskuje dostęp do strony internetowej, wpisując bezpośrednio jej adres, korzystając z zakładki, łącza w e-mailu lub łącza z innej strony, np. portalu Europa lub strony internetowej krajowego organu ochrony danych. Z łącz zwracanych przez wyszukiwarki korzysta bardzo niewielka liczba odwiedzających. Takie dane pozwalają przypuszczać, że stronę internetową EIOD odwiedza grupa stałych użytkowników, którzy ufają jej zawartości.

5.6.2. Biuletyn

Biuletyn EIOD pozostaje skutecznym narzędziem służącym informowaniu o bieżących działaniach EIOD oraz zwróceniu uwagi na nowości na stronie internetowej. Dostarcza on wiadomości na temat najnowszych opinii EIOD dotyczących wniosków ustawodawczych UE i kontroli wstępnych. Zawiera też informacje o organizowanych konferencjach i innych wydarzeniach z tej dziedziny oraz o ostatnich wystąpieniach Inspektora i jego zastępcy. Biuletyny dostępne są na stronie internetowej EIOD,

można zamówić ich subskrypcję na odpowiedniej podstronie.

W 2010 r. opublikowano pięć wydań biuletynu EIOD; ukazywały się one średnio co dwa miesiące. Do 2010 r. biuletyn był wydawany w języku angielskim i francuskim; wersja niemieckojęzyczna została wprowadzona w 2010 r. w celu dotarcia do szerszego grona odbiorców i odzwierciedlenia stosowania trzech języków roboczych w służbie prasowej EIOD.

Liczba subskrybentów wzrosła z 1220 pod koniec 2009 r. do ok. 1500 pod koniec 2010 r. Są wśród nich posłowie do Parlamentu Europejskiego, pracownicy instytucji UE oraz krajowych organów ochrony danych, a także dziennikarze, przedstawiciele środowiska akademickiego, firmy telekomunikacyjne i kancelarie prawne.

5.6.3. Intranet

W celu poprawy wewnętrznej komunikacji i wymiany informacji pomiędzy poszczególnymi sektorami urzędu EIOD, stworzono Intranet z pomocą właściwej służby Parlamentu Europejskiego. Ten nowy wewnętrzny portal stanie się w pełni funkcjonalny z początkiem 2011 r.

5.7. Publikacje

5.7.1. Sprawozdanie roczne

Sprawozdanie roczne jest podstawową publikacją EIOD. Stanowi ono przegląd działań EIOD w trakcie roku sprawozdawczego w głównych obszarach jego działalności, tj. nadzoru, konsultacji i współpracy oraz określa ścisłe priorytety na kolejny rok. Opisuje również osiągnięcia w zakresie komunikacji zewnętrznej, a także zmiany dotyczące administracji, budżetu i personelu.

Sprawozdanie to może szczególnie interesować różne grupy i osoby na szczeblu międzynarodowym, europejskim i krajowym – ogólnie osoby, który dane dotyczą, a w szczególności pracowników UE, instytucje UE, organy ochrony danych, specjalistów ds. ochrony danych, grupy interesów i organizacje pozarządowe zajmujące się tą dziedziną, dziennikarzy oraz wszystkie osoby, które poszukują informacji na temat ochrony danych osobowych na szczeblu UE.

W 2010 r. wprowadzano szereg udoskonaleń do sprawozdania, w zakresie formy i treści, w celu uzyskania publikacji bardziej przyjaznej dla użytkownika, przy jednoczesnym zapewnieniu przejrzystej prezentacji głównych wyników i wniosków sprawozdania.

Inspektor i jego zastępca przedstawili streszczenie sprawozdania rocznego EIOD za rok 2009 r. Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego w dniu 15 listopada 2010 r. Główne elementy sprawozdania przedstawiono także prasie na konferencji prasowej zorganizowanej tego samego dnia, dotyczącej przyszłości ram prawnych ochrony danych UE (zob. pkt 3.3).

5.7.2. Publikacje tematyczne

Rozpoczęto także przygotowania do publikacji tematycznych „broszur" na temat kwestii ochrony danych o strategicznym znaczeniu. Celem będzie zapewnienie ukierunkowanych porad ogółowi społeczeństwa i zainteresowanym stronom. Pierwszy zestaw faktów będzie obejmował takie kwestie, jak dyrektywa o prywatności i łączności elektronicznej, umowa w sprawie SWIFT/TFTP i dane dotyczące przelotu pasażera

Sprawozdanie roczne EIOD 2009

5.8. Wydarzenia zwiększające świadomość

EIOD bardzo chętnie korzysta ze stosownej sposobności do podkreślania coraz większego znaczenia prywatności i ochrony danych oraz krzewienia wiedzy na temat praw przysługujących osobom, których dane dotyczą, oraz obowiązków europejskich organów administracji w zakresie prywatności i ochrony danych.

5.8.1. Dzień Ochrony Danych

Państwa członkowskie Rady Europy oraz instytucje i organy europejskie świętowały 28 stycznia 2010 r. czwarty Europejski Dzień Ochrony Danych. Data ta upamiętnia rocznicę uchwalenia Konwencji Rady Europy o ochronie danych osobowych (Konwencji nr 108) – pierwszego wiążącego prawnie instrumentu międzynarodowego dotyczącego ochrony danych.

W poprzednich latach EIOD korzystał z tej sposobności, by podkreślić znaczenie prywatności i ochrony danych, w szczególności zaś, aby podnieść świadomość praw i obowiązków w tej dziedzinie wśród pracowników instytucji UE. W każdym Dniu Ochrony Danych, w siedzibie Parlamentu Europejskiego, Komisji Europejskiej oraz Rady uruchamiano stoisko informacyjne, we współpracy z inspektorami ochrony danych tych instytucji. Odwiedzający mieli możliwość zadać pytanie pracownikom urzędu EIOD i inspektorowi ochrony danych oraz sprawdzić swoją wiedzę na temat ochrony danych w quizie.

W 2010 r. EIOD wznowił tę szczególną działalność, wkładając dalej wysiłki w zwiększanie świadomości wśród pracowników instytucji UE. W dniu 8 stycznia 2010 r., w Komisji Europejskiej zorganizowano przedpołudniową debatę zatytułowaną „Prywatność i ochrona danych: co to znaczy dla Ciebie?". Peter Hustinx wystąpił z prezentacją przed pracownikami Komisji i odpowiedział na ich pytania o prawa do ochrony danych oraz środki ich wykonywania w obrębie organów administracji UE.

Zainteresowanym instytucjom przekazano również komunikat wideo od Inspektora i jego zastępcy oraz udostępniono go na stronie internetowej w celu prezentacji roli EIOD i zarysowania przyszłych wyzwań.

EIOD brał również udział w różnych wydarzeń zorganizowanych w Brukseli z okazji Dnia Ochrony Danych, takich jak konferencja i ceremonia wręczenia nagród, które zakończy kampanię „Pomyśl o prywatności" zainicjowanej przez European Schoolnet i Microsoft. Kampania obejmowała ogólnoeuropejski konkurs „Pomyśl o prywatności", w którym osoby w wieku 15–19 lat zostały zaproszone do stworzenia i przedstawienia multimedialnej pre-

Peter Hustinx, EIOD, przemawia na konferencji i ceremonii wręczenia nagród „Pomyśl o prywatności" (Bruksela, 28 stycznia 2010 r.).

zentacji na temat „Prywatność to prawo człowieka – dbaj o nią".

W dniach 29–30 stycznia 2010 r. EIOD wziął udział w międzynarodowej konferencji „Komputery, prywatność a ochrona danych", która miała być pomostem pomiędzy decydentami, przedstawicielami środowiska akademickiego, specjalistami i aktywistami w celu omówienia nowych kwestii prywatności, ochrony danych i technologii informacyjnych. W tym czwartym wydarzeniu tematem przewodnim konferencji był „element wyboru" odnoszący się do wielu opcji otwierających się przed polityką ochrony danych. Członkowie Sekretariatu EIOD wzięli udział w dyskusjach panelowych, a Peter Hustinx wygłosił końcową przemowę na konferencji.

5.8.2. Dzień Otwarty UE

W dniu 8 maja 2010 r. biuro EIOD uczestniczyło, jak co roku, w zorganizowanym w Parlamencie Europejskim w Brukseli Dniu Otwartym instytucji Unii Europejskiej.

Dzień Otwarty UE jest doskonałą okazją do krzewienia wiedzy wśród społeczeństwa na temat potrzeby ochrony ich prywatności i danych osobowych.

Stoisko EIOD działało w głównym gmachu Parlamentu Europejskiego, a pracownicy Sekretariatu EIOD byli na miejscu, gotowi odpowiadać na pytania odwiedzających. Podobnie jak w przypadku stoiska EIOD podczas Dnia Ochrony Danych – odwiedzającym rozdawano materiały informacyjne oraz udostępniono quiz na temat prywatności i ochrony danych na poziomie UE.

Odwiedzający wypełniają quiz na temat ochrony danych w trakcie Dnia Otwartego UE.

6 ADMINISTRACJA, BUDŻET I PERSONEL

6.1. Wprowadzenie

Monique Leens, kierownik administracji Sekretariatu EIOD od samego początku jej powstania, odeszła na emeryturę w czerwcu 2010 r. Jej wkład w tworzenie instytucji EIOD przez ostatnie sześć lat był ogromny i EIOD życzy jej wszystkiego dobrego na jak najbardziej zasłużonej emeryturze. Po jej odejściu Christopher Docksey, oddelegowany tymczasowo ze służby prawnej Komisji Europejskiej, zaczął pełnić obowiązki dyrektora EIOD, a następnie Sekretariat zasilił Leonardo Cervera Navas, również z Komisji Europejskiej, kierownik ds. zasobów ludzkich, budżetu i administracji.

Liczba pracowników znacznie wzrosła w ciągu 2010 r. Po publikacji list rezerwy kadrowej z otwartych konkursów dotyczących ochrony danych zorganizowanych przez EIOD przyjęto dwunastu nowych urzędników. Należało w związku z tym nie tylko znaleźć dodatkową przestrzeń biurową, ale również przyjąć nową strukturę organizacją zdolną zaspokoić potrzeby większej organizacji pełniącej nowe i złożone obowiązki.

Reorganizacja EIOD, którą rozpoczęto wewnętrznym pismem z kwietnia 2010 r., była kontynuowana przez cały rok i była przedmiotem oceny zewnętrznego doradcy ds. zarządzania. Prace te będą prawdopodobnie kontynuowane w 2011 r., ze szczególnym uwzględnieniem strategii i zarządzania wynikami.

6.2. Budżet

W 2010 r. budżet w wysokości 7 104 351 został przyznany EIOD przez władzę budżetową. Oznacza to wzrost o 6,62% w porównaniu z poprzednim rokiem.

Wzrost ten odpowiada potrzebom większej organizacji z większym personelem, większymi zadaniami i nowymi obowiązkami w wyniku wejścia w życie traktatu lizbońskiego. Oprócz wynagrodzeń i wydatków związanych z budynkami znaczna część budżetu EIOD przeznaczana jest na tłumaczenia, ponieważ opinie EIOD na temat wniosków ustawodawczych są tłumaczone na wszystkie urzędowe języki europejskie i publikowane w *Dzienniku Urzędowym Unii Europejskiej*. Opinie dotyczące kontroli wstępnych i inne publikowane dokumenty są również tłumaczone na języki robocze EIOD (angielski, francuski i niemiecki).

Poświadczenie wiarygodności (DAS) z 2009 Europejskiego Trybunału Obrachunkowego nie wymagało większych zmian. Sprawozdanie końcowe zawierało jedynie dwa zalecenia: poprawa wewnętrznych standardów kontroli przez przyjęcie systemu kontroli ex post i utworzenie centralnego rejestru w celu zapisywania odstępstw od standardowych procedur finansowych.

Komisja Europejska nadal udzielała EIOD wsparcia w sprawach finansowych w 2010 r., w szczególności w odniesieniu do usług księgowych, księgowy Komisji pełni bowiem także rolę księgowego EIOD. W tym kontekście Dyrekcja Generalna Komisji ds. Budżetu dokonała zatwierdzenia procedur lokalnych systemów księgowych i wydała pozytywne

sprawozdanie. Wyznaczenie koordynatora ds. księgowości było głównym zaleceniem w tym sprawozdaniu.

Wszystkie zalecenia zawarte w tych sprawozdaniach Europejskiego Trybunału Obrachunkowego i Komisji zostały wdrożone w następujący sposób:

a) wprowadzono nowy system wewnętrznej kontroli finansowej w stosunku do przepływu środków finansowych;

b) wyznaczono koordynatora ds. księgowości;

c) ustanowiono rejestr odstępstw;

d) system kontroli ex post jest obecnie przyjmowany.

W wyniku reorganizacji EIOD Christopher Docksey, pełniący obowiązki dyrektor EIOD, został wyznaczony na delegowanego urzędnika zatwierdzającego, a Leonardo Cervera Navas, kierownik ds. zasobów ludzkich, budżetu i administracji, na subdelegowanego urzędnika zatwierdzającego. Ta nowa struktura zapewnia większą elastyczność i wzmacnia proces zatwierdzania transakcji finansowych EIOD.

Jeśli szczegółowe przepisy nie zostały określone, EIOD stosuje wewnętrzny regulamin Komisji w zakresie wykonania budżetu.

6.3. Zasoby ludzkie

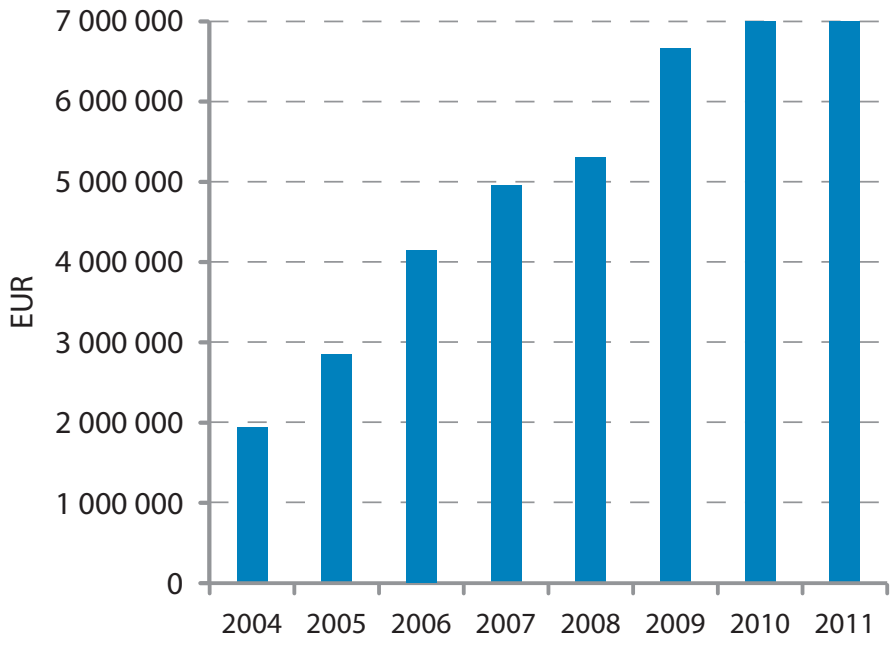
6.3.1. Rekrutacja

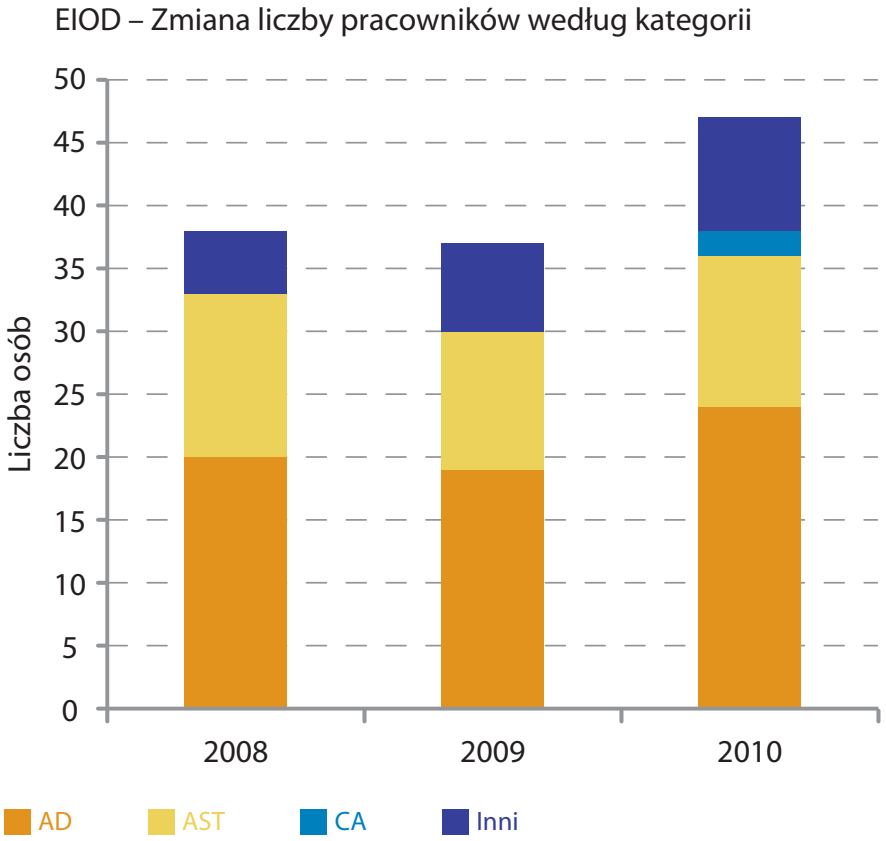
Jak w poprzednich latach, i jak wykazano w poprzednich rozdziałach niniejszego sprawozdania, rosnąca widoczność EIDO oznacza większe obciążenie pracą, a także poszerzenie zakresu zadań, których nie uwzględniono z perspektywy zasobów ludzkich.

Na podstawie umowy o gwarantowanym poziomie usług EIOD korzysta z usług Europejskiego Urzędu Doboru Kadr (EPSO) i wchodzi w skład jego zarządu jako obserwator. W związku z tym, w ścisłej współpracy z EPSO, EIOD zorganizował otwarty konkurs z dziedziny ochrony danych w 2009 r. w celu zrekrutowania wysoko wyspecjalizowanego personelu. Latem 2010 r. udostępniono trzy listy rezerwy kadrowej dla grup funkcyjnych AD9, AD6 i AST3. Ważność list rezerwy kadrowej została przedłużona co najmniej do końca 2011 r.

Po publikacji tych list EIOD wszczął główną procedurę rekrutacji, organizując rozmowy z kandydatami z list rezerwy kadrowej i urzędnikami z innych instytucji, zgodnie z art. 29 rozporządzenia pracowniczego. W ciągu 2010 r. EIOD zatrudnił 12 urzędników i wprowadził po raz pierwszy nową kategorię pracowników: personel kontraktowy. W wyniku procedury selekcji kandydatów wybranych z list CAST zatrudniono również dwóch pracowników

EIOD – rozwój budżetu w latach 2004–2011





kontraktowych. Aby odpowiedzieć na tymczasowe zapotrzebowanie zatrudniono również p.o. sekretarza w 2010 r. Podsumowując, w 2010 r. EIOD zatrudnił 15 nowych pracowników.

W końcu opublikowano ogłoszenie o naborze na stanowisko dyrektora EIOD na międzyinstytucjonalnej stronie internetowej poświęconej rekrutacji pod koniec 2010 r. Ta procedura rekrutacji kadry zarządzającej ma zostać zakończona w pierwszej połowie 2011 r.

6.3.2. Program stażowy

Program stażowy powstał 2005 r. Celem tego programu jest stworzenie osobom, które właśnie skończyły studia, możliwości wykorzystania swojej wiedzy teoretycznej w praktyce, a zarazem zdobycia doświadczenia w zakresie bieżącej działalności EIOD. Dzięki temu EIOD ma też okazję stać się bardziej rozpoznawalny wśród młodych obywateli UE, w szczególności studentów i absolwentów, którzy specjalizują się w problematyce ochrony danych.

Program zasadniczy obejmuje dwa pięciomiesięczne staże rocznie (od marca do lipca oraz od października do lutego); w każdym cyklu uczestniczy średnio dwóch stażystów. W wyjątkowych sytuacjach i stosując surowe kryteria wstępu EIOD może również przyjąć doktorantów na staże bezpłatne. Wszyscy stażyści, szkoleni odpłatnie lub nie, biorą udział w pracach teoretycznych i praktycznych oraz zbierają pożyteczne osobiste doświadczenia.

Na podstawie umowy o gwarantowanym poziomie usług podpisanej z Komisją EIOD korzysta z pomocy administracyjnej biura ds. staży Dyrekcji Generalnej ds. Edukacji i Kultury Komisji Europejskiej, które niezmiennej udziela cennego wsparcia dzięki wielkiemu doświadczeniu swoich pracowników.

6.3.3. Program dla oddelegowanych ekspertów krajowych

Realizacja programu dla oddelegowanych ekspertów krajowych rozpoczęła się w styczniu 2006 r. Co roku oddelegowywano średnio dwóch ekspertów krajowych z organów ochrony danych w państwach członkowskich. Oddelegowanie ekspertów krajowych daje EIOD możliwość korzystania z wiedzy fachowej i doświadczenia tych pracowników oraz zwiększenia rozpoznawalności jego instytucji na szczeblu krajowym. Program ten umożliwia

także oddelegowanym ekspertom krajowym zapoznanie się z problematyką ochrony danych na poziomie UE.

6.3.4. Struktura organizacyjna

Struktura organizacyjna EIOD nie uległa zmianie od czasu jest powstania w 2004 r. do 2009 r., gdy podjęto pierwsze kroki w kierunku reorganizacji wraz z utworzeniem stanowiska Dyrektora jako Kierownika Sekretariatu.

W 2010 r. struktura organizacja EIOD przeszła poważne zmiany, wraz ze zreorganizowaniem personelu w obrębie pięciu sektorów: nadzór i egzekwowanie przepisów; polityka i konsultacja; rejestr i wsparcie operacyjne; informacja i komunikacja; zasoby ludzkie, budżet i administracja – i kierownikami sektorów wyznaczonym z personelu kierowniczego średniego szczebla. W ramach nowej struktury organizacyjnej Dyrektor reprezentuje EIOD na poziomie personelu kierowniczego i zapewnia wdrażanie strategii oraz horyzontalną koordynację działań. Inspektorzy nadal ponoszą ostateczną odpowiedzialność za zarządzanie, ale obecnie koncentrują się bardziej na procesie decyzyjnym i relacjach międzyinstytucjonalnych.

Zmiany te doprowadziły do nowej struktury organizacyjnej przedstawionej na stronie internetowej EIOD.

6.3.5. Szkolenia

Jednym z priorytetów na 2010 r. były zapewnienie lepszych możliwości szkolenia się i rozwijania kariery zawodowej dla pracowników. Podpisano nową umowę o gwarantowanym poziomie usług z Departamentem ds. Zasobów Ludzkich Komisji Europejskiej, która umożliwi elektroniczny dostęp do katalogu szkoleń Komisji na początku 2011 r. Od tej pory pracownicy EIOD będą mieli bezpośredni dostęp do aplikacji SYSLOG Formation i będą mieli takie same możliwości szkolenia się jak urzędnicy Komisji.

Wielu pracowników uczestniczyło w kursach językowych, udostępniono im także szkolenia organizowane na poziomie międzyinstytucjonalnym i – jeśli była taka potrzeba – zewnętrzne szkolenia. Kurs zatytułowany „Program osobistej wydajności", zorganizowany specjalnie dla EIOD, był szczególnie udanym przedsięwzięciem. W szkoleniu uczestniczyły trzy sektory w 2010 r. i będą w nim uczestniczyli wszyscy pozostali pracownicy w pierwszej połowie 2011 r.

W wyniku reorganizacji EIOD nowe kierownictwo odbyło specjalne szkolenie i coaching z zakresu zarządzania, zarówno jako indywidualni zarządzający, jak i jako zespół.

EIOD nadal uczestniczył w międzyinstytucjonalnych komitetach (Międzyinstytucjonalna Grupa Robocza Europejskiej Szkoły Administracji (EAS), Międzyinstytucjonalna Grupa Oceny Szkoleń EAS i Międzyinstytucjonalny Komitet ds. szkoleń językowych), co pozwala łączyć siły i uzyskać korzyści skali w obszarze, w którym potrzeby są zasadniczo podobne we wszystkich instytucjach UE. Jak w poprzednich latach EIOD podpisał, wraz z innymi instytucjami, protokół w sprawie harmonizacji kosztów międzyinstytucjonalnych kursów językowych oraz nowy protokół w sprawie podziału między instytucje kosztów projektów pedagogicznych w zakresie międzyinstytucjonalnych szkoleń językowych.

W 2011 r. EIOD będzie kontynuował działania mające na celu zwiększenie możliwości szkolenia i rozwijania kariery przez jego pracowników. Planowana jest także aktualizacja decyzji w sprawie szkoleń z dnia 18 lipca 2007 r., po dogłębnej konsultacji z pracownikami.

6.3.6. Działania socjalne

Inspektor podpisał z Komisją umowę o współpracy w celu ułatwienia integracji nowych pracowników, np. przez zapewnienie im porad prawnych w zakresie spraw prywatnych (wynajmu mieszkania, kupna domu itd.) oraz dania im sposobności do aktywności towarzyskiej i nawiązywania kontaktów. Nowy personel zostaje osobiście powitany przez Inspektora i jego zastępcę oraz dyrektora EIOD. Oprócz swoich autorytetów poznają także pracowników sektora zasoby ludzkie, budżet i administracja, którzy zapewniają wytyczne administracyjne EIOD i inne informacje na temat szczegółowych procedur EIOD.

EIOD dalej rozwijał współpracę międzyinstytucjonalną w zakresie opieki nad dziećmi: dzieci pracowników EIOD mają dostęp do żłobków, ośrodków opieki nad dziećmi w godzinach polekcyjnych i ośrodków rekreacyjnych opieki nad dziećmi Komisji oraz do europejskich szkół. EIOD bierze udział w charakterze obserwatora w obradach komitetu doradczego Parlamentu Europejskiego ds. bezpieczeństwa i ochrony w miejscu pracy, co ma na celu doskonalenie środowiska pracy.

W 2010 r. nowo utworzone sektory zorganizowały własne imprezy integracyjne, by obudzić ducha współpracy i pomóc nowym pracownikom się zintegrować. Pod koniec roku miało miejsce spotkanie bożonarodzeniowe, które było okazją do powitania nowych kolegów i podsumowania intensywnego roku obfitującego w zmiany.

6.4. Funkcje kontrolne

6.4.1. Kontrola wewnętrzna

Działające od 2006 r. wewnętrzne mechanizmy kontrolne zapewniają efektywne i zgodne z regulacjami osiąganie celów EIOD. EIOD przyjął szczegółowe procedury kontroli wewnętrznej dostosowane do potrzeb, rozmiaru i działalności instytucji. System zaprojektowano tak, by zamiast wyeliminowania ryzyka nieosiągnięcia celów biznesowych zarządzać nim.

EIOD przyjął do wiadomości roczne sprawozdanie z działalności i związane z nim poświadczenie wiarygodności podpisane przez delegowanego urzędnika zatwierdzającego. Ogólnie rzecz biorąc, EIOD uważa, że funkcjonujące mechanizmy kontroli wewnętrznej dają wystarczającą pewność co do legalności i prawidłowości działań, za które instytucja jest odpowiedzialna. Mimo to, w 2010 r. przyjęto bardziej ambitne podejście. Wykaz działań, które wdrażają wewnętrzne standardy kontroli, został rozszerzony w celu zapewnienia bardziej efektywnej wewnętrznej kontroli istniejących procesów.

Przykładowo, przyjęto nowe podręczniki w celu lepszego zarządzania procesami, jak np. procesami związanymi z kontrolami wstępnymi, skargami lub sprawami sądowymi. Działania, takie jak zwiększanie świadomości na temat etyki, przyjęcie bardziej szczegółowych opisów stanowisk, dodatkowych zasad wewnętrznych lub nowego systemu indywidualnego szkolenia są opracowywane w ścisłej współpracy z pracownikami i przy pełnym poparciu inspektorów.

6.4.2. Audyt wewnętrzny

Audytor wewnętrzny Komisji jest również audytorem wewnętrznym EIOD. Aby zapewnić skuteczne zarządzanie zasobami EIOD, audytor wewnętrzny regularnie sprawdza mechanizmy kontroli wewnętrznej instytucji, jak również jej operacji finansowych.

Powstałe w wyniku audytu uzupełniającego w grudniu 2008 r. przeprowadzonego przez Służbę Audytu Wewnętrznego (IAS) sprawozdanie przyjęte w maju 2009 r. potwierdziło osiągnięcie celów EIOD, choć zidentyfikowało również kilka kwestii do ewentualnej poprawy. Niektóre z tych kwestii były już przedmiotem działań, a inne są w trakcie zmian wraz z reorganizacją EIOD.

Ocena ryzyka przez IAS została zaplanowana na początek 2011 r. z myślą o audycie w dalszej części roku.

6.4.3. Bezpieczeństwo

W grudniu 2010 r. EIOD postanowił wyznaczyć dwóch pracowników na stanowisko lokalnego inspektora bezpieczeństwa, lokalnego inspektora bezpieczeństwa danych oraz ich zastępców, w obu przypadkach na niepełny etat. Zawarto pierwsze umowy ze służbami Komisji Europejskiej i Parlamentu Europejskiego i uzgodniono pierwszy obszar współpracy. Proces poświadczenia bezpieczeństwa osobowego odnośnych pracowników został rozpoczęty. Dalszy proces będzie koncentrował się na bezpieczeństwie informacji i bezpieczeństwie technologii informacyjnej (IT), w szczególności w odniesieniu do tworzenia wewnętrznego systemu zarządzania obiegiem spraw EIOD.

W 2011 r. EIOD będzie kontynuował prace nad decyzją w sprawie bezpieczeństwa przyjętą pod koniec 2008 r., która obejmowała środki odnoszące się do zarządzania informacjami poufnymi i bezpieczeństwa systemów informatycznych, a także bezpieczeństwa i higieny pracy oraz bezpieczeństwa budynków.

6.5. Infrastruktura

Zgodnie z porozumieniem o współpracy administracyjnej siedziba EIOD znajduje się w budynku Parlamentu Europejskiego, który wspiera ponadto EIOD w zakresie technologii informacyjnej i infrastruktury. W związku ze znacznym wzrostem liczby pracowników w 2010 r. we współpracy z Parlamentem Europejskim udostępniono nową przestrzeń biurową.

Budynek będący siedzibą EIOD został częściowo odnowiony w 2010 r. Renowacja ta, przeprowadzona pod nadzorem Parlamentu Europejskiego, znacznie zwiększyła poziom komfortu i zadowolenia w pracy. Ograniczona przestrzeń pozostaje jednak poważnym problemem dla EIOD i kwestia ta

była tematem kilku spotkań z Parlamentem Europejskim.

Instytucja nadal zarządza samodzielnie zasobami biurowymi i sprzętem komputerowym przy wsparciu ze strony służb Parlamentu Europejskiego.

6.6. Otoczenie administracyjne

6.6.1. Pomoc administracyjna i współpraca międzyinstytucjonalna

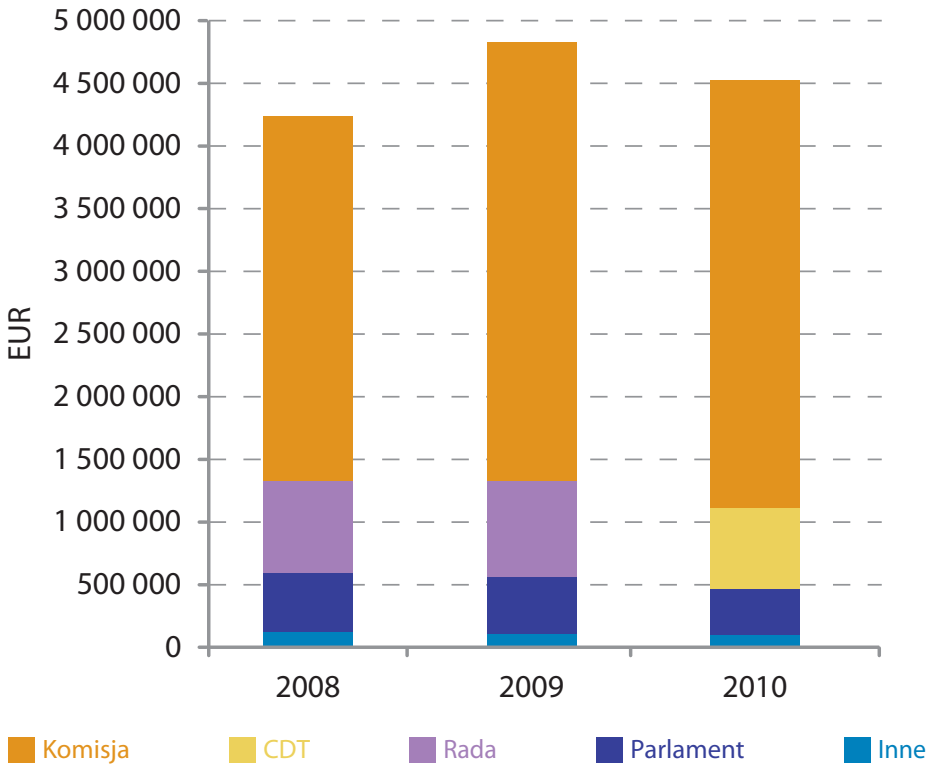
Na mocy porozumienia zawartego z sekretarzami generalnymi Komisji, Parlamentu Europejskiego oraz Rady w 2004 r. i przedłużonego w 2006 r. na okres trzech lat i w 2010 r. na okres dwóch lat EIOD korzysta ze współpracy międzyinstytucjonalnej w zakresie wielu obszarów. Współpraca ta jest dla EIOD bardzo wartościowa ze względu na zwiększenie wydajności i uzyskiwane korzyści skali.

W 2010 r. kontynuowano współpracę międzyinstytucjonalną z różnymi dyrekcjami generalnymi Komisji (DG ds. Zasobów Ludzkich i Bezpieczeństwa; DG ds. Budżetu; Służbą Audytu Wewnętrznego; DG ds. Edukacji i Kultury), Urzędem Administracji i Wypłacania Należności Indywidualnych, Europejską Szkołą Administracji (EAS) oraz z różnymi służbami Parlamentu Europejskiego (ds. technologii informacyjnej – w szczególności w związku z pracami nad utrzymaniem i rozwojem strony internetowej EIOD, jak również w zakresie wyposażenia pomieszczeń, ochrony budynków, druku, poczty, sprzętu telefonicznego, zaopatrzenia itd.). W wielu przypadkach współpraca ta odbywa się w ramach umów o gwarantowanym poziomie usług, które są regularnie aktualizowane. EIOD w dalszym ciągu brał udział w międzyinstytucjonalnych zaproszeniach do składania ofert, co zwiększało efektywność jego działania w wielu dziedzinach administracji i pozwalało poczynić postępy na drodze ku większej autonomii.

Umowa z Radą Europejską w sprawie usług tłumaczeniowych wygasła w styczniu 2010 r. Nowa umowa została podpisana z Centrum Tłumaczeń dla Organów Unii Europejskiej, które przejęło prace tłumaczeniowe od 2010 r.

EIOD jest członkiem licznych międzyinstytucjonalnych komitetów i grup roboczych, w tym Collège des Chefs d'administration, Comité de Gestion Assurances maladies, Comité de Préparation pour les Questions Statutaires, Comité du Statut, międzyinstytucjonalnej grupy roboczej ds. EAS,

EIOD wykonanie budżetu w ramach międzyinstytucjonalnej współpracy



zarządu EPSO, grupy roboczej ds. EPSO oraz Commission paritaire commune. EIOD jest członkiem Comité de préparation pour les affaires sociales i uczestniczy w doraźnej grupie roboczej ds. wdrażania Konwencji Narodów Zjednoczonych o prawach osób niepełnosprawnych w instytucjach europejskich. Udział w nich pomógł zwiększyć rozpoznawalność EIOD wśród innych instytucji i zachęcał do wymiany dobrych praktyk.

6.6.2. Przepisy wewnętrzne

Przyjmowanie przepisów wewnętrznych niezbędnych do prawidłowego funkcjonowania EIOD to aktualny proces. W tych obszarach, w których EIOD korzysta z pomocy Komisji i Parlamentu Europejskiego, przepisy te są podobne do uregulowań innych instytucji, choć uwzględniają też pewne specyficzne cechy urzędu EIOD.

EIOD jest stosunkowo młodą instytucją, która szybko się rozwija. W konsekwencji przepisy i procedury, które były odpowiednie w pierwszych latach jego działalności, mogą okazać się mniej wydajne w przyszłości, w ramach większej i bardziej złożonej struktury. Przepisy są zatem przedmiotem aktualnej oceny, która może doprowadzić do zmian w nadchodzących latach. Prace rozpoczęto w 2010 r. w celu zmiany kodeksu dobrego postępowania EIOD.

6.6.3. Zarządzanie dokumentami

Przy wsparciu służb Parlamentu Europejskiego w 2009 r. dokonano pomyślnego wdrożenia nowego systemu zarządzania pocztą elektroniczną (GEDA), który wspomaga wykonywanie zadań administracyjnych. Po wykonaniu tego pierwszego kroku podjęto badania w celu pozyskania odpowiedniego systemu zarządzania obiegiem dokumentów i spraw dla działu ochrony danych.

W ciągu 2010 r. opracowano szczegółowy zestaw wymogów operacyjnych dla odpowiedniego systemu zarządzania obiegiem dokumentów i zapisów, obejmującego zarządzanie obiegiem spraw dla EIOD. Zwrócono się do zewnętrznych doradców o przeprowadzenie analizy rynku w oparciu o te potrzeby w celu zidentyfikowania odpowiednich potencjalnych rozwiązań. Dyrekcja Generalna Parlamentu Europejskiego ds. Innowacji i Wsparcia Technologicznego (ITEC) nadal wspiera EIDO i jest dla niego partnerem w tym procesie. Utworzono wewnętrzny zespół ds. projektu prowadzony przez kierownika sektora Rejestr i Wsparcie Operacyjne. Ten multidyscyplinarny zespół obejmował członków reprezentujących pięć różnych sektorów.

Wraz z tym postępem technicznym sektor Rejestr i Wsparcie Operacyjne nadal wdrażał odpowiednie zarządzanie rejestrami. Przyjęto katalogowy system dla czterech z pięciu sektorów, a także udoskonalano procedury rejestracji poprzez uwzględnienie nowej struktury organizacyjnej EIOD. Szczególną uwagę poświęcono wymogom sprawozdawczym zarządu EIOD. Określono szczegółowe informacje dotyczące spraw i pogrupowano je według sektorów w celu udoskonalenia procesu śledzenia ich przebiegu.

7 INSPEKTOR OCHRONY DANYCH (IOD) EIOD

7.1. Nowy zespół IOD w EIOD

Jak w przypadku wszystkich innych instytucji europejskich EIOD podlega szczególnym obowiązkom prawnym w zakresie ochrony danych. Obowiązki te określono w rozporządzeniu o ochronie danych (rozporządzenie (WE) nr 45/2001).

Oprócz określenia zasad prawnych regulujących przetwarzanie danych osobowych przez administrację UE rozporządzenie stanowi, że każda instytucja lub organ europejski musi mianować co najmniej jedną osobę inspektorem ochrony danych (IOD).

We wrześniu 2010 r. EIOD wyznaczył nowego IOD i postanowił wyznaczyć jego zastępcę. Wraz z tymi nominacjami EIOD podjął nowe wysiłki w tym obszarze w celu szybkiego osiągnięcia lepszego poziomu zgodności z przepisami.

Rola IOD w EIOD wiąże się z wieloma wyzwaniami: być niezależnym w ramach niezależnej instytucji, sprostać wysokim oczekiwaniom współpracowników, którzy są szczególnie świadomi kwestii ochrony danych i wrażliwi na nie oraz oferować rozwiązania, które mogą być punktem odniesienia dla innych instytucji.

7.2. Plan działania i przepisy wykonawcze

Nowo wyznaczony zespół IOD rozesłał wśród pracowników całościowy **plan działania** wraz z priorytetami. Plan działania podkreśla cztery główne obszary, na które zespół IOD ma zamiar kłaść największy nacisk: aspekty organizacyjne, funkcja doradcza, informowanie i zwiększanie świadomości.

Pierwszym poważnym krokiem było przyjęcie **przepisów wykonawczych IOD** w październiku 2010 r. Przepisy wykonawcze są oparte na przepisach wykonawczych innych instytucji i wytycznych EIOD, dostosowano je jednak do specyfiki instytucji EIOD. Na przykład gwarancja możliwości odwołania IOD wyłącznie za zgodą EIOD została dostosowana, by wymagała zgody Inspektora i jego zastępcy. Ponadto, w oparciu o dokument w sprawie norm IOD przepisy wykonawcze podkreślają potrzebę solidnej wiedzy na temat ochrony danych oraz niezależność procesu sprawozdawczego.

7.3. Łatwo dostępny rejestr operacji przetwarzania danych

Zespół IOD przeprowadził całościową kontrolę **wykazu istniejących operacji przetwarzania danych** i pracował nad świadomością pracowników, by wszystkie operacje przetwarzania danych w EIOD były zgłaszane. W tym celu zwrócono się do administratorów danych o przygotowanie zaległych powiadomień. Zespół IOD oferował także, w stosownych przypadkach, pomoc w przygotowaniu nowych powiadomień i zamknięciu jeszcze nieukończonych powiadomień.

Wersję elektroniczną rejestru operacji przetwarzania danych udostępniono on-line. Ta elektroniczna

wersja zawiera hyperlink do wszystkich ostatecznych powiadomień, zapewniając w ten sposób łatwy dostęp wszystkim osobom, które chcą wejść do rejestru, zgodnie z art. 26 rozporządzenia o ochronie danych.

Zespół IOD również zaktualizował i udoskonalił formularze powiadomień, które należy stosować przy powiadamianiu o przetwarzaniu danych osobowych w obrębie sekretariatu EIOD.

7.4. Operacja „Wiosna"

Zespół IOD kontynuował najnowszą operację „Wiosna" (zob. pkt 2.5.2), dostarczając EIOD aktualnych informacji na temat zgodności jego instytucji z zasadami ochrony danych. Pismo przesłane do EIOD na początku 2011 r. podkreślało osiągnięte wyniki oraz chęć, w oparciu o plan działania IOD, zapewnienia przestrzegania przepisów i świadomości w zakresie ochrony danych, w szczególności w dziedzinie zasobów ludzkich.

7.5. Informowanie i zwiększanie świadomości

Zespół IOD kładzie duży nacisk na zewnętrzne i wewnętrzne zwiększanie świadomości i informowanie w zakresie zgodności EIOD z zasadami ochrony danych.

W zakresie **komunikacji zewnętrznej** zakładka IOD, zawierająca podstawowe informacje na temat roli i działań IOD, jest obecnie dostępna na stronie internetowej EIOD. Przepisy wykonawcze i rejestr operacji przetwarzania danych EIOD są także dostępne on-line.

Ponadto zespół IOD brał udział w **spotkaniach sieci IOD**, które są jedyną w swoim rodzaju okazją do nawiązania kontaktów, omówienia wspólnych problemów i wymiany dobrych praktyk. Zespół IOD odgrywał również aktywną rolę w działaniach organizowanych w ramach Dnia Ochrony Danych.

W zakresie **komunikacji wewnętrznej** niedawno utworzono Intranet jest doskonałym środkiem komunikacji z pracownikami. Zakładka IOD w Intranecie zawiera informacje, które przysłużą się pracownikom: zarys roli IOD, przepisy wykonawcze, plan działania IOD i informacje o działalności IOD. Zespół IOD ma również zamiar wykorzystać tę wirtualną przestrzeń na wyeksponowanie informacji, które powinno się zapewnić osobom, których dane dotyczą, zgodnie z art. 11 i 12 rozporządzenia. W tym względzie zespół IOD zaczął dostarczać za pośrednictwem Intranetu odniesienia do oświadczeń o ochronie prywatności w zakresie operacji przetwarzania danych mających miejsce w EIOD, w celu zapewnienia łatwego dostępu do nich wszystkim pracownikom.

8 GŁÓWNE CELE NA 2011 r.

Na 2011 r. wybrano poniższe cele. W przyszłym roku zostaną przedstawione osiągnięte wyniki.

8.1. Nadzór i egzekwowanie prawa

Zgodnie z dokumentem strategicznym w sprawie polityki przestrzegania i egzekwowania prawa przyjętym w grudniu 2010 r. EIOD wyznaczył następujące cele w zakresie nadzoru i egzekwowania prawa.

- **Zwiększanie świadomości**

EIOD będzie nadal inwestował czas i środki w zapewnianie porad i wytycznych w zakresie ochrony danych. To zwiększanie świadomości przyjmie formę wytycznych w formie dokumentów dotyczących wybranych zagadnień oraz warsztatów i interaktywnych seminariów, w ramach których EIOD przedstawia swoje stanowisko w danym zakresie.

- **Rola kontroli wstępnych**

Zważywszy, że niemal w całości pozbyto się zaległości w kontrolach wstępnych ex-post, EIOD skoncentruje się na analizie konsekwencji nowych operacji przetwarzania danych. EIOD będzie nadal kładł szczególny nacisk na wdrażanie zaleceń w opiniach dotyczących kontroli wstępnych i zapewniał odpowiednie działania następcze.

- **Monitorowanie i sprawozdawczość**

EIOD będzie kontynuował monitorowanie wdrażania reguł i zasad ochrony danych przez zaangażowane instytucje i organy, poprzez ogólne działanie w zakresie monitorowania (operacja „Wiosna 2011") i ukierunkowanych działań w zakresie monitorowania w sytuacjach, gdy poziom zgodności z przepisami w określonych instytucjach i organach budzi obawy.

- **Kontrole**

Kontrole na miejscu będą organizowane w tych przypadkach, w których EIOD ma poważne powody przypuszczać, że mechanizm zapewniania zgodności z przepisami nie funkcjonuje. Będą one traktowane jako ostatni etap przed oficjalnymi działaniami w zakresie egzekwowania przepisów. Kontrole i audyty będą również organizowane w zakresie wielkoskalowych systemów informatycznych, mieszczących się w zakresie kompetencji EIOD.

8.2. Polityka i konsultacja

Główne cele są zgodne z priorytetami w tym obszarze na 2011 r., opublikowanymi na stronie internetowej. Ponadto sformułowano cele w zakresie współpracy z organami ochrony danych i skoordynowanego nadzoru nad wielkoskalowymi systemami informatycznymi.

- **Zakres konsultacji**

EIOD będzie kontynuował wydawanie na czas opinii i uwag w sprawie wniosków dotyczących nowych przepisów i będzie nadal zapewniał odpowiednie działania następcze w odpowiednich dziedzinach. Jak podkreślono poniżej, szczególny nacisk zostanie położony na przegląd ram prawnych, wdrażanie programu sztokholmskiego i inicjatywy w zakresu technologii.

- **Przegląd ram prawnych**

EIOD potraktuje priorytetowo tworzenie całościowych ram prawnych ochrony danych. Wyda opinię w sprawie komunikatu dotyczącego całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej oraz w sprawie wszelkich powiązanych wniosków ustawodawczych oraz weźmie udział w dyskusji, jeśli będzie to konieczne i stosowne.

- **Wdrażanie programu sztokholmskiego**

EIOD będzie nadal kładł naciski na różne inicjatywy odnoszące się do dalszego wdrażania programu sztokholmskiego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, takie jak ustanowienie systemu wjazdu/wyjazdu i program rejestrowania podróżnych, zaproponowana dyrektywa w sprawie wykorzystania PNR do celów egzekwowania prawa i wprowadzenie europejskiego TFTP.

- **Inicjatywy z zakresu technologii**

Inicjatywy z zakresu technologii, które mogą mieć wpływ na prywatność i ochronę danych, zostaną również dogłębnie rozważone przez EIOD w 2011 r. W szczególności EIOD będzie nadal monitorował wdrażanie elementów technologii informacyjnej Europe 2020 przewidzianych w agendzie cyfrowej, takich jak RFID, obliczenia rozproszone, administracja elektroniczna i egzekwowanie on-line praw własności intelektualnej.

- **Inne inicjatywy**

EIOD skoncentruje się na wszystkich innych inicjatywach, które mogą znacząco wpływać na ochronę danych, takie jak inicjatywy w dziedzinie transportu (np. wykorzystanie skanerów ciała w portach lotniczych, pakiety dotyczące e-mobilności) oraz wielkoskalowa wymiana danych, która może mieć miejsce w systemie wymiany informacji na rynku wewnętrznym.

- **Współpraca z organami ochrony danych**

EIOD będzie nadal miał swój udział w działalności i sukcesie Grupy Roboczej ds. Ochrony Danych Art. 29 poprzez: dostosowywanie jej programu prac do priorytetów EIOD, zapewnianie spójności i synergii pomiędzy Grupą Roboczą a stanowiskami EIOD, podtrzymywanie konstruktywnych relacji z krajowymi organami ochrony danych. Jako sprawozdawca ds. określonych spraw EIOD będzie kierował przyjęciem odnośnych opinii Grupy Roboczej Art. 29 i będzie je przygotowywał.

- **Skoordynowany nadzór**

Prawo UE wymaga skoordynowanego nadzoru dla Eurodac, systemu informacji celnej, a od połowy 2011 r. – dla wizowego systemu informacyjnego. Ważnym celem dla EIOD będzie zapewnienie organom ochrony danych zaangażowanym w skoordynowany nadzór wydajnego sekretariatu. Jako nadzorca wielkoskalowych systemów informatycznych EIOD będzie także aktywnie uczestniczył w ich skoordynowanym nadzorze i będzie przeprowadzał regularne audyty bezpieczeństwa.

8.3. Inne dziedziny

- **Informacja i komunikacja**

Będą kontynuowane działania informacyjno-komunikacyjne i prasowe, których celem jest tworzenie i doskonalenie, ze szczególnym naciskiem na zwiększanie świadomości, publikacji i informacji on-line. EIOD przygotuje także podłoże pod przegląd strategii komunikacji, w szczególności poprzez konsultację z głównymi stronami zainteresowanymi. To ogólne działanie zostanie uzupełnione o bardziej ukierunkowane oceny skutków głównych narzędzi informacyjno-komunikacyjnych.

- **Organizacja wewnętrzna**

Głównym celem na 2011 r. będzie zakończenie wewnętrznej reorganizacji, odnowienie wysiłków w kierunku zarządzania wynikami w kontekście strategicznego przeglądu oraz rozwój i wdrożenie nowych narzędzi IT. Szczególny nacisk będzie położony na kontrolę i procedury wewnętrzne, lepszą alokację zasobów i lepsze wykonanie budżetu.

- **Zarządzanie zasobami**

EIOD będzie nadal inwestował zasoby w tworzenie i wdrażanie systemu zarządzania obiegiem spraw.

Priorytetowo zostanie także potraktowane zawarcie z Komisją Europejską umów o gwarantowanym poziomie usług w zakresie tworzenia aplikacji IT w dziedzinie zasobów ludzkich (np. Syslog Formation, systemy przetwarzania Sysper i Mission).

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 mają zastosowanie również do instytucji i organów wspólnotowych oraz że należy ustanowić niezależny organ nadzoru.

Aktami wspólnotowymi, o których mowa w tym przepisie, jest dyrektywa 95/46/WE ustanawiająca ogólne ramy dla przepisów dotyczących ochrony danych w państwach członkowskich oraz dyrektywa 97/66/WE – dyrektywa sektorowa zastąpiona przez dyrektywę 2002/58/WE o prywatności i łączności elektronicznej. Obie te dyrektywy można uznać za wynik procesu prawnego, który rozpoczął się na początku lat siedemdziesiątych na forum Rady Europy (zob. poniżej).

Na podstawie art. 286 TWE, rozporządzeniem (WE) nr 45/2001 Parlamentu Europejskiego i Rady o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, które weszło w życie w 2001 r. ustanowiono urząd Europejskiego Inspektora Ochrony Danych([23]). W rozporządzeniu ustanowiono też stosowne zasady dla instytucji i organów zgodnie z przepisami obydwu dyrektyw.

Od chwili wejścia w życie traktatu lizbońskiego wspomniany powyżej art. 286 został zastąpiony przez art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, który podkreśla znaczenie ochrony danych osobowych w sposób bardziej ogólny. Zarówno art. 16 TFUE, jak i art. 8 Karty praw podstawowych UE – obecnie wiążącej – stanowią, że zgodność z zasadami ochrony danych powinna podlegać kontroli niezależnego organu.

Informacje ogólne

Artykuł 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności przewiduje prawo do poszanowania życia prywatnego i rodzinnego, którego ograniczenia są dozwolone wyłącznie pod pewnymi warunkami. W 1981 r. za konieczne uznano jednak przyjęcie osobnej konwencji o ochronie danych w celu wypracowania pozytywnego, strukturalnego podejścia do ochrony podstawowych praw i wolności, na które może mieć wpływ przetwarzanie danych osobowych w nowoczesnym społeczeństwie. Konwencję tę, znaną również jako Konwencja nr 108, ratyfikowało ponad 40 państw członkowskich Rady Europy, w tym wszystkie państwa członkowskie UE.

Dyrektywa 95/46/WE została oparta na zasadach określonych w Konwencji nr 108, precyzując je jednak i rozwijając pod wieloma względami. Jej celem było zagwarantowanie wysokiego poziomu ochrony danych osobowych i ich swobodnego przepływu w obrębie UE. W złożonym na początku lat dziewięćdziesiątych przez Komisję wniosku w sprawie tej dyrektywy oświadczono, że instytucje i organy Wspólnoty powinny być objęte podobnymi zabezpieczeniami prawnymi, by mogły uczestniczyć w swobodnym przepływie danych osobowych, z zastrzeżeniem przestrzegania przez nie równoważnych zasad ochrony. Do czasu przyjęcia art. 286 TWE brak było jednak podstaw prawnych dla takiego rozwiązania.

Traktat lizboński, który wszedł w życie w dniu 1 grudnia 2009 r., zwiększa pod różnymi względami ochronę praw podstawowych. Poszanowanie życia prywatnego i rodzinnego oraz ochrona danych osobowych są traktowane jako odrębne prawa podstawowe wymienione w art. 7 i 8 Karty praw podstawowych, która jest teraz wiążąca prawnie zarówno dla instytucji i organów wspólnotowych, jak i dla państw członkowskich UE stosujących prawo unijne. Ochrony danych osobowych jako zagadnienia horyzontalnego dotyczy również art. 16 TFUE. Wynika z tego jasno, że ochrona danych jest uznawana za jeden z podstawowych składników „dobrej administracji". Zasadniczą częścią tej ochrony jest niezależny nadzór.

Rozporządzenie (WE) nr 45/2001

Przyglądając się uważniej rozporządzeniu, należy po pierwsze odnotować, że zgodnie z art. 3 ust. 1 ma ono zastosowanie do „przetwarzania danych osobowych przez [wszystkie] instytucje i organy

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

wspólnotowe, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu". Jednakże, od chwili wejścia w życie traktatu lizbońskiego i zniesienia struktury filarowej, w wyniku czego odniesienia do „instytucji wspólnotowych" i „prawa wspólnotowego" stały się nieaktualne – rozporządzenie co do zasady obejmuje wszystkie instytucje i organy UE, z wyjątkiem przypadków, gdy inne akty UE stanowią inaczej. Dokładnie skutki tych zmian są wciąż badane i mogą wymagać dalszych wyjaśnień.

Definicje zawarte w rozporządzeniu i jego treść są spójne z podejściem przyjętym w dyrektywie 95/46/WE. Można stwierdzić, że rozporządzenie (WE) nr 45/2001 stanowi wdrożenie tej dyrektywy na szczeblu europejskim. Oznacza to, że rozporządzenie dotyczy zasad ogólnych, takich jak rzetelne i zgodne z prawem przetwarzanie, proporcjonalność i użycie zgodne z przyjętymi celami, szczególne kategorie danych szczególnie chronionych, informacje przekazywane osobie, której dane dotyczą, prawa osoby, której dane dotyczą, obowiązki administratorów danych – uwzględniając w stosownych przypadkach szczególne okoliczności na szczeblu UE – a także nadzoru, egzekwowania prawa i środków zaradczych. Oddzielny rozdział dotyczy ochrony danych osobowych i prywatności w kontekście wewnętrznych sieci telekomunikacyjnych. Rozdział ten wdraża na szczeblu europejskim uchyloną dyrektywę 97/66/WE o prywatności i łączności elektronicznej.

Ciekawym aspektem tego rozporządzenia jest zobowiązanie instytucji i organów UE do wyznaczenia co najmniej jednej osoby jako inspektora ochrony danych. Zadaniem inspektorów jest zapewnienie w niezależny sposób wewnętrznego stosowania przepisów rozporządzenia, w tym właściwego powiadamiania o operacjach przetwarzania. Inspektorzy tacy są już obecni we wszystkich instytucjach i w większości organów; niektórzy z nich działają od wielu lat. Oznacza to, że pomimo braku organu nadzorczego poczyniono istotne kroki zmierzające do wdrożenia rozporządzenia. Inspektorom tym może także być łatwiej doradzać lub interweniować na wczesnym etapie, jak również pomagać w wypracowywaniu dobrych praktyk. Ponieważ formalnym obowiązkiem inspektora ochrony danych jest współpraca z EIOD, współdziałanie w ramach sieci współpracy oraz jej rozwój są bardzo istotne i wartościowe (zob. pkt 2.2).

Zadania i uprawnienia EIOD

Zadania oraz uprawnienia EIOD zostały wyraźnie określone w art. 41, 46 i 47 rozporządzenia (zob. załącznik B) zarówno w ujęciu ogólnym, jak i szczegółowym. W art. 41 określono 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 w ogólnym zarysie konkretne elementy misji EIOD. W art. 46 i 47 rozwinięto oraz sprecyzowano jego ogólne zadania, określając szczegółowy wykaz obowiązków i uprawnień.

Przedstawione zadania, obowiązki i uprawnienia są zasadniczo zgodne z wyznaczonymi w przypadku krajowych organów nadzorczych: obejmują one wysłuchiwanie i badanie skarg, prowadzenie innych dochodzeń, informowanie administratorów danych oraz osób, których dane dotyczą, przeprowadzanie kontroli wstępnych w przypadkach, gdy operacje przetwarzania wiążą się z konkretnym zagrożeniem itp. Rozporządzenie uprawnia EIOD do uzyskania dostępu do stosownych informacji i pomieszczeń, w przypadku gdy jest to niezbędne dla prowadzonych dochodzeń. Może on również nakładać kary i kierować sprawy do Trybunału Sprawiedliwości. Te czynności nadzorcze omówiono bardziej szczegółowo w rozdziale 2 niniejszego sprawozdania.

Część zadań EIOD ma charakter szczególny. Zadanie polegające na doradzaniu Komisji i innym instytucjom w zakresie nowego prawodawstwa, podkreślone w art. 28 ust. 2 przez nałożenie na Komisję formalnego obowiązku konsultowania się z EIOD przy przyjmowaniu wniosków ustawodawczych odnoszących się do ochrony danych osobowych, dotyczy także projektów dyrektyw i innych środków, które mają mieć zastosowanie na szczeblu krajowym lub mają być wdrażane w prawie krajowym. Jest to zadanie o charakterze strategicznym umożliwiające EIOD badanie konsekwencji z punktu widzenia prywatności na wczesnym etapie oraz omówienie możliwych rozwiązań alternatywnych, również w ramach dawnego „trzeciego filaru" (współpraca policyjna i sądowa w sprawach karnych). Ważnymi zadaniami jest też monitorowanie wydarzeń, które mogą mieć wpływ na ochronę danych osobowych, oraz interwencje w sprawach rozpatrywanych przez Trybunał Sprawiedliwości. Te czynności konsultacyjne EIOD omówiono szerzej w rozdziale 3 niniejszego sprawozdania.

Podobne znaczenie ma obowiązek współpracy z krajowymi organami nadzorczymi oraz organami nadzorczymi działającymi w obrębie dawnego „trzeciego filaru". Jako członek Grupy Roboczej Art. 29 (Grupy Roboczej ds. Ochrony Danych) powołanej w celu doradzania Komisji Europejskiej oraz formułowania zharmonizowanej polityki EIOD ma możliwość wnoszenia wkładu również na tym szczeblu. Współpraca z organami nadzorczymi działającymi w dawnym „trzecim filarze" umożliwia EIOD śledzenie rozwoju sytuacji w tym zakresie, a także przyczynienie się do wypracowania jednolitych i spójnych ram ochrony danych osobowych niezależnie od konkretnego „filaru" lub kontekstu. Tę współpracę omówiono szerzej w rozdziale 4 niniejszego sprawozdania.

Załącznik B – Fragment rozporządzenia (WE) nr 45/2001

Art. 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.

Art. 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.

Art. 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

ACTA	Umowa handlowa dotycząca zwalczania obrotu towarami podrobionymi
CIS	System informacji celnej
ETO	Trybunał Obrachunkowy
KR	Komitet Regionów
CPAS	*Comité de Préparation pour les Affaires Sociales*
DAS	Deklaracja wiarygodności
DG INFSO	Dyrekcja Generalna ds. Społeczeństwa Informacyjnego i Mediów
DG MARKT	Dyrekcja Generalna ds. Rynku Wewnętrznego i Usług
DIGIT	Dyrekcja Generalna ds. Informatyki
DPA	Organy Ochrony Danych
DPC	Koordynator Ochrony Danych

IOD	Inspektor Ochrony Danych
EAS	Europejska Szkoła Administracji
EASA	Europejska Agencja Bezpieczeństwa Lotniczego
WE	Wspólnoty Europejskie
EBC	Europejski Bank Centralny
ECDC	Europejskie Centrum ds. Zapobiegania i Kontroli Chorób
ETS	Trybunał Sprawiedliwości
EEA	Europejska Agencja Środowiska
EFSA	Europejski Urząd ds. Bezpieczeństwa Żywności
EBI	Europejski Bank Inwestycyjny
EIO	Europejski nakaz dochodzeniowy
ENISA	Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji
EKPC	Europejska konwencja praw człowieka
EPO	Europejski nakaz ochrony
EPSO	Europejski Urząd Doboru Kadr
ERCEA	Agencja Wykonawcza Europejskiej Rady ds. Badań Naukowych
UE	Unia Europejska
EWRS	System wczesnego ostrzegania i reagowania
FRA	Agencja Praw Podstawowych Unii Europejskiej
HR	Zasoby ludzkie
IAS	Służba Audytu Wewnętrznego
TIK	Technologie informacyjno-komunikacyjne
IMI	System wymiany informacji na rynku wewnętrznym
IOM	Międzynarodowa Organizacja ds. Migracji
ISS	Strategia bezpieczeństwa wewnętrznego
IT	Technologia informacyjna
JRC	Wspólne Centrum Badawcze
JRO	Wspólne działania dotyczące powrotów
JSB	Wspólny organ nadzorczy
JSIMC	Wspólny Komitet ds. Zarządzania Ubezpieczeniami Zdrowotnymi
LIBE	Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego
LISO	Lokalny inspektor bezpieczeństwa danych
LSO	Lokalny inspektor bezpieczeństwa
UHRW	Urząd Harmonizacji Rynku Wewnętrznego
OLAF	Europejski Urząd ds. Zwalczania Nadużyć Finansowych
PNR	Dane dotyczące przelotu pasażera
B+R	Badania i rozwój
RFID	Identyfikacja radiowa
SIS	System informacyjny Schengen
SNE	Oddelegowany ekspert krajowy
SOC	Centrum Usługowo-Operacyjne
s-TESTA	Bezpieczne transeuropejskie usługi telematyczne między administracjami
SWIFT	Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych
TFTP	Program śledzenia środków finansowych należących do terrorystów
TFUE	Traktat o funkcjonowaniu Unii Europejskiej

TURBINE	Pewne odwołalne tożsamości biometryczne
UNHCR	Wysoki Komisarz Narodów Zjednoczonych ds. Uchodźców
VIS	Wizowy system informacyjny
WCO	Światowa Organizacja Celna
WP 29	Grupa Robocza Art. 29 ds. Ochrony Danych
WPPJ	Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości

Załącznik D – Wykaz inspektorów ochrony danych

ORGANIZACJA	IMIĘ I NAZWISKO	E MAIL
Parlament Europejski (PE)	Jonathan STEELE	Data-Protection@europarl.europa.eu
Rada Unii Europejskiej (Consilium)	Pierre VERNHES	Data.Protection@consilium.europa.eu
Komisja Europejska (KE)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Trybunał Sprawiedliwości Wspólnot Europejskich (CURIA)	Marc SCHAUSS	Dataprotectionofficer@curia.europa.eu
Trybunał Obrachunkowy (ETO)	Johan VAN DAMME	Data-Protection@eca.europa.eu
Europejski Komitet Ekonomiczno-Społeczny (EKES)	Maria ARSENE	Data.Protection@eesc.europa.eu
Komitet Regionów (KR)	Rastislav SPÁC	Data.Protection@cor.europa.eu
Europejski Bank Inwestycyjny (EBI)	Jean-Philippe MINNAERT	Dataprotectionofficer@eib.org
Europejski Rzecznik Praw Obywatelskich	Loïc JULIEN	DPO-euro-ombudsman@ombudsman.europa.eu
Europejski Inspektor Ochrony Danych (EIOD)	Alfonso SCIROCCO, Sylvie PICARD (Zastępca Inspektora)	alfonso.scirocco@edps.europa.eu
Europejski Bank Centralny (EBC)	Frederik MALFRÈRE	DPO@ecb.int
Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF)	Laraine LAUDATI	Laraine.Laudati@ec.europa.eu
Centrum Tłumaczeń dla Organów Unii Europejskiej (CDT)	Benoît VITALE	Data-Protection@cdt.europa.eu
Urząd Harmonizacji Rynku Wewnętrznego (UHRW)	Ignacio DE MEDRANO CABALLERO	DataProtectionOfficer@oami.europa.eu
Agencja Praw Podstawowych Unii Europejskiej (FRA)	Nikolaos FIKATAS	Nikolaos.Fikatas@fra.europa.eu
Europejska Agencja Leków (EMEA)	Vincenzo SALVATORE	Data.Protection@emea.europa.eu
Wspólnotowy Urząd Ochrony Odmian Roślin (CPVO)	Véronique DOREAU	Doreau@cpvo.europa.eu
Europejska Fundacja Kształcenia (ETF)	Liia KAARLOP	Liia.Kaarlop@etf.europa.eu
Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA)	Emmanuel MAURAGE	Dataprotection@enisa.europa.eu
Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy (Eurofund)	Markus GRIMMEISEN	MGR@eurofound.europa.eu
Europäische Beobachtungsstelle für Drogen und Drogensucht (EBDD)	Cecile MARTEL	Cecile.Martel@emcdda.europa.eu

>>>

ORGANIZACJA	IMIĘ I NAZWISKO	E MAIL
Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu
Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA)	Małlgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.europa.eu
Europejska Agencja ds. Bezpieczeństwa na Morzu (EMSA)	Spyros ANTONIOU	Spyros.Antoniou@cedefop.europa.eu
Europejskie Centrum Rozwoju Kształcenia Zawodowego (Cedefop)	Hubert MONET	eacea-data-protection@ec.europa.eu
Agencja Wykonawcza ds. Edukacji, Kultury i Sektora Audiowizualnego (EACEA)	Terry TAYLOR	Taylor@osha.europa.eu
Europejska Agencja ds. Bezpieczeństwa Zdrowia w Pracy (OSHA)	Clara FERNANDEZ/Rieke ARNDT	cfca-dpo@cfca.europa.eu
Wspólnotowa Agencja Kontroli Rybołówstwa (CFCA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Organ Nadzoru Europejskiego GNSS (GSA)	Guido STÄRKLE (p.o. inspektora ochrony danych)	Dataprotectionofficer@era.europa.eu
Europejska Agencja Kolejowa (ERA)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Agencja Wykonawcza ds. Zdrowia i Konsumentów (EAHC)	Elisabeth ROBINO	Elisabeth.Robino@ecdc.europa.eu
Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC)	Gordon McINNES	Gordon.McInnes@eea.europa.eu
Europejska Agencja Środowiska (EAA)	Jobst NEUSS	J.Neuss@eif.org
Europejski Fundusz Inwestycyjny (EFI)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
Europejska Agencja Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach (Frontex)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Europejska Agencja Bezpieczeństwa Lotniczego (EASA)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Agencja Wykonawcza ds. Konkurencyjności i Innowacyjności (EACI)	Zsófia SZILVÁSSY	Zsofia.Szilvassy@ec.europa.eu
Agencja Wykonawcza ds. Transeuropejskiej Sieci Transportowej (TEN-T EA)	Alain LEFÈBVRE	Minna.Heikkila@echa.europa.eu
Europejska Agencja Chemikaliów (ECHA)	Donatella PIATTO	Donatella.Piatto@ec.europa.eu
Agencja Wykonawcza ds. Badań Naukowych (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu

>>>

ORGANIZACJA	IMIĘ I NAZWISKO	E MAIL
Fusion for Energy (Europejskie Wspólne Przedsięwzięcie na rzecz Realizacji Projektu ITER i Rozwoju Energii Termojądrowej)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu
Wspólne przedsięwzięcie SESAR	Daniella PAVKOVIC	Daniella.Pavkovic@sesarju.eu
Wspólne przedsiębiorstwo ARTEMIS	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Wspólne przedsiębiorstwo „czyste niebo”	Silvia POLIDORI	Silvia.Polidori@cleansky.eu
Inicjatywa w zakresie leków innowacyjnych (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Wspólne przedsięwzięcie na rzecz ogniw paliwowych i technologii wodorowych	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu
Europejski Instytut Innowacji i Technologii (EIT)	Camilo SOARES	Camilo.Soares@ext.ec.europa.eu

Załącznik E – Wykaz opinii wydanych w wyniku kontroli wstępnej

Empiryczna analiza korelacji pomiędzy zmiennymi systemu pracy a procesem decyzyjnym – UHRW

Opinia z dnia 22 listopada 2010 r. w sprawie „Empirycznej analizy korelacji pomiędzy zmiennymi systemu pracy a procesem decyzyjnym" zgłoszona przez Urząd Harmonizacji Rynku Wewnętrznego („UHRW") w dniu 22 lipca 2010 r. (sprawa 2010-0468)

Procédures relatives au recrutement d'agents - BEI

Avis du 11 novembre 2010 sur la notification d'un contrôle préalable concernant les procédures relatives au recrutement d'agents (Dossier 2009-0254)

Procedura rekrutacji i aplikacja e-Recruitment – EASA

Pismo z dnia 19 października 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie „Procedury rekrutacji i aplikacji e-Recruitment" (sprawa 2010-0466)

Procedury odnoszące się do dochodzeń w sprawie nadużyć finansowych – EBI

Opinia z dnia 14 października 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie procedur odnoszących się do dochodzeń w sprawie nadużyć finansowych w grupie EBI (sprawa 2009-0459)

Oddelegowanie krajowych ekspertów – KR

Pismo z dnia 5 października 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie oddelegowania krajowych ekspertów do Komitetu Regionów (sprawa 2010-0515)

Przetwarzanie danych osobowych w ramach obniżenia pensji w razie strajku – EBC

Opinia z dnia 28 września 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie przetwarzania danych osobowych w ramach obniżenia pensji w razie strajku (sprawa 2009-0514)

Selekcja i rekrutacja personelu – EAHC

Pismo z dnia 24 września 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie selekcji i rekrutacji personelu (tymczasowi pracownicy oddelegowani lub nie z Komisji Europejskiej, pracownicy kontraktowi, personel tymczasowy i stażyści) w Agencji Wykonawczej ds. Zdrowia i Konsumentów (sprawa 2010-0346)

Selekcja zewnętrznych korektorów – Komisja (Biuro Publikacji)

Opinia z dnia 6 września 2010 r. w sprawie powiadomienia o kontroli wstępnej od inspektora danych osobowych Komisji Europejskiej w zakresie „Listy uczestników egzaminów na korektorów do pracy kontraktowej" (sprawa 2010-400)

Kontrole bezpieczeństwa – Komisja (DG JRC w Isprze)

Opinia z dnia 6 września 2010 r. w sprawie powiadomienia o kontroli wstępnej od inspektora danych osobowych Komisji Europejskiej w zakresie „Kontroli bezpieczeństwa w siedzibie JRC w Isprze" (sprawa 2009-682)

Europejski system nadzoru („TESSy") – ECDC

Opinia z dnia 3 września 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie europejskiego systemu nadzoru („TESSy") Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób („ECDC") (sprawa 2009-0474)

Polityka ochrony godności osoby i zapobiegania mobbingowi i molestowaniu seksualnemu – EASA

Opinia z dnia 29 lipca w sprawie powiadomienia o kontroli wstępnej w zakresie „Polityki EASA ochrony godności osoby i zapobiegania mobbingowi i molestowaniu seksualnemu" (sprawa 201—318)

Wdrożenie nieformalnej procedury postępowania w sprawach mobbingu i molestowania seksualnego – EKES

Opinia z dnia 28 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie „Wdrożenia nieformalnej procedury postępowania w sprawach mobbingu i molestowania seksualnego w Komitecie" (sprawa 2010-321)

Selekcja i rekrutacja pracowników tymczasowych i kontraktowych, oddelegowanych krajowych ekspertów i stażystów – ECHA

Pismo z dnia 27 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie selekcji i rekrutacji pracowników tymczasowych i kontraktowych, oddelegowanych ekspertów krajowych i stażystów (sprawa 2010-0109)

Przetwarzanie danych osobowych w kontekście procesu monitorowania jakości – Rada

Opinia z dnia 26 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie przetwarzania danych osobowych w kontekście procesu monitorowania jakości (sprawa 2009-0295)

Administracyjne działania następcze w odniesieniu do nieusprawiedliwionych nieobecności z powodu choroby – Rada

Opinia z dnia 22 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej akt „administracyjne działania następcze w odniesieniu do nieusprawiedliwionych nieobecności z powodu choroby (sprawa 2009-0687)

Procedura poświadczeń dla urzędników – EMCDDA

Pismo z dnia 22 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie przetwarzania danych związanego z procedurą poświadczeń dla urzędników EMCDDA (sprawa 2010-0407)

Procedury odnoszące się do „raportu z informacją zwrotną 360° Leadership" – EBI

Opinia z dnia 20 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej procedur odnoszących się do „raportu z informacją zwrotną 360° Leadership" (sprawa 2009-0215)

Procedura promocji dla pracowników i urzędników – EKES

Opina z dnia 19 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej „procedury promocji dla pracowników i urzędników" (sprawa 2008-474)

Selekcja i rekrutacja personelu tymczasowego – Europejski Bank Inwestycyjny – EBI

Pismo z dnia 14 lipca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie selekcji i rekrutacji personelu tymczasowego (sprawa 2009-0678)

Wejścia do centralnej bazy danych o wykluczeniach i jej aktualizacja – Komitet Regionów

Opinia z dnia 4 czerwca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie dokumentacji „Procedury do zastosowania przy konsultacji i uaktualnianiu centralnej bazy danych o wykluczeniach" (sprawa 2010-248)

Procedura postępowania w przypadkach niekompetencji – Rada

Opinia z dnia 4 czerwca 2010 r., w sprawie powiadomienia o kontroli wstępnej w zakresie „procedury postępowania w przypadkach niekompetencji w Sekretariacie Generalnym Rady" (sprawa 2010-237)

Zarządzanie zewnętrznymi tłumaczeniami wykonywanymi przez DG TRAD i ich ocena – Parlament

Opinia z dnia 4 czerwca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie „zarządzania zewnętrznymi tłumaczemiami wykonywanymi przez DG TRAD i ich oceny" (sprawa 2009-0827)

Procedura selekcji pracowników tymczasowych – Komisja

Opinia z dnia 4 czerwca 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie procedury selekcji pracowników tymczasowych (sprawa 2008-704)

Rejestrowanie osób, których dane dotyczą, w centralnej bazie danych o wykluczeniach – Komisja

Opinia z dnia 26 maja 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie przetwarzania danych osobowych w przypadku „rejestrowania osób, których dane dotyczą, w centralnej bazie danych o wykluczeniach (sprawa 2009-0681)

Procedura wyznaczania dyrektorów generalnych, dyrektorów i kierowników działów – Parlament Europejski

Opinia z dnia 20 maja 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie procedury wyznaczania dyrektorów generalnych, dyrektorów i kierowników działów (sprawa 2010-0270)

Rekrutacja oddelegowanych ekspertów krajowych i stażystów – Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC)

Pismo z dnia 19 maja 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej rekrutacji oddelegowanych ekspertów krajowych i stażystów (sprawa 2009-0453)

Rekrutacja pracowników tymczasowych i kontraktowych – Europejska Agencja Środowiska (EEA)

Pismo z dnia 19 maja 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej rekrutacji pracowników tymczasowych i kontraktowych (sprawa 2009-0467)

Wsparcie psychospołeczne i finansowe – Wspólne Centrum Badawcze (JRC)

Opinia z dnia 10 maja 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej wsparcia psychospołecznego i finansowego dla Wspólnego Centrum Badawczego (JRC ITU) w Karlsruhe (sprawa 2008-713)

Gromadzenie imion i nazwisk oraz wybranych innych odnośnych danych powracających w ramach działań dotyczących łączonych powrotów – FRONTEX

Opinia z dnia 26 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej „gromadzenia imion i nazwisk oraz wybranych innych odnośnych danych powracających w ramach wspólnych działań dotyczących powrotów" (sprawa 2009-0281)

System wczesnego ostrzegania i reagowania („EWRS") – Komisja Europejska

Opinia z dnia 26 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej w zakresie systemu wczesnego ostrzegania i reagowania („EWRS") (sprawa 2009-0137)

Promocja wewnętrzna urzędników i reklasyfikacja pracowników tymczasowych – EMCDDA

Opinia z dnia 22 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej „wewnętrznej promocji urzędników i reklasyfikacji pracowników tymczasowych (sprawa 2009-0839)

Przetwarzanie danych w celu zarządzania zaproszeniami do składania ofert – ETF

Opinia z dnia 22 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej przetwarzania danych w celu zarządzania zaproszeniami do składania ofert (sprawa 2009-0037)

Postępowanie z niekompetencją zawodową – Trybunał Sprawiedliwości

Opinia z dnia 21 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej „procedury postępowania z niekompetencją zawodową" (sprawa 2009-860)

Dochodzenia administracyjne i postępowania dyscyplinarne – EMA

Opinia z dnia 21 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej przetwarzania danych osobowych w dochodzeniach administracyjnych i postępowaniach dyscyplinarnych (sprawa 2010-0047)

Procedury zaopatrzenia i wezwanie do wyrażenia zainteresowania dla wyboru ekspertów – Komisja

Opinia z dnia 15 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej procedury zaopatrzenia i wezwania do wyrażenia zainteresowania dla wyboru ekspertów (sprawa 2009-570)

Skuteczność przywództwa – Komisja

Opinia z dnia 7 kwietnia 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej „skuteczności przywództwa" (sprawa 2010-0002)

Procédures de sélection du personnel par des panels - EBI

Avis du 26 mars 2010 sur la notification d'un contrôle préalable à propos du dossier «procédures relatives à la sélection du personnel par des panels» (sprawa 2009-679)

Zarządzanie urlopami – Parlament

Opinia z dnia 25 marca 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej zarządzania urlopami (sprawa 2009-595)

Ręczne wypełnianie dokumentów gości związanych z niepełnosprawnością – Parlament Europejski

Opinia z dnia 16 marca 2010 r. w sprawie powiadomienia o kontroli wstępnej dotyczącej ręcznego wypełniania dokumentów gości związanych z niepełnosprawnością (sprawa 2009-564)

Wewnętrzne procedury mobilności – UHRW

Opinia z dnia 15 marca 2010 r. w sprawie powiadomienia o kontroli wstępnej otrzymanego od inspektora danych osobowych Urzędu Harmonizacji Rynku Wewnętrznego w zakresie wewnętrznej mobilności (sprawa 2008-426)

EAS – role zespołowe Belbina - Komisja Europejska

Opinia z dnia 15 marca 2010 r. w sprawie powiadomienia otrzymanego od inspektora danych osobowych Komisji Europejskiej dotyczącego „EAS – role zespołowe Belbina" (sprawa 2009-377)

Ocena wyników - EMCDDA

Opinia wyrażona w piśmie z dnia 8 marca 2010 r. w sprawie powiadomienia dotyczącego oceny wyników (sprawa 2009-838)

Zarządzanie nieobecnościami i zwolnieniami chorobowymi – EKES

Opinia z dnia 5 marca 2010 r. w sprawie powiadomienia dotyczącego zarządzania nieobecnościami i chorobowymi przy użyciu bazy danych „Centurio" (połączone sprawy 2009-0702 i 2009-0703)

Selekcja tajnych doradców – FRA

Opinia z dnia 10 lutego 2010 r. w sprawie powiadomienia dotyczącego procedur selekcji tajnych doradców (sprawa 2009-857)

Wyznaczenie kadry zarządzającej średniego szczebla – Wspólnotowy Urząd Ochrony Odmian Roślin (CPVO)

Opinia z dnia 28 stycznia 2010 r. w sprawie powiadomienia dotyczącego wyznaczenia średniej kadry zarządzającej (sprawa 2009-0666)

E-probation – Europejski Bank Inwestycyjny

Opinia z dnia 21 stycznia 2010 r. w sprawie powiadomienia dotyczącego przetwarzania danych osobowych w ramach zarządzania okresami próbnymi (e-probation) (sprawa 2009-716)

Skargi od członków – Komitet Zarządzania Ubezpieczeniami Chorobowymi

Opinia z dnia 18 stycznia 2010 r. w sprawie powiadomienia otrzymanego od Komitetu Zarządzania Ubezpieczeniami Chorobowymi w zakresie sprawy „skarg od członków" (sprawa 2009-070)

Dostęp do prywatnych dysków i e-maili – Trybunał Obrachunkowy

Opinia z dnia 18 stycznia 2010 r. w sprawie powiadomienia dotyczącego „procedury dostępu do prywatnych dysków i e-maili" (sprawa 2009-716)

Załącznik F – Wykaz opinii w sprawie wniosków ustawodawczych

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA)

Opinia z dnia 20 grudnia 2010 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA)

Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy

Opinia z dnia 17 grudnia 2010 r. dotycząca komunikatu Komisji – „Strategia bezpieczeństwa wewnętrznego UE w działaniu: Pięć kroków w kierunku bezpieczniejszej Europy"

EURODAC

Opinia z dnia 15 grudnia 2010 r. w sprawie ustanowienia systemu EURODAC do porównywania odcisków palców

Wniosek dotyczący rozporządzenia w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych

Opinia z dnia 15 grudnia 2010 r. na temat wniosku dotyczącego rozporządzenia w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych

Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania

Opinia z dnia 24 listopada 2010 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady – „Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania"

Globalne podejście do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim

Opinia z dnia 19 października 2010 r. dotycząca globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim

Europejski nakaz ochrony i europejski nakaz dochodzenia w sprawach karnych

Opinia z dnia 5 października 2010 r. w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzenia w sprawach karnych

Zarządzanie informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości

Opinia z dnia 30 września 2010 r. dotycząca komunikatu Komisji do Parlamentu Europejskiego i Rady – „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości"

Systemy gwarancji depozytów

Opinia z dnia 9 września 2010 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie systemów ochrony depozytów (wersja przekształcona)

Przetwarzanie i przekazywanie danych z komunikatów finansowych przez Unię Europejską Stanom Zjednoczonym do celów Programu śledzenia środków finansowych należących do terrorystów (TFTP II)

Opinia z dnia 22 lipca 2010 r. na temat wniosku dotyczącego decyzji Rady w sprawie zawarcia Umowy między Unią Europejską i Stanami Zjednoczonymi w sprawie przetwarzania i przekazywania danych z komunikatów finansowych przez Unię Europejską Stanom Zjednoczonym do celów Programu śledzenia środków finansowych należących do terrorystów (TFTP II)

Europejska Agencja Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej (FRONTEX)

Opinia z dnia 17 maja 2010 r. dotycząca wniosku w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 2007/2004 ustanawiające Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej (FRONTEX)

Niegodziwe traktowanie dzieci w celach seksualnych i pornografia dziecięca

Opinia z dnia 10 maja 2010 r. na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, uchylającej decyzję ramową 2004/68/JHA

Inicjatywa obywatelska

Opinia z dnia 21 kwietnia 2010 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie inicjatywy obywatelskiej

Zużyty sprzęt elektryczny i elektroniczny (WEEE)

Opinia z dnia 14 kwietnia 2010 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE)

Wspieranie zaufania w społeczeństwie informacyjnym

Opinia z dnia 18 marca 2010 r. w sprawie wspierania zaufania w społeczeństwie informacyjnym poprzez działanie na rzecz ochrony danych i prywatności

Wspólny Komitet Współpracy Celnej UE-Japonia

Opinia z dnia 12 marca 2010 r. w sprawie wniosku dotyczącego decyzji Rady w sprawie stanowiska Unii w ramach Wspólnego Komitetu Współpracy Celnej UE-Japonia dotyczącego wzajemnego uznawania programów upoważnionego przedsiębiorcy w Unii Europejskiej i w Japonii

Zwalczanie obrotu towarami podrobionymi (ACTA)

Opinia z dnia 22 lutego 2010 r. na temat bieżących negocjacji Unii Europejskiej w sprawie umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA)

Wypadki i incydenty w lotnictwie cywilnym

Opinia z dnia 4 lutego 2010 r. dotycząca wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie badania wypadków i incydentów w lotnictwie cywilnym i zapobiegania im

Współpraca w dziedzinie opodatkowania

Opinia z dnia 6 stycznia 2010 r. w sprawie wniosku dotyczącego dyrektywy Rady w sprawie współpracy administracyjnej w dziedzinie opodatkowania

Załącznik G – Wystąpienia Inspektora i jego zastępcy

Inspektor oraz jego zastępca w dalszym ciągu poświęcali wiele czasu i wysiłku, by wyjaśnić swoje zadania oraz propagować wiedzę o ochronie danych w ogólności, a także o szeregu konkretnych zagadnień, występując publicznie i podejmując podobne formy aktywności w różnych instytucjach oraz państwach członkowskich w ciągu całego roku.

Parlament Europejski – Komisje

27 stycznia	Zastępca, Komisja LIBE w sprawie polityk zwalczania terroryzmu (Bruksela) *
4 marca	Inspektor, Komisja LIBE w sprawie PNR i prywatności transatlantyckiej (Bruksela)
21 czerwca	Inspektor, Komisja LIBE w sprawie Karty Praw Podstawowych (Bruksela) *
23 lipca	Inspektor, Komisja LIBE w sprawie umowy TFTP II (Bruksela)
28 września	Zastępca, Komisja LIBE w sprawie zwalczania niegodziwego traktowania w celach seksualnych (Bruksela) *
9 listopada	Inspektor, Komisja PETI w sprawie publicznego dostępu do dokumentów (Bruksela) *
15 listopada	Inspektor i jego zastępca, Komisja LIBE w sprawie sprawozdania rocznego 2009 (Bruksela)

Parlament Europejski – Inne

28 stycznia	Inspektor, Dzień Ochrony Danych (Bruksela)
9 lutego	Inspektor, Dzień Bezpieczniejszego Internetu (Strasburg) *

* Tekst dostępny na stronie internetowej EIOD.

16 marca	Inspektor, posłowie do Parlamentu Europejskiego na temat ACTA (Bruksela)
24 marca	Zastępca, Platforma Prywatności: Wolność w Internecie (Bruksela)
8 kwietnia	Inspektor, posłowie do Parlamentu Europejskiego na temat PNR (Bruksela)
1 grudnia	Inspektor, Platforma Prywatności: Przegląd ochrony danych (Bruksela)

Rada

19 stycznia	Zastępca, Konferencja o ECRIS (Bruksela) *
25 stycznia	Inspektor, polska reprezentacja, Dzień Ochrony Danych (Bruksela)
11 lutego	Inspektor, Konferencja na temat zaufania do TIK (Leon) *
24 marca	Inspektor, Grupa Robocza ds. Ochrony Danych (Bruksela)

Komisja

28 stycznia	Inspektor, Dzień Ochrony Danych, minisympozjum (Bruksela)
28 stycznia	Inspektor, Dzień Ochrony Danych, przedpołudniowa przemowa (Bruksela)
22 czerwca	Inspektor, Konferencja na temat inteligentnych systemów transportowych (Bruksela) *
29 czerwca	Inspektor i Zastępca, przesłuchanie na temat przeglądu ochrony danych (Bruksela)
22 września	Inspektor, grupa zadaniowa ds. społeczności internetowych (Bruksela)
5 października	Inspektor, okrągły stół w sprawie przyszłości ochrony danych osobowych (Bruksela) *
18 listopada	Inspektor, konferencja OLAF (Paryż) *
3 grudnia	Inspektor, konferencja na temat dyrektywy w sprawie zatrzymania danych (Bruksela) *

Inne instytucje i organy UE

27 stycznia	Zastępca, Dzień Ochrony Danych w EMA (Londyn-Bruksela)
7 maja	Inspektor, Agencja Praw Podstawowych (Wiedeń)
27-28 maja	Inspektor i Zastępca, warsztat organizacji międzynarodowych (Florencja)
31 maja	Inspektor, ochrona danych i egzekwowanie prawa (Trier) *
7 czerwca	Zastępca, EKES o cybermolestowaniu (Bruksela) *
15-16 czerwca	Inspektor i Zastępca, Ochrona danych w postępowaniu karnym (Madryt)
13 września	Inspektor, ENISA FORTH szkoła letnia (Heraklion)
15 listopada	Inspektor i Zastępca, konferencja prasowa na temat sprawozdania rocznego 2009 (Bruksela) *

Konferencje międzynarodowe

30 stycznia	Inspektor, Komputery, prywatność i ochrona danych (Bruksela)
10 marca	Inspektor, Okrągły stół w 30 rocznicę wytycznych OECD o prywatności (Paryż) *
20 kwietnia	Inspektor, Globalny szczyt prywatności IAPP (Waszyngton) **
29 kwietnia	Inspektor i Zastępca, europejskie organy ochrony danych (Praga) *
6 lipca	Inspektor, Prywatność w prawie i biznesie (Cambridge)
25 października	Zastępca, Publiczny głos w sprawie społeczeństwa obywatelskiego (Jerozolima) *

26 października	Inspektor, 30 lat wytycznych OECD o prywatności (Jerozolima)
27 października	Inspektor, Prywatność i komisarze ochrony danych (Jerozolima)
28 października	Zastępca, Prywatność i komisarze ochrony danych (Jerozolima) *

Inne wydarzenia

22 stycznia	Zastępca, 30 rocznica CRID (Namur) *
2 lutego	Inspektor, Europejski Kongres Policji (Berlin) *
26 lutego	Inspektor, Własność intelektualna i społeczeństwo informacyjne (Barcelona) *
5 marca	Inspektor, Kolokwium PLN (Bruksela)
9 marca	Inspektor, Brytyjska Izba Handlowa w Belgii (Bruksela) *
12 marca	Zastępca, Etyka medyczna i prawa pacjentów (San Remo)
23 marca	Inspektor, Wspólne spotkanie parlamentarne na temat bezpieczeństwa (Paryż) *
26 marca	Inspektor, Globalna mobilności bezpieczeństwo (Bruksela) *
13 kwietnia	Inspektor, Europejski Dzień Świadomości Bezpieczeństwa Cyfrowego (Bruksela) *
23 kwietnia	Inspektor, Amerykańska Izba Handlowa w UE (Bruksela)
28 kwietnia	Zastępca, Rada Sądownictwa (Rzym)
11 maja	Zastępca, Warsztaty na temat obliczeń rozproszonych (Bruksela)
20 maja	Inspektor, Inicjatywa ochrony danych (Londyn)
1 czerwca	Inspektor, Poufność cyfrowa (Bruksela)
2 czerwca	Inspektor, Internet rzeczy (Bruksela)
8 czerwca	Zastępca, Okrągły stół w sprawie bezpieczeństwa (Bruksela)
15 czerwca	Zastępca, Traktat lizboński (Londyn)
17 czerwca	Zastępca, Europejskie Forum Urzędników ds. Prywatności (Bruksela)
22 czerwca	Inspektor, Amerykańska Izba Handlowa w UE (Bruksela)
23 czerwca	Inspektor, Cyfrowa UE i IAPP (Bruksela)
29 czerwca	Zastępca, CEPS na temat granic i sądownictwa karnego (Bruksela)
8 lipca	Zastępca, Szkoła podyplomowa Alma (Bolonia)
12 lipca	Zastępca, Rada Sądownictwa (Rzym)
7 września	Inspektor, Przyszłość bezpieczeństwa (Berlin)
15 września	Inspektor, Prywatność i bezpieczeństwo (Bruksela)
16 września	Inspektor, Rada Lizbońska na temat cyfrowego rynku (Bruksela)
20 września	Inspektor, Przeciwdziałanie terroryzmowi i ochrona danych (Bruksela)
23 września	Inspektor, Warsztat na temat przeglądu ochrony danych (Bruksela)
28 września	Inspektor, Ochrona danych i wolność informacji (Bruksela)
29 września	Inspektor, Bezpieczeństwo informacji i prywatność (Budapeszt)
29 września	Zastępca, Bezpieczeństwo granic UE (Bruksela) *

* Tekst dostępny na stronie internetowej EIOD.
** Wideo dostępne na stronie internetowej EIOD.

13 października	Inspektor, Prywatność w cyfrowym świecie (Bruksela)
22 października	Zastępca, Sądownictwo karne w Europie (Luksemburg) *
5 listopada	Zastępca, Przestrzeganie prawa prywatności (Rzym)
17 listopada	Zastępca, Inteligentny transport (Mediolan)
23 listopada	Inspektor, Prywatność a badania naukowe (Bruksela) *
23 listopada	Zastępca, Badania medyczne a prywatność (Bruksela) *
24 listopada	Zastępca, Seminarium o ochronie danych – wypowiedź wideo (Buenos Aires)
29 listopada	Inspektor, Przyjaciele Europy o ochronie danych UE (Bruksela)
30 listopada	Inspektor, Forum Europa o ochronie danych UE (Bruksela)
30 listopada	Inspektor, Europejskie Forum Internetu (Bruksela)
2 grudnia	Inspektor, Hogan & Lovells (Londyn)
9 grudnia	Inspektor, Etyka i zarządzanie biometryką (Bruksela) *
10 grudnia	Zastępca, Prawa pasażerów UE (Trier)
16 grudnia	Inspektor, Rada Przyszłości Internetu (Ghent) *

Załącznik H – skład Sekretariatu EIOD

EIOD i jego zastępca z większością pracowników.

• Nadzór i egzekwowanie prawa

Sophie LOUVEAUX *Kierownik ds. nadzoru i egzekwowania prawa*	John-Pierre LAMB *Oddelegowany ekspert krajowy*
Laurent BESLAY *Koordynator ds. bezpieczeństwa i technologii*	Xanthi KAPSOSIDERI *Radca prawny*
Jaroslaw LOTARSKI *Koordynator ds. skarg*	Luisa PALLA Asystent ds. nadzoru i egzekwowania
Maria Verónica PEREZ ASINARI *Koordynator ds. konsultacji*	Dario ROSSI Asystent ds. nadzoru i egzekwowania Korespondent ds. księgowości Menedżer zewnętrznej hurtowni danych (EDWM)
Isabelle CHATELIER *Radca prawny*	Tereza STRUNCOVA *Radca prawny*

Bart DE SCHUITENEER Administrator ds. technologii Lokalny administrator ds. bezpieczeństwa/LISO	Michaël VANFLETEREN *Radca prawny*
Delphine HAROU Radca prawny	

• Polityka i konsultacja

Hielke HIJMANS *Kierownik ds. polityki i konsultacji*	Raffaele DI GIOVANNI BEZZI Asystent ds. polityki i konsultacji
Bénédicte HAVELANGE *Koordynator ds. wielkoskalowych informatycznych systemów polityki granicznej*	Herke KRANENBORG *Radca prawny*
Anne-Christine LACOSTE *Koordynator ds. współpracy z organami ochrony danych*	Roberto LATTANZI *Oddelegowany ekspert krajowy*
Rosa BARCELO *Radca prawny*	Alfonso SCIROCCO *Inspektor ochrony danych* *Zarządzanie jakością*
Zsuzsanna BELENYESSY *Radca prawny*	Luis VELASCO Administrator ds. technologii
Katarzyna CUADRAT-GRZYBOWSKA *Radca prawny*	

• Rejestry i wsparcie operacyjne

Andrea BEACH *Kierownik ds. rejestru i wsparcia operacyjnego*	Kim Thien LÊ *Asystent ds. administracyjnych*
Christine HUC *Asystent ds. administracyjnych*	Ewa THOMSON *Asystent ds. administracyjnych*
Kim DAUPHIN *Asystent ds. administracyjnych*	

• Sektor informacji i komunikacji

Nathalie VANDELLE *Kierownik ds. informacji i komunikacji*	Agnieszka NYKA Asystent ds. informacji i komunikacji
Olivier ROSSIGNOL Asystent ds. informacji i komunikacji	

• Zasoby ludzkie, budżet i administracja

Leonardo CERVERA NAVAS *Kierownik ds. zasobów ludzkich, budżetu i administracji*	Aida PASCU *Asystent ds. administracyjnych* *Asystent LSO*
Isabelle DELATTRE *Asystent ds. finansowych i księgowych*	Sylvie PICARD *Asystent inspektora ochrony danych* *COFO - ICO*
Anne LEVÊCQUE *Asystent ds. zasobów ludzkich GECO*	Anne-Françoise REYNDERS *Asystent ds. administracyjnych*
Vittorio MASTROJENI *Kierownik ds. zasobów ludzkich*	Marian SANCHEZ LOPEZ *Kierownik ds. finansowych i księgowych*

Europejski Inspektor Ochrony Danych

Sprawozdanie roczne 2010

Luksemburg: Urząd Publikacji Unii Europejskiej

2011 — 118 str. — 21 x 29,7 cm

ISBN 978-92-95073-20-3
doi:10.2804/2085

JAK OTRZYMAĆ PUBLIKACJE UE

Publikacje bezpłatne:

- w EU Bookshop (http://bookshop.europa.eu)
- w przedstawicielstwach i delegaturach Unii Europejskiej (dane kontaktowe można uzyskać pod adresem http://ec.europa.eu lub wysyłając faks pod numer 352 2929-42758)

Publikacje płatne:

- w EU Bookshop (http://bookshop.europa.eu)

Płatne subskrypcje (np. *Dziennik Urzędowy Unii Europejskiej*, zbiory orzeczeń Trybunału Sprawiedliwości Unii Europejskiej):

- u dystrybutorów Urzędu Publikacji Unii Europejskiej (http://publications.europa.eu/others/agents/index_pl.htm)

EUROPEJSKI INSPEKTOR
OCHRONY DANYCH

QT-AA-11-001-PL-C

EIOD – Europejski Inspektor Ochrony Danych

www.edps.europa.eu

Urząd Publikacji

ISBN 978-92-95073-20-3