ISSN 1830-9518

Sprawozdanie roczne

2009

Sprawozdanie roczne

2009

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, 2011

ISBN 978-92-95073-08-1
doi:10.2804/12320

Printed in Luxembourg

WYDRUKOWANO NA PAPIERZE BIELONYM BEZ CHLORU PIERWIASTKOWEGO (ECF)

Spis treści

7 GŁÓWNE CELE NA ROK 2010

PRZEWODNIK UŻYTKOWNIKA

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

Rozdział 1 – Najważniejsze wydarzenia 2009 r. – przedstawia główne działania EIOD w 2009 r. oraz wyniki osiągnięte w poszczególnych dziedzinach.

Rozdział 2 – Nadzór – opisuje działania wdrażane w celu zapewnienia oraz monitorowania wykonywania 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 2009 r. Zaprezentowano także założenia tematyczne przyjęte przez EIOD w dziedzinie rekrutacji, danych dotyczących zdrowia oraz nadzoru wideo, jak też nowe informacje odnoszące się do nadzoru nad systemem Eurodac.

Rozdział 3 – Konsultacje – obejmuje działania EIOD dotyczące jego funkcji doradczej, koncentrując się na opiniach i uwagach na temat wniosków prawodawczych oraz dokumentów pokrewnych, jak również na wpływie, jaki wywierają one w coraz liczniejszych dziedzinach. Rozdział ten zawiera także analizę tematów ogólnych: przedstawia się w nim pewne nowe kwestie odnoszące się do techniki oraz nowe wydarzenia w dziedzinie polityki i prawodawstwa.

Rozdział 4 – Współpraca – opisuje działania podejmowane w ramach najważniejszych forów, takich jak grupa robocza art. 29 ds. ochrony danych, w obrębie wspólnych organów nadzoru trzeciego filaru oraz podczas europejskich i międzynarodowych konferencji dotyczących ochrony danych.

Rozdział 5 – Komunikacja – przedstawia działania i osiągnięcia EIOD w zakresie informacji i komunikacji, w tym komunikacji zewnętrznej z mediami oraz informacji dla społeczeństwa.

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

Rozdział 7 – Główne cele na 2010 r. – opisuje pokrótce przyszłe działania i najważniejsze priorytety na 2010 r.

Sprawozdanie uzupełnia szereg załączników, które zawierają przegląd stosownych ram prawnych, przepisy rozporządzenia (WE) nr 45/2001, wykaz inspektorów ochrony danych, wykazy opinii 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 2009 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 oraz jego streszczenia można zamówić bezpłatnie w EU Bookshop (http://www.bookshop.europa.eu) lub u EIOD. Dane kontaktowe znajdują się na naszej stronie internetowej w dziale „Contact".

OKREŚLENIE 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 45/200 ([1]), jak również innych wspólnotowych aktów 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 prawodawczych 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 („współpracę").

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 sprawowania władzy;

- 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 12.1.2001, s. 1).

PRZEDMOWA

Peter Hustinx, Europejski Inspektor Ochrony Danych, i Giovanni Buttarelli, Zastępca Inspektora.

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 2009 jako piąty pełny rok działalności EIOD w charakterze nowego, niezależnego organu nadzoru mającego za zadanie zapewnienie poszanowania przez instytucje i organy wspólnotowe podstawowych praw i wolności osób fizycznych, w szczególności ich prywatności, w odniesieniu do przetwarzania danych osobowych. Obejmuje ono również pierwszy rok wspólnej pięcioletniej kadencji obecnych dwóch członków tego organu.

Omawiany rok był bardzo ważny z punktu widzenia podstawowego prawa do ochrony danych. Było to skutkiem kilku znaczących wydarzeń: wejścia w życie traktatu lizbońskiego, który zapewnia mocne podstawy prawne kompleksowej ochrony danych we wszystkich dziedzinach polityki UE; rozpoczęcia konsultacji społecznych dotyczących przyszłości ram prawnych ochrony danych w UE; przyjęcia nowego pięcioletniego programu w sprawie przestrzeni wolności, bezpieczeństwa i sprawiedliwości („programu sztokholmskiego"), który kładzie znaczący nacisk na ochronę danych jako fundamentalny element legitymacji oraz skuteczności działań w tym obszarze.

EIOD jest i pozostanie w najbliższej przyszłości aktywnie zaangażowany w działania w tych dziedzinach. Jednocześnie dopilnowaliśmy, aby rola niezależnego organu nadzorczego była wykonywana we wszystkich obszarach jego regularnej działalności. Doprowadziło to do znaczących postępów zarówno w nadzorze nad przetwarzającymi dane osobowe instytucjami i organami UE, jak i w konsultacjach dotyczących nowej polityki oraz działań 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 2009

1.1. Najważniejsze wydarzenia

Kilka wydarzeń, które miały miejsce w 2009 r., przyczyniło się do zwiększenia zainteresowania podstawowym prawem do ochrony danych osobowych oraz nowoczesnymi sposobami zapewnienia skuteczniejszej ochrony tych danych w praktyce. Ten wzrost zainteresowania bardzo cieszy, biorąc pod uwagę wyzwania stawiane przez nowe technologie, globalizację i sprzeczne interesy publiczne.

Wejście w życie traktatu lizbońskiego w grudniu 2009 r. zapewniło mocne podstawy prawne kompleksowej ochrony danych we wszystkich dziedzinach polityki UE. Karta praw podstawowych zyskała taką samą wagę prawną jak traktaty; jest tak również w przypadku art. 8, który dotyczy ochrony danych osobowych. Artykuł 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) wymienia obecnie – wśród postanowień ogólnych Traktatu – możliwe do bezpośredniego wyegzekwowania prawo każdej osoby do ochrony danych osobowych jej dotyczących.

Artykuł 16 TFUE zapewnia również ogólną podstawę prawną środków prawnych dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje i organy UE oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa UE. Przestrzeganie tych zasad podlega kontroli niezależnych organów, o czym stanowi również art. 8 Karty. Umożliwi to – a wręcz wymusi – całościowy przegląd istniejących ram prawnych ochrony danych w celu zagwarantowania, by wszystkie osoby podlegające jurysdykcji UE w pełni korzystały z podstawowego prawa do ochrony danych.

Drugim ważnym wydarzeniem była – powzięta jeszcze przed zaistnieniem prawnych i politycznych skutków wejścia w życie traktatu lizbońskiego – decyzja Komisji Europejskiej o rozpoczęciu konsultacji społecznych dotyczących przyszłości istniejących ram prawnych ochrony danych.

W związku z powyższym w maju 2009 r. zorganizowano publiczną konferencję, od lipca do grudnia 2009 r. trwały zaś konsultacje społeczne. W konferencji uczestniczyli osobiście zarówno Inspektor, jak i jego zastępca. Obydwaj brali też wraz ze współpracownikami bardzo aktywny udział w pracach grupy roboczej art. 29 oraz Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości, aby wnieść w konsultacje społeczne wspólny wkład, który pozwoli Komisji wypracować kompleksowe ramy prawne we wszystkich obszarach polityki UE oraz zagwarantować ich skuteczność w praktyce pomimo licznych wyzwań.

Przyjęty w grudniu 2009 r. przy pełnym i aktywnym wsparciu Europejskiego Inspektora Ochrony Danych (EIOD) wspólny wynik prac obydwu grup roboczych był jednym z najważniejszych wkładów wniesionych w konsultacje społeczne. EIOD będzie w najbliższej przyszłości aktywnie monitorować ten temat, będzie też gotów udzielać dalszych porad w miarę potrzeb.

Trzecim bardzo ważnym wydarzeniem było przyjęcie wkrótce po wejściu w życie traktatu lizbońskiego,

również w grudniu 2009 r., nowego pięcioletniego programu w sprawie przestrzeni wolności, bezpieczeństwa i sprawiedliwości (program sztokholmski), który kładzie znaczący nacisk na ochronę danych jako fundamentalny element legalności oraz skuteczności działań w tym zakresie. W programie tym uwzględniono skutki wejścia w życie traktatu lizbońskiego w omawianym obszarze, określając najważniejsze kierunki polityki UE na najbliższe pięć lat. Jego wdrożenie będzie w każdym razie sprawniejsze dzięki zmianom instytucjonalnym, jakie przyniósł traktat lizboński.

Integralną częścią wspomnianej polityki jest wymiana danych osobowych między organami imigracyjnymi, organami ścigania oraz organami odpowiedzialnymi za bezpieczeństwo publiczne w poszczególnych państwach członkowskich. Dopilnowanie, aby ochrona danych była „wbudowana" od samego początku w takie działania i systemy, jest ważnym zobowiązaniem, którego realizację EIOD wspiera i zachęca do niej; Inspektor będzie też nadal monitorować jego wdrażanie w praktyce.

Wspomniane wydarzenia okazują się jeszcze ważniejsze, jeżeli weźmiemy pod uwagę fakt, że w lutym 2010 r. zaczyna kadencję nowa Komisja, która również kładzie znaczny nacisk na ochronę praw podstawowych w ogóle, przyznając przy tym wysoki priorytet konkretnie ochronie danych osobowych. Jeżeli chodzi o wyzwania, o których wspomniano na początku, należy podkreślić, że są one w znacznym stopniu konsekwencją powszechnego wykorzystywania przez społeczeństwo technologii informacyjnych w wielu dziedzinach życia.

Jako że proces ten będzie zapewne się rozwijać, a jego znaczenie w kontekście agendy cyfrowej Komisji jeszcze wzrośnie, tym ważniejsze jest zapewnienie w najbliższej przyszłości skuteczniejszej i bardziej kompleksowej ochrony danych osobowych. EIOD oczekuje na wnioski Komisji dotyczące wszystkich stosownych dziedzin, które podda bardzo uważnej analizie i ocenie.

1.2. Ogólny przegląd 2009

Najważniejsze działania EIOD w 2009 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 ([2]), 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 misji jego urzędu:

- funkcja „nadzorcza" polegająca na monitorowaniu i zapewnieniu poszanowania przez instytucje i organy UE ([3]) istniejących zabezpieczeń prawnych podczas przetwarzania danych osobowych;

- funkcja „konsultacyjna" polegająca na udzielaniu instytucjom i organom UE porad we wszystkich stosownych kwestiach, w szczególności w sprawie wniosków prawodawczych mających wpływ na ochronę danych osobowych;

- funkcja „współpracy" z krajowymi instytucjami oraz organami nadzorczymi w ramach dawnego „trzeciego filaru" UE obejmująca współpracę policyjną i sądową w sprawach karnych w celu poprawienia spójności ochrony danych osobowych.

Funkcje te zostaną szerzej omówione w rozdziałach 2, 3 i 4 niniejszego sprawozdania, gdzie przedstawiono główne działania EIOD i postępy osiągnięte w 2009 r. Najważniejsze elementy zostaną podsumowane w niniejszej części.

Znaczenie informacji na temat tych działań oraz komunikacji w tym zakresie w pełni uzasadnia ich oddzielne omówienie w rozdziale 5. Wszystkie powyższe działania bazują na skutecznym zarządzaniu zasobami finansowymi, ludzkimi i innymi, co zostanie przedstawione w rozdziale 6.

Nadzór

Zadania nadzoru obejmują doradztwo i wparcie dla inspektorów ochrony danych, jak również kontrole wstępne powodujących zagrożenie operacji przetwarzania danych, prowadzenie dochodzeń (w tym kontroli na miejscu) oraz rozpatrywanie skarg.

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

([3]) W niniejszym sprawozdaniu stosowane są pojęcia „instytucje" i „organy" pojawiające się w rozporządzeniu (WE) nr 45/2001. Obejmuje to również agencje wspólnotowe. Pełny wykaz znajduje się na stronie: http://europa.eu/agencies/community_agencies/index_pl.htm.

Dalsze doradztwo dla administracji wspólnotowej może też przyjmować postać konsultacji związanych ze środkami administracyjnymi lub publikacji wytycznych na dany temat.

Każda instytucja i organ UE musi zatrudniać co najmniej jednego inspektora ochrony danych. W 2009 r. łączna liczba inspektorów ochrony danych wzrosła do 45. Regularne kontakty z inspektorami i siecią, w ramach której działają, są ważnym warunkiem skutecznego nadzoru.

Kontrole wstępne czynności przetwarzania stwarzających zagrożenie pozostawały w 2009 r. głównym aspektem nadzoru. EIOD przyjął 110 opinii dotyczących kontroli wstępnych związanych z danymi dotyczącymi zdrowia, oceną personelu, rekrutacją, zarządzaniem czasem, nagrywaniem rozmów telefonicznych, narzędziami do pomiaru wydajności oraz dochodzeniami w sprawach bezpieczeństwa. 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 wykonania dla wszystkich instytucji i organów UE. Po działaniu „Wiosna 2009" EIOD opublikował raport, w którym wskazał, że instytucje wspólnotowe osiągnęły zadowalające postępy w spełnianiu wymogów ochrony danych, lecz w przypadku większości agencji poziom zgodności z przepisami był niższy.

EIOD przeprowadził również cztery kontrole na miejscu w różnych instytucjach i organach. Kontrole takie staną się wkrótce częstsze, a działania podejmowane w związku z nimi są systematycznie monitorowane. W lipcu 2009 r. EIOD przyjął podręcznik procedur kontrolnych i opublikował najważniejsze elementy tych procedur na swojej stronie internetowej.

W 2009 r. łączna liczba skarg wzrosła do 111, lecz tylko 42 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, gromadzenia nadmiernej ilości danych lub bezprawnego wykorzystania danych przez administratora. W 8 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 przekazywania danych państwom trzecim lub organizacjom międzynarodowym, przetwarzania danych w przypadku wdrożenia procedur związanych z pandemią, ochrony danych w obrębie Służby Audytu Wewnętrznego oraz przepisów wykonawczych do rozporządzenia (WE) nr 45/2001.

EIOD przyjął wytyczne dotyczące przetwarzania danych osobowych w celach rekrutacji oraz danych dotyczących zdrowia w miejscu pracy. W 2009 r. EIOD przeprowadził również konsultacje społeczne w sprawie wytycznych w zakresie nadzoru wideo, kładąc nacisk m.in. na „wbudowaną ochronę prywatności" (privacy by design) oraz rozliczalność jako najważniejsze zasady w tym kontekście.

Najważniejsze liczby dotyczące działalności EIOD w 2009 r.

→ **Przyjęto 110 opinii dotyczących kontroli wstępnych** związanych z danymi dotyczącymi zdrowia, oceną personelu, rekrutacją, zarządzaniem czasem, dochodzeniami w sprawach bezpieczeństwa, nagrywaniem rozmów telefonicznych oraz narzędziami do pomiaru wydajności

→ **Wpłynęło 111 skarg, z tego 42 dopuszczalne**. Główne rodzaje zarzucanych naruszeń: naruszenie poufności danych, gromadzenie nadmiernej ilości danych lub bezprawne wykorzystanie danych przez administratora

- **Rozstrzygnięto 12 spraw**, w których EIOD nie stwierdził naruszenia zasad ochrony danych
- **8 zadeklarowanych przypadków niezgodności** z zasadami ochrony danych

→ **32 konsultacje dotyczące środków administracyjnych**. Udzielano porad dotyczących licznych aspektów prawnych związanych z przetwarzaniem danych osobowych przez instytucje i organy UE

→ **Przeprowadzono 4 kontrole na miejscu** w różnych instytucjach i organach UE

→ **Opublikowano 3 wytyczne** na temat rekrutacji, danych dotyczących zdrowia oraz nadzoru wideo

→ **Wydano 16 opinii prawnych** dotyczących wielkoskalowych systemów informacyjnych, wykazów terrorystów, przyszłych ram ochrony danych, zdrowia publicznego, opodatkowania i transportu

→ **Wydano 4 formalne uwagi** dotyczące publicznego dostępu do dokumentów, usługi powszechnej i prywatności w kontekście łączności oraz negocjacji między UE i USA w sprawie nowej umowy SWIFT

→ **Zorganizowano 3 spotkania grupy ds. koordynowania nadzoru nad systemem Eurodac**, w wyniku których opublikowany został drugi raport ze skoordynowanej kontroli dotyczący informacji przekazywanych podmiotom danych oraz oceny wieku młodych osób ubiegających się o azyl

Konsultacje

W omawianym roku zaszły znaczące wydarzenia, które przybliżyły perspektywę nowych ram prawnych ochrony danych. Osiągnięcie tego celu będzie dominującym tematem działań EIOD w nadchodzących latach.

Pod koniec 2008 r. na szczeblu UE przyjęto ogólne ramy prawne ochrony danych w obszarze współpracy policyjnej i sądowej. Choć nie są one w pełni zadowalające, stanowią ważny krok we właściwym kierunku.

Drugim ważnym wydarzeniem 2009 r. było przyjęcie w ramach większego pakietu zmienionej dyrektywy o prywatności i łączności elektronicznej. Był to również pierwszy krok w kierunku modernizacji ram prawnych ochrony danych.

Wejście w życie traktatu lizbońskiego w dniu 1 grudnia 2009 r. poskutkowało nie tylko tym, że Karta praw podstawowych stała się wiążącą dla instytucji i organów, jak też dla państw członkowskich, gdy działają one w ramach prawa UE, lecz także tym, że wprowadzono ogólne podstawy dla kompleksowych ram prawnych w postaci art. 16 TFUE.

W 2009 r. Komisja rozpoczęła również konsultacje społeczne w sprawie przyszłości ram prawnych ochrony danych. EIOD ze współpracownikami wniósł wkład w te konsultacje, podkreślając przy różnych okazjach potrzebę bardziej kompleksowej i skuteczniejszej ochrony danych w Unii Europejskiej.

EIOD nadal wdrażał ogólną politykę w dziedzinie konsultacji, wydając rekordową liczbę opinii prawnych na różne tematy. Polityka ta obejmuje także aktywne podejście oparte na regularnym sporządzaniu spisu wniosków prawodawczych, które mają zostać przedłożone do konsultacji, oraz gotowości do zgłaszania nieformalnych uwag na etapie przygotowywania wniosków prawodawczych. Większość opinii EIOD była później omawiana z Parlamentem i Radą.

W 2009 r. EIOD śledził ze szczególnym zainteresowaniem wydarzenia związane z programem sztokholmskim oraz zawartą w nim wizją następnego pięciolecia w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych. EIOD udzielał porad związanych z opracowywaniem programu, jak też wziął udział w pracach przygotowawczych nad europejskim modelem informacji.

Inne działania w tym obszarze dotyczyły przeglądu rozporządzenia Eurodac i rozporządzenia dublińskiego, ustanowienia agencji odpowiedzialnej za zarządzanie operacyjne wielkoskalowymi systemami informatycznymi oraz spójnego podejścia do nadzoru w tej dziedzinie.

W kontekście prywatności w łączności elektronicznej i technologii, oprócz ogólnego przeglądu, o którym wspomniano powyżej, EIOD zajmował się kwestiami dotyczącymi dyrektywy o przechowywaniu danych, wykorzystania etykiet RFID, inteligentnych systemów transportowych oraz raportem RISEPTIS na temat zaufania w społeczeństwie informacyjnym.

W kontekście globalizacji EIOD uczestniczył w opracowywaniu globalnych standardów, w dialogu transatlantyckim dotyczącym ochrony danych oraz danych wykorzystywanych przez organy ścigania, jak też zajmował się kwestią środków ograniczających w odniesieniu do osób podejrzanych o terroryzm oraz niektórych państw trzecich.

Innymi obszarami znaczącego zainteresowania EIOD było zdrowie publiczne (w tym transgraniczna opieka zdrowotna, e-zdrowie i nadzór nad bezpieczeństwem farmakoterapii) oraz publiczny dostęp do dokumentów, np. zmiana rozporządzenia (WE) nr 1049/2001 w sprawie publicznego dostępu

i różne sprawy sądowe dotyczące związku między publicznym dostępem a ochroną danych.

Współpraca

Podstawową platformą współpracy między organami ochrony danych w Europie jest grupa robocza art. 29. 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 wyzwaniami stawianymi przez nowe technologie. EIOD wsparł też zdecydowanie inicjatywy na rzecz ułatwienia międzynarodowych przepływów danych.

Należy tutaj wspomnieć o wspólnym wkładzie wniesionym w dyskusję o przyszłości prywatności w związku z konsultacjami Komisji Europejskiej dotyczącymi ram prawnych ochrony danych w UE oraz konsultacjami Komisji związanymi ze skutkami wprowadzenia skanerów ciała w dziedzinie ochrony lotnictwa.

Jedno z najważniejszych zadań EIOD w ramach współpracy wiąże się z systemem Eurodac – odpowiedzialność za zarządzanie nim spoczywa równocześnie na Inspektorze oraz na krajowych organach ochrony danych. Grupa ds. koordynowania nadzoru nad systemem Eurodac, obejmująca krajowe organy ochrony danych oraz EIOD, zebrała się trzykrotnie, skupiając się na wdrożeniu programu prac przyjętego w grudniu 2007 r.

Jednym z najważniejszych rezultatów było przyjęcie w czerwcu 2009 r. drugiego raportu z kontroli, który skupiał się na dwóch zagadnieniach: prawo osób ubiegających się o azyl do informacji oraz metody oceny wieku młodych osób ubiegających się o azyl.

EIOD kontynuował ścisłą współpracę z organami ochrony danych w ramach dawnego „trzeciego filara", czyli w obszarze policji i sądownictwa – oraz z Grupą Roboczą ds. Policji i Wymiaru Sprawiedliwości. W 2009 r. Inspektor wniósł m.in. wkład w debatę o programie sztokholmskim oraz ocenę efektów decyzji ramowej Rady w sprawie ochrony danych.

Zainteresowanie budziła nadal współpraca na innych forach międzynarodowych, zwłaszcza podczas 31. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w Madrycie, gdzie wypracowano zestaw ogólnoświatowych norm dotyczących ochrony danych.

W kontekście „inicjatywy londyńskiej", zapoczątkowanej podczas 28. Międzynarodowej Konferencji w listopadzie 2006 r. w celu zwiększenia świadomości w zakresie ochrony danych i poprawy jej skuteczności, EIOD zorganizował też warsztaty dotyczące reakcji na naruszanie bezpieczeństwa.

1.3. Wyniki 2009

W sprawozdaniu rocznym z 2008 r. poniższe cele wymieniono jako najważniejsze na 2009 r. Większość z nich została w pełni lub częściowo zrealizowana.

- Wspieranie sieci inspektorów ochrony danych

EIOD nadal wspierał inspektorów ochrony danych, zwłaszcza w niedawno utworzonych agencjach, zachęcając ich do wymiany wiedzy fachowej i najlepszych praktyk w celu zwiększenia skuteczności ich działań.

- 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. Szczególną uwagę zwrócono na kontrole wstępne operacji przetwarzania danych wspólnych dla większej liczby agencji.

- Wytyczne horyzontalne

EIOD opublikował wytyczne na temat rekrutacji personelu i danych dotyczących zdrowia oraz projekt wytycznych na temat nadzoru wideo, które były przedmiotem konsultacji. Wytyczne te mają pomóc w zagwarantowaniu zgodności działań instytucji i organów z prawem oraz w usprawnieniu procedur kontroli wstępnej.

- Rozpatrywanie skarg

EIOD przyjął podręcznik dla personelu dotyczący rozpatrywania skarg, publikując jego najważniejsze zalecenia na swojej stronie internetowej, aby poinformować wszystkie zainteresowane strony

o stosownych procedurach, w tym kryteriach decydujących o tym, czy zostanie wszczęte dochodzenie w sprawie przedłożonych skarg. Na stronie internetowej dostępny jest teraz również formularz skargi.

- Polityka kontroli

EIOD nadal bada wykonywanie przepisów rozporządzenia (WE) nr 45/2001 przez wszystkie instytucje i organy; w związku z tym przeprowadzono pewną liczbę różnego rodzaju kontroli na miejscu. Opublikowano pierwszy zestaw procedur kontrolnych, by zapewnić większą przewidywalność tego procesu.

- Zakres konsultacji

Sporządziwszy systematyczny spis stosownych tematów i priorytetów, EIOD wydał rekordową liczbę 16 opinii i 4 zestawów formalnych 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.

- Program sztokholmski

EIOD poświęcił szczególną uwagę opracowaniu nowego pięcioletniego programu politycznego dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który został przyjęty przez Radę pod koniec 2009 r. Za jeden z głównych warunków uznano potrzebę skutecznej ochrony danych.

- Działania informacyjne

EIOD podniósł jakość i skuteczność internetowych narzędzi informacyjnych (strony internetowej i elektronicznego biuletynu) oraz przeprowadził w miarę potrzeb aktualizację innych działań informacyjnych (przez opracowanie nowej broszury informacyjnej i organizację wydarzeń służących zwiększaniu świadomości).

- Regulamin wewnętrzny

Wkrótce zostanie przyjęty regulamin wewnętrzny dotyczący poszczególnych działań EIOD. Będzie on w większości stanowić potwierdzenie lub wyjaśnienie obecnych zasad i zostanie opublikowany na stronie internetowej.

- Zarządzanie zasobami

EIOD skonsolidował i rozwinął działania związane z zasobami finansowymi oraz ludzkimi; szczególną uwagę zwrócono na rekrutację personelu za pośrednictwem konkursu EPSO w zakresie ochrony danych. Oczekuje się, że pierwsi zwycięzcy zostaną wyłonieni w 2010 r.

2

NADZÓR

2.1. Wprowadzenie

Zadaniem EIOD jest niezależny nadzór nad przeprowadzanymi przez instytucje lub organy UE operacjami przetwarzania danych, które w całości lub częściowo wchodzą w zakres dawnego „prawa wspólnotowego" ([4]) (z wyjątkiem Trybunału Sprawiedliwości działającego w ramach swych kompetencji sądowych). Rozporządzenie (WE) nr 45/2001 („rozporządzenie") określa i wskazuje szereg obowiązków oraz uprawnień umożliwiających EIOD wykonywanie tego zadania.

W związku z wprowadzeniem art. 16 TFUE, który zastępuje art. 286 Traktatu WE, traktat lizboński oznacza zmianę ram prawnych ochrony danych w administracji europejskiej. Dokładne implikacje tej zmiany, jak również likwidacji filarowej struktury działań nadzorczych EIOD podlegają obecnie analizie i mogą wymagać dalszych wyjaśnień.

Kontrola wstępna czynności przetwarzania pozostawała ważnym aspektem nadzoru w 2009 r. (zob. rozdz. 2.3), jednak EIOD rozwinął również inne formy nadzoru, takie jak rozpatrywanie skarg, kontrole, doradztwo w zakresie środków administracyjnych oraz opracowywanie wytycznych tematycznych. Specyficznym obszarem działalności EIOD był nadzór nad systemem Eurodac.

W 2009 r., podobnie jak w latach poprzednich, nie było konieczne wydanie przez EIOD żadnego nakazu, ostrzeżenia ani zakazu, jako że administratorzy danych wykonywali zalecenia, wyrażali zamiar ich wykonania lub podejmowali niezbędne kroki. Szybkość reagowania różniła się jednak w poszczególnych przypadkach.

2.2. Inspektorzy ochrony danych

Interesującą zasadą w zakresie ochrony danych w instytucjach Unii Europejskiej jest obowiązek wyznaczenia inspektora ochrony danych (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 jednostce.

W 2009 r. w nowych agencjach lub w ramach wspólnych przedsięwzięć mianowano 7 nowych inspektorów, w wyniku czego ich łączna liczba wyniosła 45.

Od kilku lat inspektorzy spotykają się regularnie w celu wymiany wspólnych doświadczeń i omówienia zagadnień horyzontalnych Ta nieformalna sieć okazała się przydatnym narzędziem współpracy i funkcjonowała także w 2009 r.

W celu koordynacji sieci utworzono „kwartet" złożony z czterech inspektorów (z Rady, Parlamentu

([4]) Art. 3 ust. 2 rozporządzenia (WE) nr 45/2001.

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 2009 r. w Europejskim Banku Centralnym oraz w październiku 2009 r. w Komisji Europejskiej (wspólnie z OLAF-em), korzystając z tej sposobności, by przekazać inspektorom aktualne informacje o swojej pracy, przedstawić przegląd najnowszych wydarzeń w dziedzinie ochrony danych w UE oraz omówić zagadnienia będące przedmiotem zainteresowania obu stron.

EIOD wykorzystał to forum do wyjaśnienia i omówienia procedury kontroli wstępnych, przedstawienia postępów w powiadamianiu o kontrolach wstępnych, poinformowania inspektorów o działaniu „Wiosna 2009" i późniejszych działaniach związanych z monitorowaniem (zob. rozdz. 2.5), przekazania aktualnych informacji o kontrolach EIOD oraz przedstawienia polityki i procedury kontroli EIOD. Inspektor skorzystał też z okazji, by wznowić prace nad ustanowieniem standardów zawodowych dla inspektorów ochrony danych oraz podzielić się informacjami o inicjatywach związanych z Europejskim Dniem Ochrony Danych (28 stycznia).

Inspektorzy ochrony danych podczas 26. spotkania w Brukseli (październik 2009 r.).

2.3. Kontrole wstępne

2.3.1. Podstawa prawna

Artykuł 27 ust. 1 rozporządzenia (WE) nr 45/2001 przewiduje, że wszelkie operacje przetwarzania mogące ze swej natury, przez swój zakres lub swoje cele stworzyć konkretne zagrożenia dla praw i wolności podmiotów danych podlegają kontroli wstępnej ze strony EIOD. Inspektor uznaje na przykład, że obecność pewnych danych biometrycznych (poza fotografiami) sama w sobie stwarza konkretne zagrożenia dla praw i wolności podmiotów danych oraz uzasadnia wstępną kontrolę operacji przetwarzania przez EIOD. Pogląd ten wynika przede wszystkim z faktu, że wszelkie dane biometryczne mają wrażliwy charakter.

Artykuł 27 ust. 2 rozporządzenia zawiera niewyczerpujący wykaz operacji przetwarzania danych, które mogą stworzyć takie zagrożenia. Przy interpretacji tego przepisu nadal stosowano kryteria opracowane w poprzednich latach ([5]) – zarówno przy podejmowaniu decyzji, 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 rozdz. 2.3.4).

([5]) Zob. Sprawozdanie roczne 2005, rozdz. 2.3.1.

2.3.2. Procedura

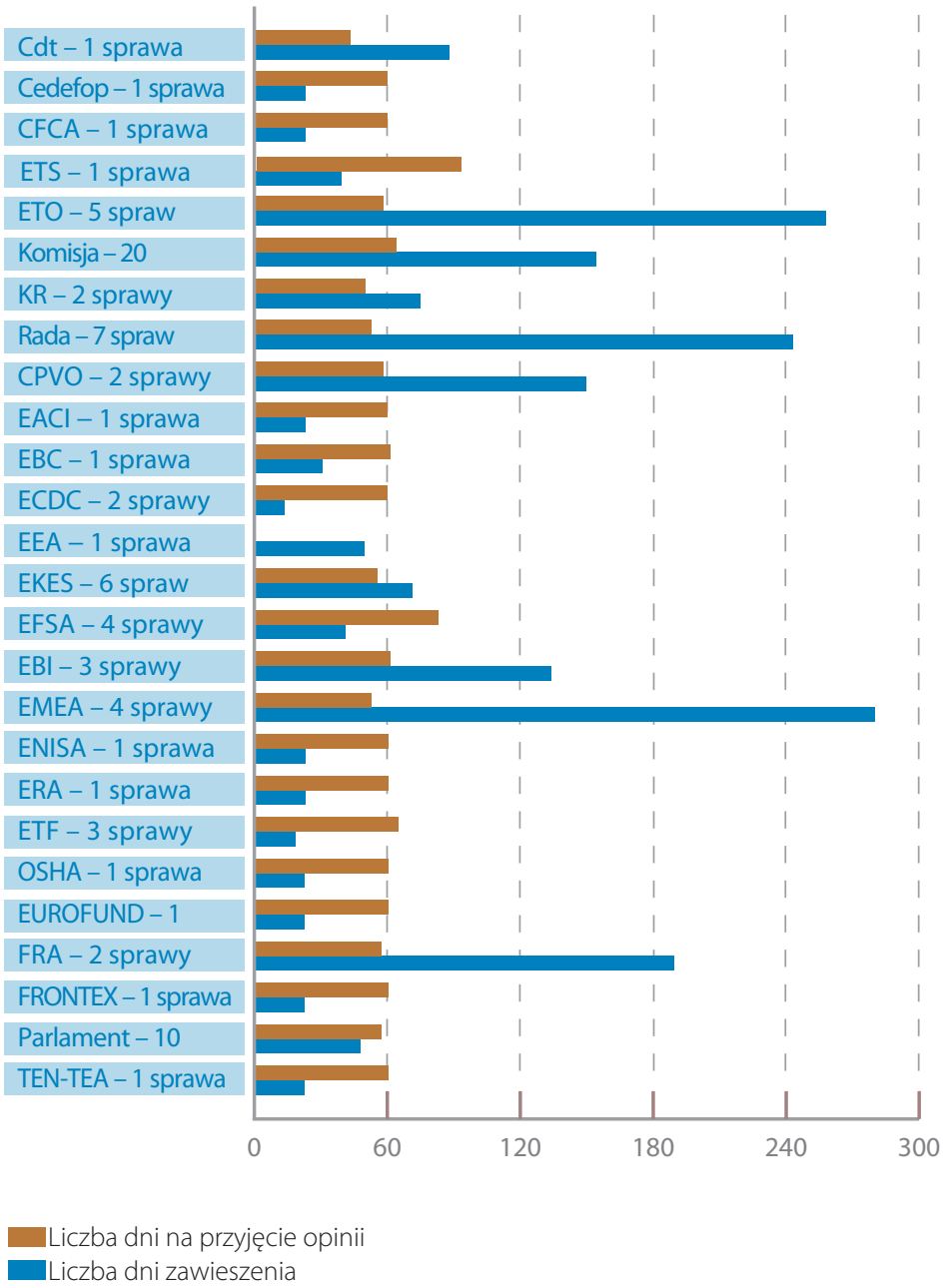
Powiadomienie

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. rozdz. 2.3.4).

Kontrole wstępne dotyczą nie tylko operacji, które jeszcze się nie rozpoczęły, lecz również przetwarzania, które rozpoczęło się przed 17 stycznia 2004 r. (data mianowania EIOD oraz zastępcy EIOD) 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*.

Termin, zawieszenie i przedłużenie

Średni czas w dniach dla instytucji/agencji

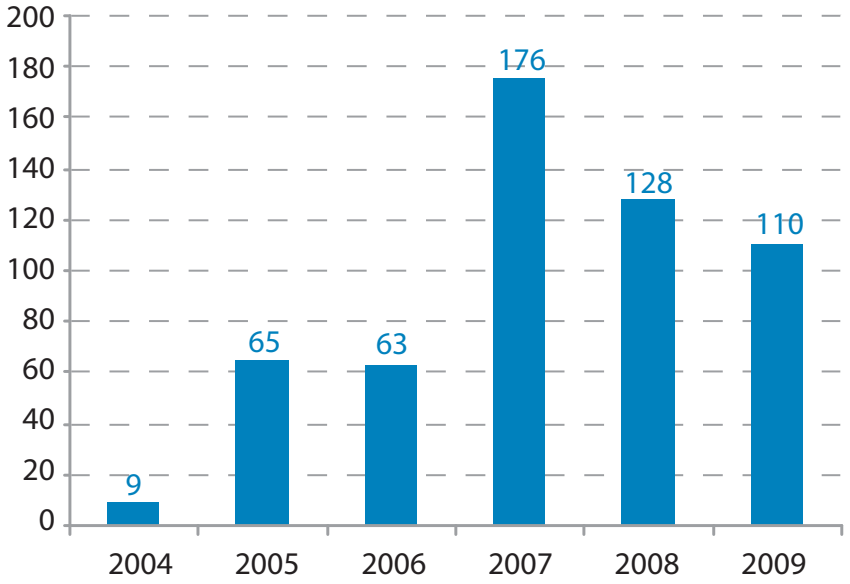


EIOD musi wydać opinię w terminie dwóch miesięcy od otrzymania powiadomienia ([6]). W przypadku gdy EIOD zwraca się z wnioskiem o dostarczenie dalszych informacji, bieg tego dwumiesięcznego terminu ulega zwykle zawieszeniu do chwili uzyskania takich informacji przez EIOD. Okres zawieszenia obejmuje czas przysługujący danemu inspektorowi ochrony danych na zgłoszenie uwag oraz w razie potrzeby – 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 takiej milczącej zgody.

([6]) W wypadku spraw *ex post*, które wpłynęły przed 1 września 2009 r., miesiąca sierpnia nie uwzględniano w odniesieniu do instytucji i organów ani też w odniesieniu do EIOD.

Rejestr

Powiadomienia kierowane do EIOD

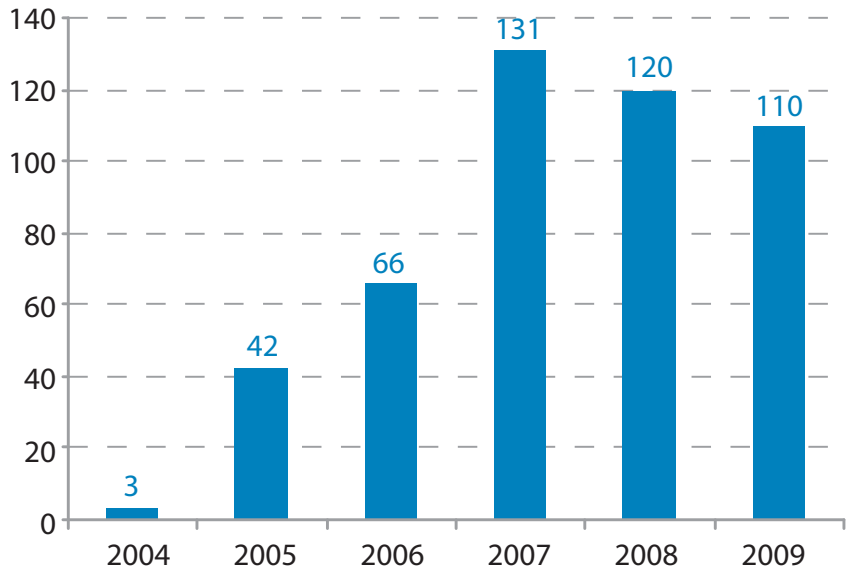


W 2009 r. EIOD otrzymał 110 powiadomień dotyczących kontroli wstępnej. Liczba ta jest nieznacznie niższa w porównaniu do 2008 r., gdyż EIOD likwiduje ostatnie zaległości związane z kontrolami wstępnymi *ex post*.

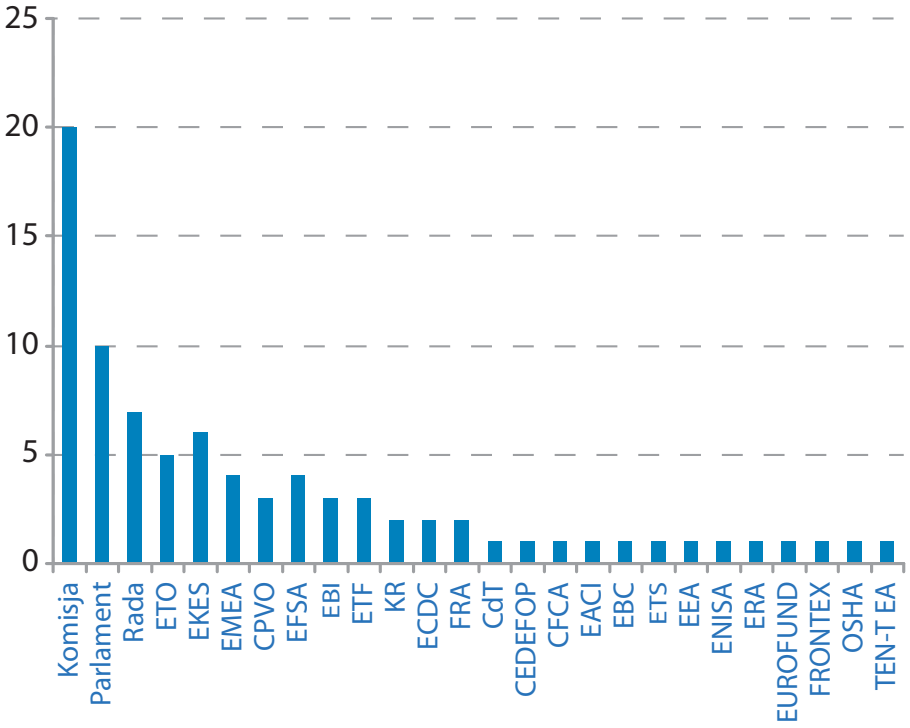
Artykuł 27 ust. 5 rozporządzenia przewiduje, że EIOD musi prowadzić rejestr wszystkich operacji przetwarzania, o których został powiadomiony w celu przeprowadzenia kontroli wstępnej. Rejestr ten musi zawierać informacje, o których mowa w art. 25, i być ogólnodostępny. Aby zapewnić przejrzystość, wszystkie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

Opinie

Liczba opinii EIOD dotyczących kontroli wstępnych rocznie



Liczba opinii EIOD dotyczących kontroli wstępnych według instytucji w 2009 r.



Zgodnie z art. 27 ust. 4 rozporządzenia stanowisko końcowe EIOD przyjmuje postać opinii, o której należy powiadomić administratora danej operacji przetwarzania oraz inspektora ochrony danych danej instytucji lub organu. **W 2009 r. EIOD przyjął 110 opinii dotyczących kontroli wstępnych** (zob. wykres „Liczba opinii EIOD dotyczących kontroli wstępnych rocznie" powyżej). Stanowi to nieznaczny spadek w porównaniu z poprzednimi dwoma latami.

Większość opinii dotyczyła **instytucji dużych** – 20 wiązało się z operacjami przetwarzania w Komisji Europejskiej, 10 w Parlamencie Europejskim i 7 w Radzie (zob. wykres „Liczba opinii EIOD według instytucji" powyżej). Wiele agencji zaczęło również wystosowywać powiadomienia o działaniach związanych ze swoją podstawową działalnością i standardowych procedurach administracyjnych zgodnie ze stosownymi procedurami opracowanymi przez EIOD (zob. rozdz. 2.3.2).

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

Opinie wydawane przez EIOD są upubliczniane. Wszystkie opinie są dostępne na stronach internetowych 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. Służy on stworzeniu ogólnych ram dla wydawania opinii na podstawie nagromadzonego doświadczenia praktycznego 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. rozdz. 2.3.6).

Procedura kontroli wstępnych *ex post* w agencjach

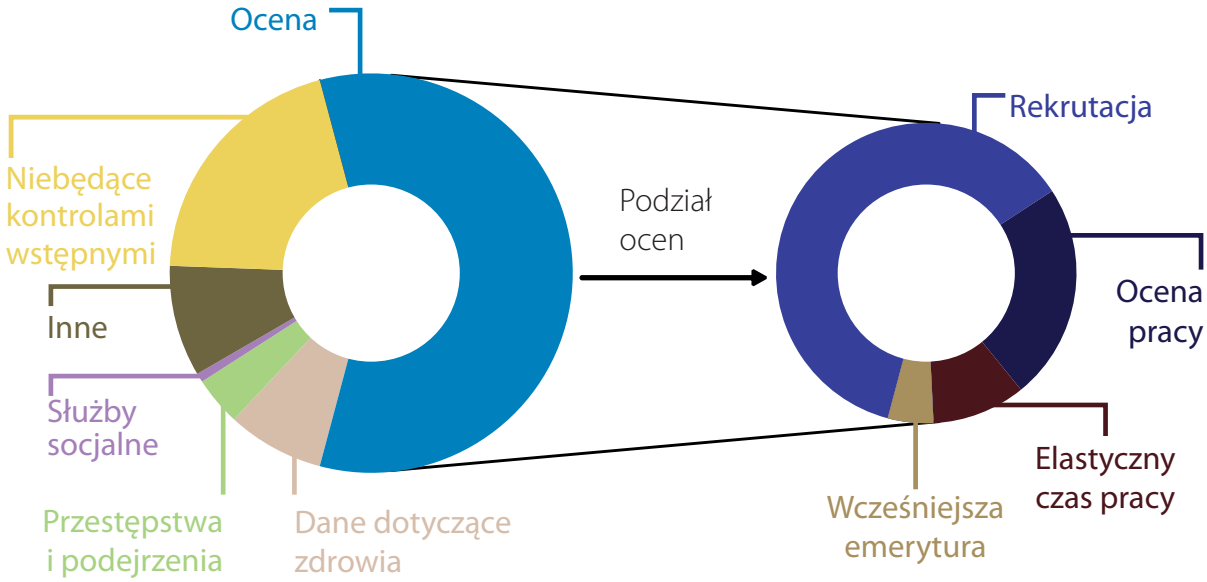
W październiku 2008 r. EIOD wdrożył nową procedurę przeprowadzania kontroli wstępnych *ex post* w agencjach UE. Ponieważ w wielu przypadkach standardowe procedury są takie same w większości agencji UE i opierają się na decyzjach Komisji, polega ona na zebraniu powiadomień na podobne tematy i przyjęciu 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. rozdz. 2.7 Wytyczne tematyczne). Następnie inspektor ochrony danych agencji przedkłada powiadomienie na mocy art. 27 wraz z pismem przewodnim wskazującym konkretne aspekty związane ze stanowiskiem EIOD w tej dziedzinie (szczególne aspekty przetwarzania w danej agencji, kwestie problematyczne itp.).

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 okresie poprzedzającym przyjęcie opinii horyzontalnej na początku 2010 r. EIOD nadal otrzymywał powiadomienia w tej dziedzinie.

2.3.3. Najważniejsze zagadnienia związane z kontrolami wstępnymi

Opinie w 2009 r. wg kategorii



Dane medyczne i inne dane związane ze zdrowiem

Europejskie instytucje i agencje przetwarzają dane medyczne i inne dane związane ze zdrowiem osób fizycznych w licznych sytuacjach związanych z zastosowaniem regulaminów pracowniczych (badania lekarskie poprzedzające rekrutację, coroczne badania lekarskie, zwrot wydatków medycznych, zwolnienia lekarskie itp.). Ze względu na szczególnie wrażliwy charakter danych związanych ze zdrowiem operacje przetwarzania dotyczące tych danych podlegają kontroli wstępnej EIOD.

W 2009 r. EIOD przyjął kolejne opinie dotyczące danych związanych ze zdrowiem (zob. wykres powyżej).

We wrześniu 2009 r. EIOD wydał wytyczne w sprawie przetwarzania takich danych w świetle powiadomień o operacjach przetwarzania danych związanych ze zdrowiem przez agencje UE (zob. rozdz. 2.7. Wytyczne tematyczne). Wytyczne te spełniają też rolę zestawu standardów EIOD dla instytucji.

EIOD dokonał kontroli wstępnej w konkretnym przypadku dotyczącym przetwarzania danych związanych ze zdrowiem przez **system Parlamentu Europejskiego służący zapewnieniu bezpieczeństwa** (sprawa 2009-225). Gromadzenie danych w tym systemie ma na celu zapewnienie wsparcia dla misji poza trzema lokalizacjami, w których urzęduje PE, w razie nagłych przypadków. Podmiot danych podaje informacje dobrowolnie, będą one wykorzystane jedynie w nagłych

przypadkach i zostaną przekazane lokalnej służbie zdrowia tylko w razie potrzeby.

EIOD przyznał, że przetwarzanie danych związanych ze zdrowiem może nastąpić na podstawie zgody podmiotu danych zgodnie z art. 5 lit. d) i art. 10 ust. 2 lit. a) rozporządzenia. Chociaż EIOD podkreślił, że w kontekście zatrudnienia wykorzystanie „zgody" jako podstawy prawnej wiąże się z pewnymi ograniczeniami, niemniej w analizowanym przypadku podmiot danych ma swobodę wyboru, czy chce udostępnić wspomniane kategorie danych i jest informowany o możliwych konsekwencjach ich nieudostępnienia.

Przetwarzanie danych osobowych przez **międzyinstytucjonalne żłobki** w Brukseli (sprawa 2009-088) oraz przez żłobek i świetlicę w Luksemburgu (sprawa 2009-089) wiązało się z pewnymi zagadnieniami dotyczącymi ochrony danych medycznych. W przypadku przetwarzania dokonywanego przez brukselskie żłobki EIOD skrytykował w szczególności fakt, że przetwarzanie danych medycznych wychodzi poza weryfikację przyjęć do żłobków i reakcję w nagłych przypadkach, stanowiąc *de facto* monitorowanie medyczne dzieci przez służby medyczne Komisji.

EIOD zalecił, aby monitorowanie stanu zdrowia i wzrostu dzieci w żłobkach lub innych ośrodkach opieki dziennej przez służby medyczne odbywało się jedynie na zasadzie dobrowolności, po uzyskaniu wyraźnej zgody rodziców.

EIOD skrytykował również przyjęty przez Komisję 30-letni okres, przez który przechowywane są kartoteki medyczne dzieci zapisanych do brukselskich żłobków. Podobną krytykę skierowano pod adresem żłobka i świetlicy w Luksemburgu, gdzie dane medyczne są przechowywane przez 10 lat, a następnie archiwizowane. EIOD zalecił, aby dokonać przeglądu tych okresów zatrzymywania danych stosownie do konkretnych potrzeb dotyczących danych i kartotek. Ponadto EIOD zalecił, aby po opuszczeniu żłobka przez dziecko umożliwić rodzicom przeniesienie kartoteki medycznej dziecka do lekarza rodzinnego.

Ponadto w obydwu przypadkach EIOD uznał za niezbędne, aby personel pracujący w żłobku czy świetlicy, który ma dostęp do pewnych danych medycznych dotyczących dzieci, podlegał obowiązkowi zachowania tajemnicy.

Ocena personelu

Znaczna część operacji przetwarzania przedłożonych EIOD do wstępnej kontroli dotyczy oceny personelu; wiele operacji przetwarzania wiąże się z okresami próbnymi, procedurą oceny wyników i awansu (zob. wykres powyżej).

Szczególnie interesującym przykładem z dziedziny oceny jest opinia EIOD dotycząca **360-stopniowej oceny inteligencji emocjonalnej** przeprowadzanej w Europejskiej Szkole Administracji (EAS) Komisji Europejskiej (sprawa 2009-100).

Instytucje oraz organy UE gromadzą i przetwarzają dane dotyczące zdrowia.

Szczególny nacisk w swoich opiniach dotyczących oceny personelu EIOD kładł na **okres zatrzymywania** danych osobowych po przeprowadzeniu oceny.

Zdaniem EIOD **raporty z oceny** powinny być przechowywane tylko przez pięć lat po jej zakończeniu, chyba że toczy się postępowanie sądowe. Wszelkie decyzje wynikające z oceny powinny być przechowywane w aktach osobowych danego pracownika.

W sprawach tych EIOD stwierdził również, że **prawo do wprowadzenia poprawek**, jakie daje podmiotowi danych art. 14 rozporządzenia, może implikować możliwość domagania się przez podmiot danych wprowadzenia dowolnego postanowienia sądu lub innego organu w przypadku zmiany decyzji dotyczącej oceny lub awansu.

Celem tej procedury jest umożliwienie uczestnikom kursów organizowanych przez EAS uzyskania informacji zwrotnych w formie raportu, który ma im pomóc podwyższyć swoje kompetencje w dziedzinie samokontroli, kontaktów z ludźmi i komunikacji. Ocena jest przeprowadzana przy wykorzystaniu internetowego narzędzia „Emotional Intelligence-View 360". Na podstawie odpowiedzi uczestników i ich współpracowników generowany jest automatycznie raport, który nie ujawnia, w jaki sposób współpracownicy odpowiadali na pytania.

Chociaż EAS nie ma dostępu do danych przetwarzanych przez wykonawcę, wykonawca musi działać zgodnie z poleceniami EAS. Dlatego też EIOD uznał, że EAS jest administratorem przetwarzanych danych, gdyż określa ona cel ich przetwarzania oraz wykorzystywane środki (narzędzie internetowe). Tak więc wykonawca nie jest upoważniony do jakiegokolwiek przetwarzania wychodzącego poza zakres określony przez EAS i wskazany w umowie.

EIOD zalecił, aby EAS zbadała możliwości anonimowego korzystania ze wspomnianego narzędzia internetowego. Musiałyby przy tym zostać wzięte pod uwagę takie zmienne, jak rozwój infrastruktury informatycznej, procedury oraz koszty.

EIOD zajął się też kwestią **notatek roboczych**, które pracownik sporządzający raport może robić podczas spotkania dotyczącego oceny (sprawa 2007-0421) Według EIOD notatki te są robione przez pracowników sporządzających raporty w ramach ich obowiązków służbowych, a więc podlegają rozporządzeniu. Chociaż robienie notatek podczas procesu oceny nie jest niezgodne z prawem, szczególnie ważne jest, aby status tych „notatek osobistych" nie był nieokreślony, co skutkowałoby brakiem odpowiednich zabezpieczeń służących ochronie danych.

EIOD uznał, że wszelkie notatki osobiste robione przez pracownika sporządzającego raport (i dokonującego oceny) podczas rozmów powinny być niszczone po sporządzeniu raportu z oceny.

Znaczny odsetek powiadomień dotyczących kontroli wstępnej kierowanych do EIOD odnosi się do operacji przetwarzania związanych z oceną personelu.

Rekrutacja

Pod koniec 2008 r. EIOD wydał wytyczne w sprawie przetwarzania danych osobowych w ramach procedur rekrutacji w świetle powiadomień o takich operacjach przetwarzania danych przez agencje UE (zob. rozdz. 2.7. Wytyczne tematyczne).

EIOD zbadał konkretne procedury naboru w Parlamencie Europejskim, w szczególności przetwarzanie danych osobowych w ramach **przesłuchań desygnowanych Komisarzy** (sprawa 2009-332) oraz **wyboru Dyrektora Europejskiego Instytutu ds. Równości Kobiet i Mężczyzn** (sprawa 2008-785). W przypadku obydwu procedur dane gromadzono początkowo w Komisji Europejskiej i przekazywano Parlamentowi, który następnie przesłuchiwał kandydatów. EIOD zwrócił szczególną uwagę na informacje przedstawiane kandydatom przez Komisję Europejską podczas pozyskiwania od nich danych.

Wydano również zalecenia dotyczące przechowywania danych osobowych do celów historycznych. Chociaż nie było to problemem w przypadku konkretnych zbadanych procedur selekcyjnych, opinie dotyczące kontroli wstępnych ujawniły brak odpowiedniego, opartego na kryteriach ustalonych na szczeblu instytucji procesu selekcji i weryfikacji zmierzającego do zatrzymywania jedynie danych o wartości historycznej. EIOD wydał również zalecenia dotyczące środków bezpieczeństwa.

Narzędzia do pomiaru wyników

Hurtownia danych DG ds. Przedsiębiorstw i Przemysłu (EDW) jest systemem pobierającym dane z wielu źródeł oraz przetwarzającym i wiążącym je ze sobą w celu uzyskania miar, wskaźników oraz raportów dotyczących działalności tej DG w ramach Komisji Europejskiej (sprawa 2008-487). Na podstawie zgromadzonych informacji DG generuje raporty przedstawiające metryki wydajności pracy na użytek kierowników jednostek, dyrektorów oraz dyrektora generalnego. System nie ma zatem na celu pomiaru indywidualnych wyników pracy członków personelu, lecz ocenę wyników DG jako całości. W tym kontekście EIOD podkreślił, że wykorzystanie danych powinno ograniczać się do zakresu zadeklarowanego w powiadomieniu, tj. stworzenia tablicy wyników dla kierownictwa oraz raportowania rozbieżności między poszczególnymi źródłami danych.

EIOD podkreślił, że taka agregacja baz danych zwiększa ryzyko **rozrastania się funkcjonalności** w przypadku, gdy połączenie dwóch (lub większej liczby) baz danych zaprojektowanych w konkretnych celach skutkuje pojawieniem się nowego celu, którego ich projektanci nie przewidzieli, co stoi w oczywistej sprzeczności z zasadą ograniczania celów. Aby cel taki był dopuszczalny, jego zakres musi być w wyraźny sposób ograniczony, a jego konieczność wykazana. W związku z tym system EDW powinien ograniczać się do wykorzystania danych pochodzących z baz danych zadeklarowanych w powiadomieniu, a przed dodaniem innych źródeł danych niezbędne jest osobne zezwolenie.

Zarządzanie czasem

Systemy zarządzania czasem nadal budziły szczególne zainteresowanie, zwłaszcza gdy instytucje i organy UE decydowały się **łączyć systemy zarządzania czasem** z innymi systemami.

Trybunał Obrachunkowy miał zamiar połączyć system zarządzania audytem (ASSYST) z systemem zarządzania elastycznym czasem pracy Trybunału (EFFICIENT) za pośrednictwem narzędzia zwanego **ART** (sprawa 2008-239). Celem przetwarzania danych jest umożliwienie poszczególnym audytorom i kierownikom jednostek uzgodnienia czasu rejestrowanego przez systemy ASSYST i EFFICIENT, zapewnienie spójności między tymi systemami oraz weryfikacja ewentualnych rozbieżności.

EIOD podkreśla, że ponieważ agregacja baz danych zwiększa ryzyko „rozrastania się funkcjonalności", cel działania systemu musi być wyraźnie ograniczony, a jego konieczność wykazana. W tym konkretnym przypadku konieczności nie wykazano początkowo w jasny sposób, więc kwestię tę należy dodatkowo rozwinąć. Trybunał Obrachunkowy ostatecznie wdrożył wspomniane narzędzie.

EIOD zgłosił również pewne zastrzeżenia w swojej opinii dotyczącej planowanego systemu **porównującego zapisy elastycznego czasu pracy z danymi o dostępie fizycznym** do Sekretariatu Generalnego Rady (SGR) (sprawa 2009-477). SGR wykorzystuje system elastycznego czasu pracy rejestrujący czas pracy i obecność, co ułatwia ustalanie liczby nadgodzin i uprawnień urlopowych. EIOD dokonał już wcześniej kontroli wstępnej tej aplikacji. SGR dysponuje również systemem kontroli dostępu zarządzanym przez Biuro ds. Bezpieczeństwa i dostępnym

Zarządzanie czasem może wiązać się z kwestiami ochrony danych, zwłaszcza gdy instytucje UE decydują się łączyć systemy zarządzania czasem z innymi systemami.

dla służb administracyjnych w przypadku formalnych dochodzeń. Porównanie tych dwóch zestawów danych ma na celu identyfikację osób naruszających zasady dotyczące elastycznego czasu pracy oraz ocenę ich postępowania. Prawdopodobne jest też, że wprowadzenie systemu doprowadzi do wdrożenia środków dyscyplinarnych.

W swojej opinii EIOD uznał, że konieczność i proporcjonalność porównywania danych dotyczących elastycznego czasu pracy z danymi o dostępie fizycznym jest wątpliwa. Według EIOD brakuje racjonalnych dowodów na to, że wdrożenie systemu kontrolnego porównującego czas z kart zegarowych z danymi o dostępie fizycznym jest niezbędne w celu zarządzania personelem lub wypełniania funkcji SGR.

W związku z tym EIOD uznał, że planowane przetwarzanie naruszałoby przepisy rozporządzenia w kilku aspektach (konieczności i proporcjonalności, zmiany celu, jakości danych), chyba że byłoby dokonywane w związku z konkretnym dochodzeniem administracyjnym.

Dochodzenia w sprawie bezpieczeństwa

EIOD przeanalizował procedury wdrożone w celu uporania się z zagrożeniami dla interesów Komisji w dziedzinie **kontrwywiadu** i **zwalczania terroryzmu** (sprawa 2008-440). Zbadano dwie konkretne operacje przetwarzania: **dochodzenia w sprawie bezpieczeństwa** oraz **procedury sprawdzające**. Dochodzenia w sprawie bezpieczeństwa dotyczą przecieków informacji niejawnych UE zawinionych przez pracowników Komisji, natomiast procedury sprawdzające służą zapobieżeniu zatrudniania osób stanowiących zagrożenie dla interesów Komisji lub zawieraniu umów z takimi osobami.

EIOD z zadowoleniem przyjął różne środki wdrożone przez jednostkę odpowiedzialną za powyższe działania, w szczególności fakt, iż jednostka ta ocenia przede wszystkim w poszczególnych przypadkach **konieczność** przeprowadzenia procedury sprawdzającej, posługując się określonymi kryteriami. EIOD zalecił, aby podczas gromadzenia i przetwarzania danych osobowych śledczy brali pod uwagę również kryteria **proporcjonalności**.

Rejestracja głosu

*Rejestracja głosu podczas rozmów telefonicznych budzi szczególne obawy, gdyż nagrywanie rozmów jest naruszeniem **zasady poufności komunikacji**.*

EIOD zbadał zagadnienie nagrywania połączeń dla celów bezpieczeństwa w Instytucie Energii Wspólnego Centrum Badawczego (sprawa 2008-0014). Sprawa ta dotyczyła nagrywania połączeń przychodzących i wychodzących (wraz z informacją o numerze źródłowym i docelowym oraz dacie, czasie i długości połączenia) do celów wykorzystania w przypadku incydentów operacyjnych, awarii, oceny ćwiczeń awaryjnych oraz dochodzeń dotyczących potencjalnych zagrożeń. EIOD potwierdził, że rejestracja głosu podczas rozmów telefonicznych jest zgodna z krajowym ustawodawstwem dotyczącym instalacji jądrowych, zalecił jednak, by osoby z zewnątrz kontaktujące się z centralą były informowane na początku połączenia, iż będzie ono nagrywane do celów bezpieczeństwa.

EudraVigilance

Europejska Agencja Leków (EMEA) utrzymuje bazę danych EudraVigilance i zarządza nią; baza ta zawiera **sprawozdania dotyczące podejrzewanych niepożądanych reakcji na produkty lecznicze stosowane u ludzi** (indywidualne sprawozdania dotyczące bezpieczeństwa przypadku – ICSR). System EudraVigilance ułatwia raportowanie oraz

ocenianie takich sprawozdań. Informacje te przekazują właściwe organy krajowe, posiadacze pozwoleń na dopuszczenie do obrotu oraz organizatorzy badań klinicznych.

EIOD przeanalizował operacje przetwarzania danych związane z EudraVigilance oraz podkreślił wspólną odpowiedzialność poszczególnych administratorów danych za zapewnienie poszanowania praw podmiotów danych (sprawa 2008-402). Administratorzy danych zarówno na szczeblu krajowym, jak i UE muszą koordynować oraz łączyć wysiłki, by zapewnić przestrzeganie ustawodawstwa krajowego i prawodawstwa wspólnotowego w zakresie ochrony danych.

EIOD zalecił, aby EMEA zbadała możliwość anonimizacji lub pseudonimizacji informacji osobowych zawartych w indywidualnych sprawozdaniach dotyczących bezpieczeństwa przypadku oraz ograniczenia do minimum występowania danych osobowych w tych sprawozdaniach. Zalecił również, by EMEA wraz z krajowymi administratorami danych opracowała standardowy formularz powiadomienia służący dostarczaniu wymaganych prawem informacji osobom fizycznym, który powinien zawierać odniesienie do EudraVigilance.

Uchylanie immunitetów

Na mocy Protokołu w sprawie przywilejów i immunitetów Wspólnot Europejskich urzędników Wspólnot chronią pewne immunitety. **Biuro dochodzeń i dyscypliny** Komisji (IDOC) jest odpowiedzialne za ocenę wniosków dotyczących uchylenia tych immunitetów kierowanych przez sądy lub inne organy krajowe. EIOD dokonał kontroli wstępnej procedury wdrożonej przez IDOC w przypadku uchylania takich immunitetów (sprawa 2008-645).

W większości przypadków organy krajowe wnioskują, by IDOC przeprowadzał swoje dochodzenie w sposób tajny, co ogranicza prawa podmiotów danych, gdyż nie są one informowane o dochodzeniu ani nie mogą skorzystać ze swoich praw dostępu do danych i poprawienia ich podczas dochodzenia. EIOD wskazał, że wszelkie ograniczenia praw podmiotów danych muszą być tymczasowe, a podmiot danych musi być w stanie skorzystać ze swojego prawa dostępu, gdy tylko zniknie uzasadnienie dla tajności.

Po zakończeniu dochodzenia IDOC przekazuje podjęte decyzje wraz z pewnymi danymi wnioskującemu sądowi czy organowi krajowemu. EIOD zalecił, aby IDOC przechowywał listę odbiorców tych danych, odnotowując uzasadnienie prawne ich przekazania.

Ponieważ uchylenie immunitetu stanowi zazwyczaj część ogólniejszej procedury, która może, lecz nie musi skutkować dalszym postępowaniem, EIOD zalecił skrócenie okresu zatrzymywania akt, w przypadku gdy postępowanie dyscyplinarne lub sądowe jest umarzane lub podmiot danych zostaje uniewinniony.

Projekty pilotażowe

W trzech przypadkach projektów pilotażowych EIOD skorzystał ze sposobności, by przypomnieć instytucjom i agencjom o **zasadach związanych z kontrolami wstępnymi projektów pilotażowych**. Wydając zalecenia przed pełnym wdrożeniem systemu, EIOD pragnie zminimalizować konieczność późniejszych zmian ze strony administratora danych.

Wyniki projektu pilotażowego muszą zostać przeanalizowane i zakomunikowane EIOD **przed** wdrożeniem projektu końcowego; EIOD musi być też informowany o wszelkich modyfikacjach, które mogą mieć wpływ na przetwarzanie danych osobowych. Opinię z kontroli wstępnej należy traktować jako zamknięcie pełnej analizy projektu pilotażowego.

2.3.4. Konsultacje dotyczące potrzeby przeprowadzenia kontroli wstępnej

W 2009 r. EIOD odbył z inspektorami ochrony danych 21 konsultacji dotyczących potrzeby kontroli wstępnej (na podstawie art. 27 ust. 3 rozporządzenia), z czego 11 konsultacji z inspektorem ochrony danych Parlamentu Europejskiego.

*W kilku przypadkach stwierdzono, że dana sprawa **podlega kontroli wstępnej**, na przykład w odniesieniu do:*

- *danych związanych ze strajkiem w Europejskim Banku Centralnym,*
- *przesłuchań desygnowanych komisarzy w Parlamencie Europejskim,*
- *oceny ergonomicznej środowiska pracy w Parlamencie Europejskim,*
- *mianowania pracowników wyższych szczebli w Parlamencie Europejskim.*

Przetwarzania danych osobowych **przez służby prawne i jednostkę ds. prawnych Parlamentu Europejskiego** w kontekście ich obowiązków związanych z badaniem spraw, sporządzaniem odpowiedzi na wnioski i skargi oraz postępowaniami prawnymi nie uznano za podlegające kontroli wstępnej EIOD (sprawa 2009-263).

Sama potencjalna obecność **danych wrażliwych** nie czyni automatycznie danej sprawy przedmiotem kontroli wstępnej. Niemniej obecność danych wrażliwych, takich jak dane dotyczące zdrowia lub przestępstw, oznacza, że należy przywiązywać szczególną wagę do wdrożenia środków bezpieczeństwa zgodnie z art. 22 rozporządzenia.

Chociaż część operacji przetwarzania może wiązać się z oceną aspektów osobistych, przetwarzanie to nie ma na celu oceny podmiotu danych, tak więc art. 27 ust. 2 lit. b) nie ma tu zastosowania.

Podobnie jest w odniesieniu do art. 27 ust. 2 lit. d) – chociaż operacje przetwarzania mogą skutkować pozbawieniem jednostki prawa lub świadczenia lub wyłączeniem jej z umowy, nie jest to ich konkretnym i jedynym celem.

Z EIOD konsultowano się również w związku z przetwarzaniem danych osobowych w ramach **procedury selekcji asystentów posłów do PE.** Zgodnie z uzyskanymi informacjami procedury selekcji nie przeprowadza PE, w związku z czym EIOD uznał, że operacja przetwarzania nie powinna podlegać kontroli wstępnej. EIOD podkreślił jednak, że nie oznacza to, iż asystentom posłów do PE nie przysługują pewne prawa do ochrony danych, które muszą zostać zagwarantowane przez Parlament Europejski.

2.3.5. Powiadomienia niepodlegające kontroli wstępnej lub wycofane

W 2009 r. EIOD zajmował się również 21 sprawami, które po wnikliwej analizie uznano za niepodlegające kontroli wstępnej. W takich sytuacjach EIOD może mimo to wydać zalecenia.

Youthlink 2

Interesująca sprawa dotyczyła **Youthlink 2** – głównego repozytorium danych statystycznych i finansowych na temat projektów oraz działań przedłożonych w ramach programu Komisji Europejskiej „Młodzież w działaniu" (sprawa 2008-484).

Na podstawie przedstawionych faktów EIOD stwierdził, że wybór beneficjentów programu „Młodzież w działaniu" **nie wiąże się z oceną indywidualnego postępowania lub umiejętności**, polega natomiast na porównaniu zaproponowanego projektu z uprzednio zdefiniowanymi kryteriami oraz weryfikacji zdolności finansowych i operacyjnych podmiotów prawnych lub grup składających wniosek. Ponadto ocena taka jest przeprowadzana w sposób zdecentralizowany – nie przez administratora danych w obrębie Komisji Europejskiej, lecz przez agencje krajowe podlegające odpowiedniemu ustawodawstwu o ochronie danych lub przez Agencję Wykonawczą ds. Edukacji, Kultury i Sektora Audiowizualnego. Z tych powodów EIOD uznał, że art. 27 ust. 2 lit. b) rozporządzenia nie ma zastosowania.

Badanie zadowolenia klienta

EIOD uznał, że „**badanie zadowolenia klienta**" w Europejskim Banku Centralnym **nie podlega kontroli wstępnej**, gdyż celem badań nie jest ocena poszczególnych osób, lecz usług – podobnie jak celem audytu jest ocena zgodności działania jednostki organizacyjnej lub procesu z regulacjami, nie zaś ocena wyników pracy poszczególnych osób (sprawa 2008-780). EBC dołożył wysiłków, aby zminimalizować prawdopodobieństwo oceny aspektów osobistych jakiejkolwiek osoby. EIOD zasugerował jednak, aby EBC podjął dodatkowe kroki zmierzające do minimalizacji prawdopodobieństwa uwzględnienia w wynikach badań informacji osobistych, w szczególności pochodzących z odpowiedzi na pytania otwarte.

Wykorzystanie telefonów komórkowych

W związku z powiadomieniem dotyczącym **wykorzystania telefonów komórkowych** przez personel Agencji Wykonawczej ds. Konkurencyjności i Innowacyjności udający się na misje EIOD stwierdził, że sprawa ta **nie podlega kontroli wstępnej** (sprawa 2009-162). Celem przetwarzania było zagwarantowanie uzyskania przez Agencję zwrotu kosztów rozmów prywatnych. Ocena zdolności, wydajności pracy lub postępowania personelu wykraczała zatem poza zakres przetwarzania, które nie podlegało zapisom art. 27 ust. 2 lit. b).

Zarządzanie tożsamością i dostępem

EIOD uznał również, że kontroli wstępnej nie podlega **system zarządzania tożsamością i dostępem** Trybunału Obrachunkowego (sprawa 2009-639).

Chociaż system wykorzystuje pewne informacje (imię, nazwisko, datę urodzenia) w celu przyznania użytkownikom kont aplikacyjnych i umożliwienia dostępu do nich, nie „ocenia" wszakże osób, a jedynie weryfikuje ich tożsamość oraz prawa dostępu. Sama weryfikacja praw z wykorzystaniem uprzednio zdefiniowanych reguł nie wiąże się zatem *de facto* z oceną wydajności, kompetencji, zdolności do pracy lub zachowania użytkownika, a więc sprawa nie podlega art. 27 ust. 2 lit. b).

2.3.6. Dalsze działania po wydaniu opinii dotyczących kontroli wstępnej

*Opinia dotycząca kontroli wstępnej EIOD zawiera **zalecenia**, które należy uwzględnić, aby dana operacja przetwarzania była zgodna z rozporządzeniem. 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 przedsięwzięcia środków naprawczych. W przypadku gdy administrator danych nie stosuje się do tych zaleceń, EIOD może skorzystać z uprawnień przyznanych mu na mocy art. 47 rozporządzenia (WE) nr 45/2001. EIOD może w szczególności przekazać sprawę do danej instytucji lub organu wspólnotowego.*

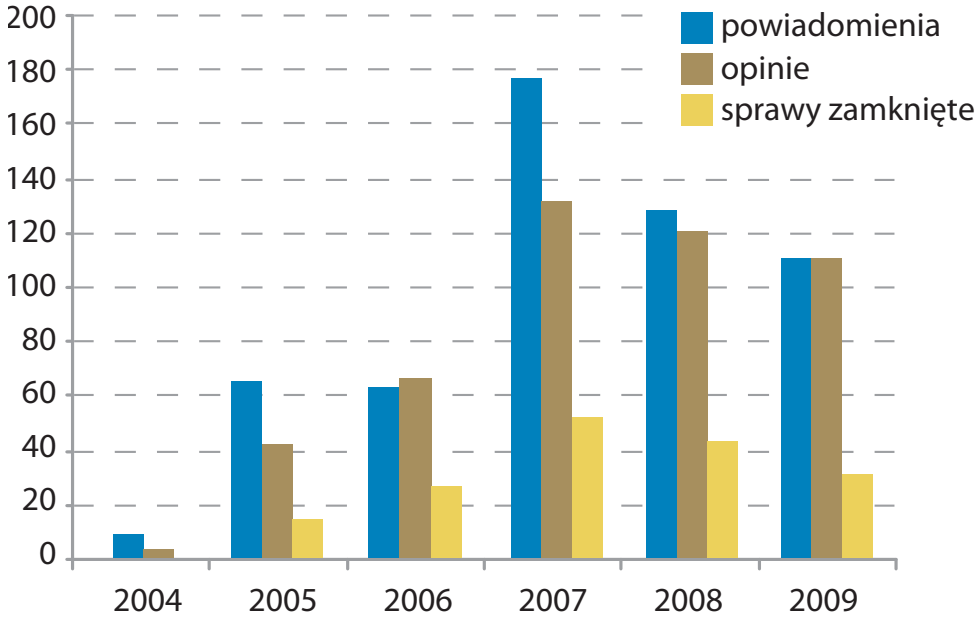
W większości przypadków kontrole wstępne skutkowały wydaniem zaleceń dotyczących:

- informacji dla podmiotów danych,
- okresów przechowywania danych,
- ograniczenia celów,
- prawa dostępu do danych i ich poprawy.

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 przedsięwziętych w celu realizacji zaleceń.

Pomimo przypomnień kierowanych do instytucji i organów, aby przedstawiały one takie informacje zwrotne, w 2009 r. EIOD zamknął tylko 32 sprawy, a wiele pozostało otwartych. EIOD wezwał w związku z tym instytucje i organy, aby wdrażały dalsze działania związane z opiniami, co pozwoli zamknąć sprawy.

Porównanie sytuacji



Każdy może skierować do EIOD skargę dotyczącą przetwarzania danych osobowych przez administrację UE.

2.3.7. Wnioski i przyszłość

Większość najważniejszych instytucji kończy przekazywanie powiadomień dotyczących prowadzonych operacji przetwarzania, a większość agencji czyni postępy w powiadamianiu o operacjach stanowiących część ich podstawowej działalności i związanych z przetwarzaniem danych osobowych oraz standardowych procedurach administracyjnych (zgodnie z nową procedurą ustanowioną dla agencji).

110 wydanych opinii dało EIOD dobry wgląd w operacje przetwarzania administracji europejskiej, pozwalając też podkreślić pewne zalecenia. Doświadczenia zgromadzone w związku ze stosowaniem rozporządzenia pozwoliły też EIOD zyskać wiedzę i wystosować ogólne wytyczne w pewnych dziedzinach (zob. rozdz. 2.7 Wytyczne tematyczne).

Większość kontroli wstępnych skutkowała wydaniem przez EIOD zaleceń związanych z wymogiem przedstawienia przez instytucje i organy informacji zwrotnych o ich realizacji. W 2009 r. zamknięto niewiele spraw, w związku z czym EIOD będzie naciskać na dalsze usprawnienia w tej dziedzinie.

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).

W interesującym przypadku dotyczącym **danych osoby niepełnoletniej** EIOD uznał, że z zasady rodzic sprawujący władzę rodzicielską ma prawo dostępu do danych dziecka. Sprawa dotyczyła dostępu do dokumentów związanych z rejestracją dziecka w żłobku zarządzanym przez instytucję UE. Skarżący zarzucił, że nie umożliwiono mu pełnego dostępu do tych dokumentów przedłożonych przez drugiego rodzica, z którym się rozwiódł.

W szczególności częściowo wymazano nazwiska osób uprawnionych do odbioru dziecka ze żłobka.

EIOD oświadczył, że z zasady rodzic sprawujący wspólną władzę rodzicielską ma prawo uzyskać dostęp do danych swojego dziecka. W przedmiotowej sprawie EIOD doszedł do wniosku, że prawo takie obejmuje również dane osób trzecich uprawnionych do odbioru dziecka, gdyż dane takie z natury powiązane są z danymi dziecka.

EIOD stwierdził, że odmawiając skarżącemu dostępu do danych jego dziecka w czytelnej formie, wspomniana instytucja naruszyła art. 13 rozporządzenia.

Zgodnie z rozporządzeniem EIOD może badać jedynie skargi przedłożone przez **osoby fizyczne**. Skargi przedkładane przez przedsiębiorstwa lub inne osoby prawne nie są dopuszczalne. Skarżący muszą również podać swoje dane, więc wnioski anonimowe 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).

Skarga do EIOD może dotyczyć jedynie przetwarzania danych osobowych. *EIOD nie ma kompetencji, by badać sprawy dotyczące niewłaściwego administrowania, modyfikować treść dokumentów, które kwestionuje skarżący, lub przyznawać odszkodowanie finansowe związane z poniesionymi szkodami.*

W szczególności fakt, że w rozporządzeniu mówi się o „poprawie danych osobowych", nie oznacza, że EIOD jest władny zmieniać treść decyzji, gdyż zawierają one pewne dane osobowe. W takich przypadkach skarżącemu zalecane jest zwrócenie się do Europejskiego Rzecznika Praw Obywatelskich lub właściwego sądu.

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 podstawami prawnymi, ogólnymi zasadami prawa UE oraz dobrymi praktykami administracyjnymi wspólnymi dla instytucji i organów UE. Aby ułatwić rozpatrywanie skarg, w grudniu 2009 r. EIOD przyjął **podręcznik wewnętrzny**, który zawiera wytyczne dla personelu je rozpatrującego. EIOD przeprowadził w szczególności wnikliwy przegląd warunków dopuszczalności skarg. W 2009 r. 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 jeden lub większą liczbę podmiotów danych w wyniku naruszenia;
- potencjalne ogólne znaczenie sprawy, również w odniesieniu do innych interesów publicznych lub prywatnych;
- prawdopodobieństwo stwierdzenia, że doszło do naruszenia;
- dokładną datę wydarzeń, wszelkie postępowanie, które nie powoduje już skutków, usunięcie tych skutków lub stosowne gwarancje ich usunięcia.

Każda skarga wpływająca do EIOD jest wnikliwie badana. Wstępne badanie skargi ma 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 informuje skarżącego o wszelkich innych właściwych organach (sąd, 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. Zamiast wszczynać dochodzenie w konkretnej sprawie przedłożonej przez skarżącego EIOD może na przykład wszcząć dochodzenie z własnej inicjatywy w związku z ogólnym problemem. W takich przypadkach skarżący jest informowany o podjętych innych środkach.

*EIOD otrzymał anonimową informację o tym, że dane osobowe kandydatów, którzy przeszli **wstępną selekcję** w konkursach na stanowiska urzędnicze w UE, są przetwarzane przez **zewnętrznego wykonawcę znajdującego się w państwie spoza UE**. EIOD wszczął w tej sprawie dochodzenie z własnej inicjatywy, które wykazało, że w rzeczywistości – mimo iż Europejski Urząd Doboru Kadr (EPSO) zawarł umowę z zewnętrzną firmą zarejestrowaną w Wielkiej Brytanii – same operacje przetwarzania danych są wykonywane w Stanach Zjednoczonych. EIOD nakazał EPSO sprawdzenie, czy wszystkie warunki określone w art. 9 rozporządzenia są przestrzegane, i zmianę umowy w celu zawarcia w niej dodatkowych gwarancji w odniesieniu do objętych nią podmiotów danych.*

Skarga jest z zasady niedopuszczalna, jeżeli skarżący nie skontaktował się w pierwszej kolejności z daną instytucją w celu zaradzenia sytuacji. 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.

Jeżeli chodzi o **ograniczenia czasowe**, jeżeli fakty dotyczące sprawy zostają przedstawione EIOD z opóźnieniem przekraczającym dwa lata, 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** w zakresie, który uznaje za właściwy. Dochodzenie to może obejmować wniosek do danej instytucji o udzielenie informacji, przegląd stosownych dokumentów, spotkanie z administratorem, kontrolę na miejscu itp. EIOD ma uprawnienia, by żądać 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, 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 podmiotom danych, przez ostrzeżenia lub upomnienia dla administratora, aż do nałożenia zakazu przetwarzania lub skierowania sprawy do Trybunału Sprawiedliwości.

Każda zainteresowana strona może zwrócić się do EIOD o rewizję 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).

2.4.3. Gwarancja poufności dla skarżących

EIOD zdaje sobie sprawę z faktu, że niektórzy skarżący narażają swoją karierę zawodową, ujawniając naruszenia 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 informacji osobistych 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.

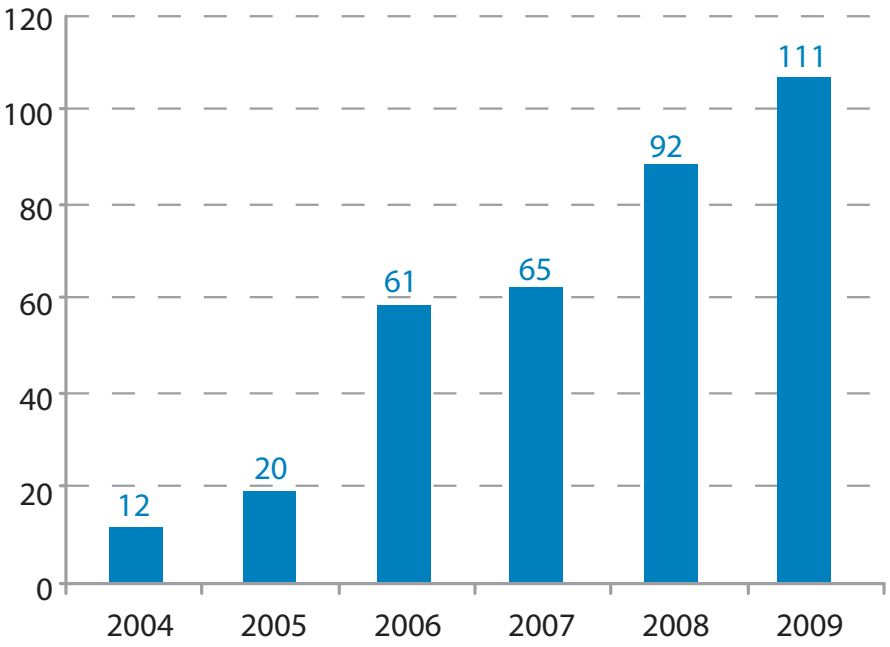
Jeżeli skarżący wnioskuje o **anonimowość** przed instytucją, inspektorem ochrony danych lub osobami trzecimi związanymi ze sprawą, jest wzywany do wyjaśnienia powodów takiego wniosku. Następnie EIOD analizuje argumenty skarżącego i bada konsekwencje wniosku z punktu widzenia możliwości przeprowadzenia dochodzenia. 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 wszelkie wnioski skarżącego o zachowanie poufności, a zatem nie pozwala na zidentyfikowanie skarżącego ani innych zainteresowanych osób.

2.4.4. Skargi rozpatrzone w 2009 r.

2.4.4.1. Liczba skarg

Liczba otrzymanych skarg (ewolucja 2004–2009)



Zarówno liczba, jak i złożoność skarg wpływających do EIOD wzrasta. ***W 2009 r. EIOD otrzymał 111 skarg*** *(o 32% więcej niż w 2008 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 42 skargi wymagały wnikliwszego zbadania (o 83% więcej niż w 2008 r.). Ponadto 14 dopuszczalnych skarg przedłożonych w latach poprzednich (13 w 2008 r. i jedna w 2007 r.) pozostawało na etapie dochodzenia lub rewizji.*

2.4.4.2. Skarżący

Spośród 111 otrzymanych skarg 26 (23%) pochodziło od pracowników instytucji lub organów UE, w tym byłych pracowników i kandydatów do pracy. Jedna skarga była anonimowa, a w przypadku pozostałych 84 skarg skarżący, jak się wydaje, nie pozostawali w stosunku pracy z administracją UE.

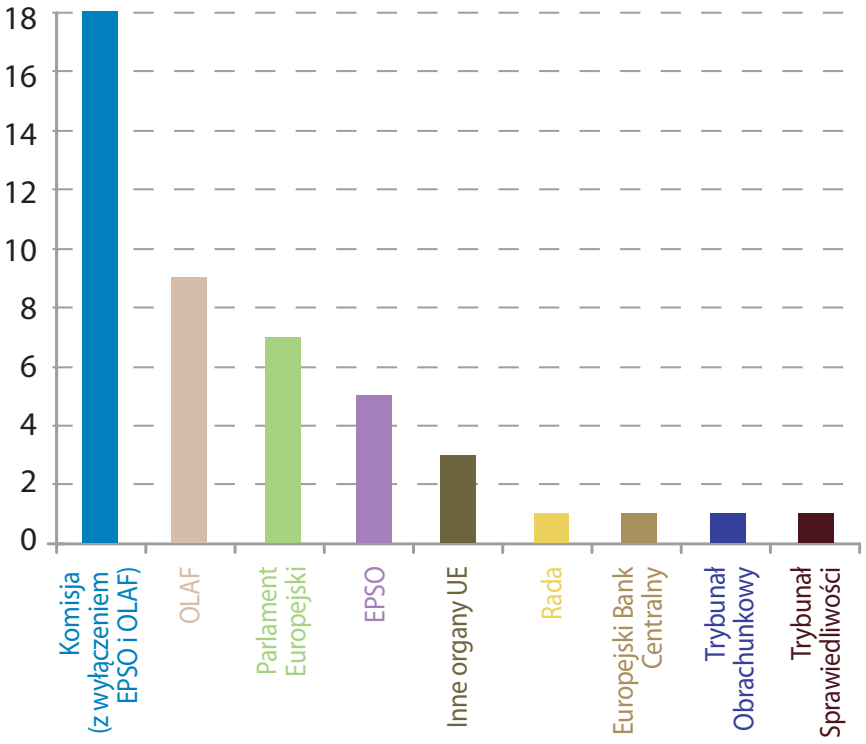
2.4.4.3. Instytucje, których dotyczyły skargi

Spośród dopuszczalnych skarg przedłożonych w 2009 r. większość (ponad 70%) dotyczyła **Komisji Europejskiej, w tym OLAF-u i EPSO**. Nie jest to zaskakujące, ponieważ Komisja przetwarza dane osobowe na większą skalę niż inne instytucje i organy UE. Znaczną liczbę skarg dotyczących OLAF-u i EPSO można wyjaśnić charakterem działań podejmowanych przez te organy.

2.4.4.4. Język skarg

Większość skarg przedłożono w języku angielskim (64%); rzadziej wykorzystywane były niemiecki (19%) i francuski (9%). Skargi w innych językach są względnie rzadkie (8%).

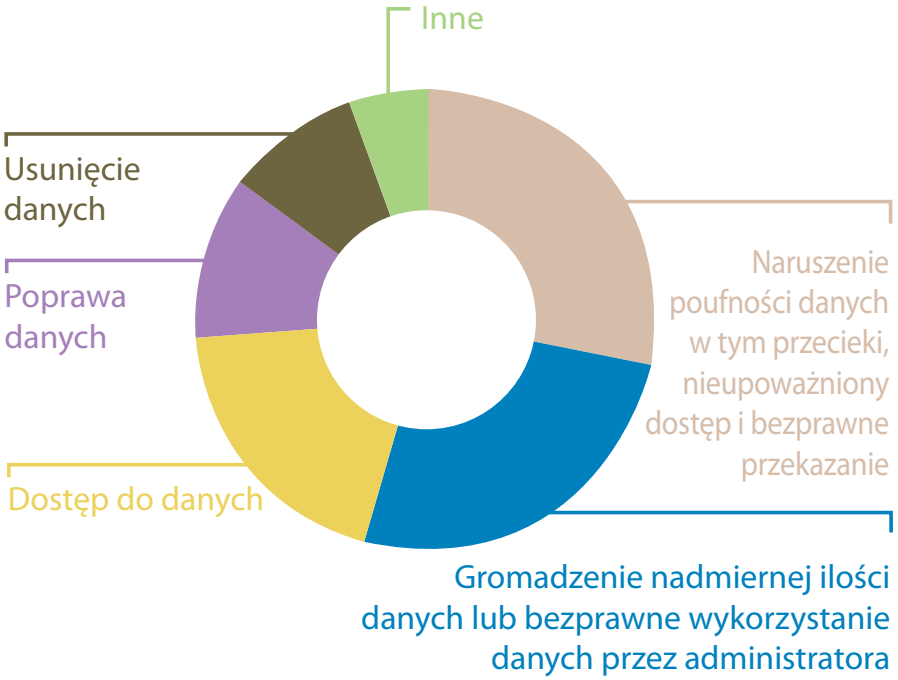
Skargi według instytucji



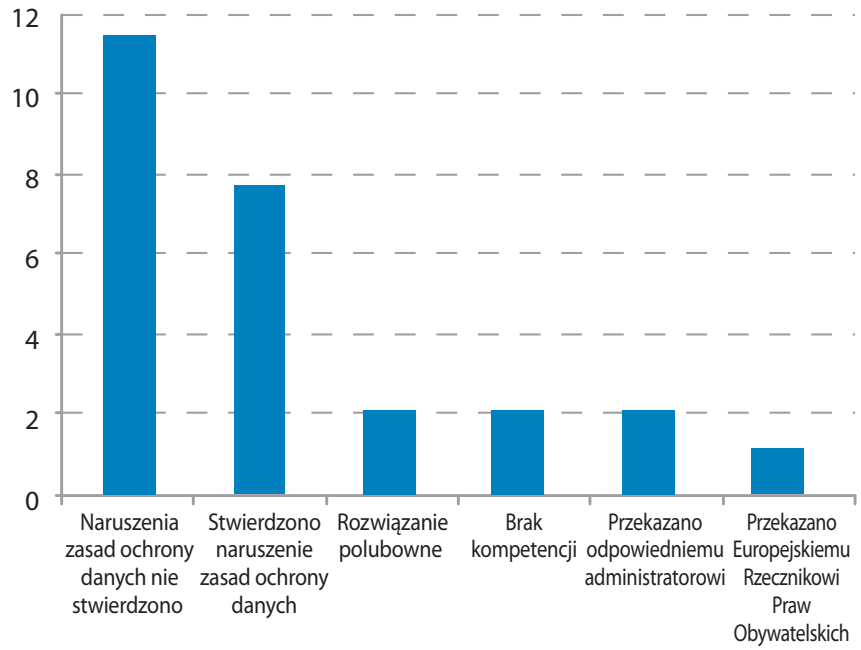
2.4.4.5. Rodzaje zarzucanych naruszeń

Najważniejszymi rodzajami naruszeń zasad ochrony danych zarzucanymi przez skarżących w 2009 r. były: naruszenie poufności danych (w tym przecieki), nieupoważniony dostęp i bezprawne przekazanie danych (31%) oraz gromadzenie nadmiernej ilości danych lub bezprawne wykorzystanie danych przez administratora (28%). Inne naruszenia zarzucano rzadziej; dotyczyły one kwestii dostępu do danych (20%), poprawek dotyczących danych (12%), kasowania danych (10%), nadzoru wideo (2%), przekazania danych poza UE (2%) oraz utraty danych (2%).

Rodzaje zarzucanych naruszeń



Wyniki dochodzeń EIOD



2.4.4.6. Rezultaty dochodzeń EIOD

W 12 sprawach rozstrzygniętych w 2009 r. EIOD nie stwierdził naruszenia zasad ochrony danych.

W sprawie przeciwko Komisji Europejskiej były pracownik zaskarżył odmowę udostępnienia mu egzemplarza raportu dotyczącego dochodzenia administracyjnego przeprowadzonego przez Komisję. Komisja odmówiła udostępnienia pełnego tekstu raportu, uzasadniając odmowę koniecznością ochrony praw i wolności innych osób, w szczególności świadków, którzy zeznawali w tej sprawie. Udostępniła jednak skarżącemu dotyczące go ustalenia faktyczne i wnioski końcowe raportu. Ze względu na fakt, że udostępnienie pełnego tekstu mogło rzeczywiście mieć negatywne skutki dla niektórych osób, których dotyczyła sprawa, EIOD uznał, że działania Komisji spełniły wymagania określone w art. 13 rozporządzenia przy zachowaniu praw i wolności innych osób.

Z kolei w 8 przypadkach doszło do naruszenia zasad ochrony danych i skierowano zalecenia do administratora danych.

W jednym z przypadków pracownik zaskarżył niestosowność działań organu w odniesieniu do dochodzenia dotyczącego kwalifikacji zawodowych pracownika. Skarżący zarzucił, że jego pracodawca bezprawnie przekazał „oznaczone jako poufne" dokumenty poświadczające te kwalifikacje odbiorcom w obrębie instytucji UE i poza nimi.

Na podstawie informacji dostarczonych przez administratora danych EIOD stwierdził, że przekazywanie danych w obrębie UE było niezbędne, aby odbiorcy mogli wykonywać swoje zadania zgodne z prawem. Jeżeli chodzi o przekazanie danych osobom trzecim, EIOD zgodził się wprawdzie, że zostało ono dokonane zgodnie z art. 8, uznał jednak, iż przekazanie danych firmie zajmującej się konsultingiem medialnym (wynajętej, aby obsługiwała potencjalne relacje prasowe dotyczące dochodzenia) było nadmierne w świetle zadań wykonywanych przez tego odbiorcę. EIOD uznał więc, że takie przekazanie danych stanowi naruszenie zasady jakości danych, a właściwy organ UE naruszył tym samym art. 4 ust. 1 lit. c) rozporządzenia.

W 2 przypadkach EIOD przyczynił się do osiągnięcia nieformalnego porozumienia między skarżącym a daną instytucją i żadna decyzja nie została wydana.

2.4.5. Dalsze prace w dziedzinie skarg

Przyjęcie **wewnętrznego podręcznika rozpatrywania skarg** w grudniu 2009 r. ułatwiło przebudowę odpowiednich stron internetowych EIOD. Nowa strona opisuje główne elementy procedury i umożliwia pobranie formularza służącego do złożenia skargi; zawiera też informacje o dopuszczalności skarg. Informacje te zostały udostępnione na stronie internetowej EIOD na początku 2010 r. i pomogą potencjalnym skarżącym w składaniu skarg. Oczekuje się również, że ograniczą one liczbę skarg w oczywisty sposób niedopuszczalnych oraz dostarczą EIOD pełniejszych i istotnych z jego punktu widzenia informacji, co umożliwi skuteczniejsze rozpatrywanie skarg. Istnieje szansa, że w następnej kolejności pojawi się interaktywna wersja formularza służącego do składania skargi, który użytkownicy będą mogli wypełnić na ekranie, a następnie przesłać automatycznie do EIOD.

2.5. Monitorowanie przestrzegania przepisów

Zgodnie z art. 41 ust. 2 rozporządzenia EIOD jest odpowiedzialny za monitorowanie i zapewnienie stosowania rozporządzenia (WE) nr 45/2001. Monitorowanie prowadzono w szczególności w ramach działania sprawozdawczego znanego pod nazwą „Wiosna 2009". Stanowiło ono kontynuację podobnej inicjatywy („Wiosna 2007") i miało formę pism skierowanych do dyrektorów instytucji i organów UE, w których zawarto wnioski o informacje na temat postępów w niektórych dziedzinach. Oprócz tego ogólnego monitorowania przeprowadzono kontrole w niektórych instytucjach i organach w celu sprawdzenia przestrzegania przepisów w konkretnych dziedzinach.

2.5.1. Działanie „Wiosna 2009"

Po zakończeniu działania EIOD wydał drugi ogólny raport dotyczący postępów we wdrażaniu zasad ochrony danych przez instytucje i organy UE. Zgodnie z raportem instytucje wspólnotowe osiągnęły ogólnie zadowalające postępy w spełnianiu wymogów ochrony danych, choć w przypadku agencji poziom zgodności z przepisami był niższy.

Najważniejsze wyniki w przypadku instytucji

- **IWykaz operacji przetwarzania:** EIOD zyskał przekonanie, że wszystkie instytucje z wyjątkiem jednej sporządziły wykaz operacji przetwarzania obejmujących dane osobowe, co pozwala na bardziej systematyczne podejście do ich wdrażania;
- **IPowiadamianie inspektorów ochrony danych o operacjach przetwarzania przez administratorów:** EIOD odnotował wzrost liczby instytucji, które zakończyły ten proces. Na koniec 2008 r. co najmniej sześć instytucji mogło wykazać się powiadomieniem inspektora ochrony danych o wszystkich operacjach przetwarzania, podczas gdy na początku 2008 r. były to tylko dwie instytucje;
- **IPowiadamianie EIOD o operacjach przetwarzania do celów kontroli wstępnej:** jak do tej pory tylko dwie instytucje zdołały powiadomić EIOD o wszystkich prowadzonych operacjach do celów kontroli wstępnej. Większość instytucji wskazała jednak, że EIOD zostanie powiadomiony o wszystkich zidentyfikowanych operacjach przetwarzania do końca 2009 r.

Najważniejsze wyniki w przypadku agencji

EIOD zauważył, że **nastąpił postęp** w identyfikacji operacji przetwarzania oraz przyjmowaniu przepisów wykonawczych dotyczących zadań i obowiązków inspektora ochrony danych. Liczba powiadomień o operacjach przetwarzania danych kierowanych do inspektora ochrony danych i dalej do EIOD w celu kontroli wstępnej była jednak na ogół bardzo niska. Tylko jedna agencja stwierdziła, że EIOD został powiadomiony o wszystkich zidentyfikowanych operacjach.

Chociaż nie było żadnych lub było bardzo niewiele wniosków o dostęp do danych na mocy rozporządzenia, EIOD z zadowoleniem odnotował, że agencje rozważają ustanowienie narzędzi monitorowania w celu rejestracji tych wniosków.

Dalsze działania

EIOD będzie wspierać i uważnie monitorować dalsze postępy, w szczególności w tych instytucjach i agencjach, gdzie poziom przestrzegania przepisów dotyczących powiadamiania EIOD do celów kontroli wstępnej oraz inspektora ochrony danych należy poprawić. W celu oceny dalszych postępów

zostaną wystosowane kolejne zapytania dotyczące przestrzegania przepisów.

2.5.2. 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 lub instytucja bądź organ UE prowadzi działalność. Kontrole mogą następować na podstawie skargi lub z własnej inicjatywy EIOD.

Artykuł 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 2009 r. EIOD kontynuował kontrole ogłoszone w ramach działania „Wiosna 2007", w szczególności w Parlamencie Europejskim i EPSO, a także rozpoczął kontrolę w Europejskim Trybunale Obrachunkowym. W lipcu 2009 r., na podstawie doświadczeń zgromadzonych w trakcie kontroli, EIOD przyjął wewnętrzny podręcznik procedur kontrolnych i opublikował najważniejsze elementy tych procedur na swojej stronie internetowej.

Polityka i procedura kontroli EIOD

Rolą **wewnętrznego podręcznika kontroli dla personelu** EIOD jest dostarczenie wytycznych pracownikom EIOD. Opiera się on zasadniczo na istniejących podstawach prawnych, ogólnych zasadach prawa UE oraz dobrych praktykach administracyjnych wspólnych dla instytucji i organów UE.

Podręcznik zawiera szczegółowe informacje na temat postępowania administracyjnego, zadań kontrolerów, a także polityki bezpieczeństwa, jak również standardowe formularze służące do sporządzania dokumentów kontrolnych. Objaśnia on funkcje tych dokumentów oraz dostarcza użytecznych wskazówek dotyczących przygotowania kontroli.

Podręcznik kontroli jest dokumentem otwartym, podlegającym regularnym przeglądom w miarę ewolucji praktyk i doświadczeń EIOD. W stosownym czasie opracowany zostanie dokument określający politykę w zakresie roli kontroli oraz kryteriów ich przeprowadzania.

Kontrola w Parlamencie Europejskim

W lutym 2009 r. EIOD przeprowadził kontrolę w Parlamencie Europejskim. Celem kontroli było zbadanie okoliczności operacji przetwarzania danych osobowych przez służby medyczne w Brukseli i Luksemburgu oraz przez służbę ds. zwolnień lekarskich w związku z trzema opiniami z kontroli wstępnych wydanymi przez EIOD. Celem była także kontrola realizacji zaleceń zawartych w tych opiniach. Przedmiotem kontroli był również obowiązek administratorów danych w Dyrekcji Generalnej ds. Polityki Zewnętrznej (DG EXPO) dotyczący powiadomienia inspektora ochrony danych o operacjach przetwarzania danych osobowych na mocy art. 25 rozporządzenia.

Po przeprowadzeniu kontroli EIOD wyraził obawy dotyczące pewnych niedociągnięć (organizacyjnych, fizycznych i technicznych) w zakresie **bezpieczeństwa informacji przechowywanych przez służby medyczne**, wskazując potrzebę wprowadzenia znaczących usprawnień. EIOD nakazał w szczególności znalezienie właściwego rozwiązania w zakresie przekazywania przez służbę ds. zwolnień lekarskich dokumentacji medycznej służbie medycznej.

EIOD przesłał listę zaleceń do sekretarza generalnego Parlamentu i nakazał mu podjąć odpowiednie środki. Niektóre z tych środków zostały później wdrożone, nadal trwają jednak działania związane z tą kontrolą.

Kontrola w Europejskim Urzędzie Doboru Kadr

W marcu 2009 r. EIOD przeprowadził kontrolę w Europejskim Urzędzie Doboru Kadr (EPSO). Celem kontroli było zbadanie okoliczności operacji przetwarzania danych osobowych w związku z kilkoma kontrolami wstępnymi w zakresie doboru urzędników, pracowników czasowych i kontraktowych, jak również wszelkich związanych z tym operacji przetwarzania danych osobowych.

Kontrola wykazała, że EPSO poczynił znaczne **postępy w odniesieniu do przejrzystości** swoich procedur i informacji dostarczanych kandydatom. W swoich wnioskach EIOD ponownie wskazał jednak obowiązek przedstawienia przez EPSO arkuszy oceny sporządzonych przez komisję konkursową podczas egzaminów ustnych tym kandydatom, którzy o to wystąpią. Podczas kontroli nie badano kwestii dostępu do pytań w testach wielokrotnego wyboru, gdyż trwa dotyczące jej postępowanie sądowe.

Jeżeli chodzi o **politykę przechowywania**, EIOD wezwał do sporządzenia udokumentowanej procedury archiwizacji akt w archiwach historycznych Komisji.

Celem kontroli była również weryfikacja zgodności z przepisami **wybranych baz danych EPSO i narzędzi informatycznych** wykorzystywanych podczas procedur selekcyjnych. EIOD nakazał ogólnie udokumentowanie technicznych i organizacyjnych środków bezpieczeństwa oraz bardziej systematyczne ich uwzględnienie w procedurach konkursowych.

Wnioski z kontroli zostały przesłane do dyrektora EPSO, który przyjął plan działań związany z zaleceniami wydanymi przez EIOD. Jako że wspomniany plan działań jest elementem planu ciągłego doskonalenia, w związku z którym dokonywany jest przegląd procedur, EIOD sformułuje ostateczne wnioski na początku 2010 r.

Kontrola w Europejskim Trybunale Obrachunkowym

W marcu 2009 r. EIOD przeprowadził kontrolę w Europejskim Trybunale Obrachunkowym (ETO) w odniesieniu do **personelu monitorującego** (raport dotyczący narzędzia służącego do monitorowania Internetu i audytu).

EIOD z zadowoleniem przyjął zastosowanie przez ETO **technik filtrowania**, które umożliwiają podejście zapobiegawcze do niewłaściwego wykorzystywania Internetu w miejsce podejścia represyjnego. EIOD uznał w szczególności za niewłaściwe cechy i funkcje filtrów programowych wykorzystywane w celu monitorowania nieudanych prób uzyskania dostępu do Internetu i zwrócił uwagę na znaczenie **oceny wpływu na prywatność** jako narzędzia wykorzystywanego w procesie doboru oprogramowania do celów monitorowania. EIOD uznał również za najlepszą praktykę zastosowanie zasad **wbudowanej ochrony prywatności** w całym procesie projektowania systemów i procesów służących do monitorowania Internetu oraz sieci. EIOD wezwał ETO do udoskonalenia polityki mającej zapewnić utrzymanie **wysokiego poziomu zgodności polityki bezpieczeństwa z przepisami** w celu opracowania niezawodnych, bezpiecznych, sprawiedliwych oraz cechujących się poszanowaniem prywatności i zasad ochrony danych procedur monitorowania Internetu.

Jeżeli chodzi o aspekt kontroli odnoszący się do konsultacji w sprawie procedury **dostępu do prywatnych nośników i poczty elektronicznej pracowników**, EIOD przeanalizował stosowne cele i obecne praktyki ETO, po czym stwierdził, że istnieje zagrożenie naruszenia poufności komunikacji. W związku z tym EIOD podkreślił konieczność formalnego powiadomienia go w celu przeprowadzenia wstępnej kontroli tej operacji przetwarzania, ponieważ stwarza ona konkretne zagrożenie zgodnie z art. 27 ust. 1 rozporządzenia.

Kontrola s-TESTA

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

Jako organ nadzorujący systemy informatyczne i aplikacje Komisji Europejskiej, które przetwarzają dane osobowe, EIOD postanowił we wrześniu 2009 r. przeprowadzić kontrolę sieci s-TESTA, a konkretnie jej Centrum Usługowo-Operacyjnego w Bratysławie. Komisja Europejska powierzyła zarządzanie Centrum wykonawcy – Orange Business Services/Hewlett Packard (OBS/HP). Głównym celem kontroli było zgromadzenie informacji dotyczących bezpieczeństwa i ochrony danych oraz wdrożonych środków i porównanie ich z wymaganiami określonymi w umowie oraz odpowiednich regulacjach. Kontrola EIOD dotyczyła w tym zakresie infrastruktury Centrum, jego personelu, organizacji i technologii.

EIOD był ogólnie zadowolony ze środków bezpieczeństwa określonych w wymaganiach KE i wdrożonych przez OBS/HP w odniesieniu do systemów informatycznych, aplikacji oraz procesów organizacyjnych w Centrum. Wprowadzenie różnych udoskonaleń w zakresie bezpieczeństwa oraz wdrożenie planu ciągłego doskonalenia poskutkuje powstaniem jeszcze bardziej niezawodnego mechanizmu ochrony danych.

2.6. Środki administracyjne

*W art. 28 ust. 1 rozporządzenia (WE) nr 45/2001 stwierdza się, że EIOD ma prawo do uzyskiwania informacji o środkach administracyjnych, które dotyczą przetwarzania danych osobowych. 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 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 lub w kwestiach ogólnych dotyczących interpretacji rozporządzenia.

W ramach konsultacji w sprawie środków administracyjnych planowanych przez instytucje i organy poruszano rozmaite zagadnienia; były wśród nich na przykład:

- przekazywanie danych osobowych do państw trzecich;
- przetwarzanie danych osobowych w ramach procedury związanej z pandemią;
- korzystanie z prawa dostępu;
- stosowanie zasad ochrony danych do Służby Audytu Wewnętrznego;
- przepisy wykonawcze do rozporządzenia (WE) nr 45/2001.

2.6.1. Przekazywanie danych osobowych do państw trzecich

Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) zadał pytanie, czy trzy grupy państw można uznać za gwarantujące **wystarczający poziom ochrony danych** w świetle ich stosunku do Konwencji Rady Europy nr 108 i protokołu dodatkowego do niej.

OLAF zadał również pytanie, czy jednej lub większej liczby spośród tych grup nie należy uznać za niegwarantującą wystarczającego poziomu ochrony w rozumieniu rozporządzenia o ochronie danych (art. 9 ust. 1) – czy zobowiązania podjęte przez nie w kontekście Konwencji lub umów o wzajemnej pomocy administracyjnej w sprawach celnych są uważane za „odpowiednie zabezpieczenia" (art. 9 ust. 7) (sprawa 2009-0333).

Po analizie EIOD stwierdził, że **nie ma wystarczających dowodów** zadowalającego wdrożenia Konwencji nr 108 i protokołu dodatkowego do niej we wskazanych państwach. Dlatego też w zasadzie nie można uznać, że te trzy grupy państw gwarantują wystarczający poziom ochrony.

EIOD dodał jednak, że OLAF może rozważyć przeprowadzenie oceny, czy jest możliwe przekazanie konkretnych danych (lub przekazanie ich w pewnych przypadkach) przy ograniczeniu ich do konkretnych celów i odbiorców w państwie przeznaczenia, co efektywnie zapewniłoby wystarczający poziom ochrony. Taka ocena wiązałaby się z przeglądem prawa krajowego, które wdraża Konwencję i protokół do niej, oraz samego ich wdrożenia.

EIOD wspomniał również, że trzecią możliwością mogłoby być wprowadzenie odpowiednich zabezpieczeń przez OLAF i odbiorców danych.

2.6.2. Przetwarzanie danych osobowych w ramach procedury związanej z pandemią

Z EIOD konsultowano się w kwestii przetwarzania danych osobowych przez **Europejski Bank Centralny** (EBC) w przypadku **pandemii** (sprawa 2009-0456). Oprócz przetwarzania danych osobowych przez służby medyczne EBC pandemia wymagałaby również informowania lokalnego kierownictwa o podejrzeniu, że dana osoba jest zarażona, aby ostrzec odpowiednich członków zespołu.

EIOD uznał, że w sytuacji braku obowiązków prawnych na szczeblu krajowym art. 5 lit. a) rozporządzenia może stanowić podstawę prawną do przetwarzania danych w ramach procedury związanej z pandemią. Ponieważ jednak jest to sytuacja wyjątkowa, byłoby pożądane, aby EBC podjął formalną decyzję, na której można byłoby oprzeć komunikację z kierownictwem.

Ponadto EIOD podkreślił, że ponieważ przetwarzanie obejmuje dane dotyczące zdrowia, jest ono

zabronione, chyba że zgodnie z art. 10 uda się znaleźć wyłączenie. Przetwarzanie danych dotyczących zdrowia może opierać się na obowiązku prawnym pracodawcy do przestrzegania wymogów związanych z bezpieczeństwem i higieną pracy. EIOD uznał również, że w omawianym przypadku wzgląd na *istotny interes publiczny* mógłby uzasadniać takie przetwarzanie danych dotyczących zdrowia, ale muszą zostać wprowadzone odpowiednie zabezpieczenia w celu ochrony interesów podmiotów danych.

2.6.3. Korzystanie z prawa dostępu

OLAF konsultował się z EIOD w sprawie hipotetycznego przypadku związanego przede wszystkim z korzystaniem z **prawa dostępu** (sprawa 2009-0550).

EIOD uznał, że wniosku o wykaz spraw, w których pojawiają się dane osobowe podmiotu danych, dotyczy z zasady art. 13 lit. a) rozporządzenia, ponieważ jest to sposób uzyskania *potwierdzenia, czy dane odnoszące się do niego są przetwarzane*. Sposób, w jaki potwierdzenie takie może być udzielone, zależy w pewnym stopniu od charakteru i cech danych oraz od rodzaju przetwarzania. Zależy on również od tego, czy dany sposób udzielenia potwierdzenia pozwalałby podmiotowi danych wykonywać przysługujące mu prawa do ochrony danych ([7]).

Podczas oceny metod i parametrów dostępu każdy przypadek należy oceniać indywidualnie. Informacje udzielone podmiotowi danych muszą być zrozumiałe (w zrozumiałej formie) oraz wskazywać, jakie przetwarzanie ma miejsce i jakich danych dotyczy. Poziom szczegółowości powinien umożliwiać podmiotowi danych ocenę ich poprawności oraz zgodność z prawem ich przetwarzania, jak również powinien być uzależniony od niezbędnego nakładu pracy administratora.

2.6.4. Zastosowanie zasad ochrony danych do Służby Audytu Wewnętrznego (IAS)

W obliczu zbliżającego się audytu zarządzania zasobami ludzkimi w Europejskiej Agencji Leków (EMEA) dyrektor EMEA ds. administracji wniósł, aby EIOD potwierdził, czy rozporządzenie ma zastosowanie do prac zespołu IAS podczas prowadzonego audytu (sprawa 2009-0097).

EIOD uznał, że IAS jest organem Wspólnoty przetwarzającym dane osobowe w ramach wykonywania czynności wchodzących w zakres obowiązującego w tej sytuacji prawa wspólnotowego, a zatem jeżeli IAS uzyskuje podczas audytu dostęp do danych osobowych, zastosowanie mają zasady określone w rozporządzeniu.

2.6.5. Przepisy wykonawcze do rozporządzenia (WE) nr 45/2001

Pewna liczba inspektorów ochrony danych przedstawiła EIOD do konsultacji opracowane w ich agencjach projekty przepisów wykonawczych do rozporządzenia nr 45/2001. EIOD odnotował, że wszystkie projekty dotyczyły nie tylko zadań, obowiązków i uprawnień inspektorów ochrony danych (art. 24 ust. 8 oraz załącznik do rozporządzenia), ale obejmowały również rolę administratorów oraz prawa podmiotów danych. Niektóre szczególnie istotne zalecenia EIOD dotyczyły następujących kwestii:

- inspektor ochrony danych powinien zapewnić wewnętrzne stosowanie przepisów rozporządzenia **w sposób niezależny**, nie otrzymując instrukcji od nikogo (sprawy 2009-0656 i 2009-0684);
- inspektor ochrony danych może korzystać z **pomocy z zewnątrz**, o ile nie zagraża to jego niezależności (sprawa 2009-0656);
- w razie potrzeby agencja powinna zorganizować **szkolenie w zakresie ochrony danych** (sprawa 2009-0656);
- pracownicy wspierający inspektora ochrony danych w wykonywaniu zadań powinni podlegać takiemu samemu obowiązkowi zachowania **tajemnicy zawodowej** jak inspektor ochrony danych (sprawa 2009-0684);
- **Komitet Pracowniczy** powinien również mieć możliwość konsultacji z inspektorem ochrony danych, który ogólnie powinien udzielać konsultacji bez konieczności zwracania się do niego w drodze urzędowej (sprawy 2009-0684, 2009-0204 i 2009-0163).

([7]) Zob. pkt 57 wyroku ETS w sprawie C-553/07 Rotterdam przeciwko Rijkeboer.

2.7. Wytyczne tematyczne

Doświadczenia zgromadzone w związku ze stosowaniem rozporządzenia (WE) nr 45/2001 pozwoliły personelowi EIOD przełożyć swoją wiedzę na ogólne wytyczne dla instytucji i organów. W 2009 r. EIOD opracował wytyczne na konkretne tematy w formie opracowań tematycznych.

2.7.1. Wytyczne w sprawie rekrutacji

Wytyczne EIOD w sprawie przetwarzania danych osobowych w związku z rekrutacją (przyjęte pod koniec 2008 r.) odnoszą się do cyklu procedur administracyjnych (selekcji, rekrutacji i ustaleń umownych) wdrożonych w celu naboru pracowników na stałe, jak również pracowników czasowych i kontraktowych, a także ekspertów krajowych i stażystów.

W wytycznych przeanalizowano między innymi **gromadzenie** przez instytucje danych dotyczących **karalności** w celu przestrzegania regulaminu pracowniczego: pracownik może zostać zatrudniony tylko pod warunkiem, że korzysta z pełni praw obywatelskich i może przedstawić odpowiednie referencje potwierdzające przydatność do wykonywania swoich obowiązków. EIOD uznał gromadzenie danych dotyczących karalności za zgodne z prawem. Podkreślił jednak, że sposób ich gromadzenia – w postaci różnych dokumentów, takich jak rejestr karny, kartoteki policyjne lub zaświadczenia o niekaralności – może prowadzić do gromadzenia nadmiernej ilości danych. Dokumenty te mogą zawierać informacje, które wykraczają poza uzasadniony cel stwierdzenia, czy osoba korzysta z pełni praw.

W wytycznych zaleca się zatem, aby analiza treści tych dokumentów odbywała się w sposób indywidualny, tak aby przetwarzane były jedynie dane stosowne w świetle wymagań regulaminu pracowniczego.

W odniesieniu do **okresu zatrzymywania** danych dotyczących karalności wytyczne wskazują na konieczność zwrotu informacji o karalności danej osobie bezpośrednio po selekcji i ewentualnej rekrutacji. Dokumenty te zawierają informacje aktualne w danej chwili, które mogą nie być dokładne już dzień po ich sporządzeniu. Do ewidencji i audytu można stworzyć standardowy formularz, w którym stwierdza się, że dana osoba jest przydatna do wykonywania swoich obowiązków oraz korzysta z pełni praw obywatelskich.

W wytycznych analizuje się również **przekazywanie danych na zewnątrz** – firmom organizującym testy w imieniu komisji rekrutacyjnej lub zewnętrznym ekspertom zatrudnionym w roli członków komisji rekrutacyjnej. Konieczność takiego przekazywania danych należy określić zgodnie z art. 8 lit. a). Ponadto dokładny zakres zadań wykonawców zewnętrznych należy określić w umowie lub akcie prawnym, a ich obowiązki w zakresie poufności i bezpieczeństwa należy zagwarantować zgodnie z art. 23 rozporządzenia.

Prowadząc nabór personelu, instytucje UE powinny dopilnować, aby gromadzone były tylko dane niezbędne.

2.7.2. Wytyczne w sprawie danych dotyczących zdrowia

We wrześniu 2009 r. EIOD wydał wytyczne na temat przetwarzania w miejscu pracy danych dotyczących zdrowia przez instytucje i organy UE.

W wytycznych przeanalizowano **podstawę prawną** przetwarzania danych dotyczących zdrowia przez instytucje i organy UE zgodnie z regulaminem pracowniczym, określając dopuszczalne cele i warunki przetwarzania danych dotyczących zdrowia. Regulamin pracowniczy przewiduje na przykład przetwarzanie danych dotyczących zdrowia w odniesieniu do badań lekarskich poprzedzających rekrutację w celu ustalenia, czy przyszły pracownik jest fizycznie zdolny do wykonywania swoich obowiązków. Regulamin nie wskazuje jednak, aby te same badania lekarskie przed rekrutacją mogły również służyć profilaktyce. Pomimo tego EIOD uznaje, że dane zebrane podczas tego badania lekarskiego mogą dodatkowo posłużyć poinformowaniu przyszłego pracownika o konkretnym problemie dotyczącym jego stanu zdrowia, a zatem mogą służyć profilaktyce. Nie oznacza to jednak, iż należy domagać się dodatkowych danych w celach profilaktycznych.

Wytyczne te powołują się również na **zasadę jakości danych.** Zasada ta oznacza ocenę wszystkich ankiet medycznych kierowanych do pracowników w celu zapewnienia, aby gromadzone oraz przetwarzane były tylko niezbędne i stosowne dane. Jeżeli podczas wizyty lekarskiej podmiot danych ma możliwość wykonania testu na obecność wirusa HIV, należy wyraźnie go poinformować, że test ten nie jest obowiązkowy i może zostać wykonany jedynie po wyrażeniu przezeń świadomej zgody, dotyczącej konkretnie tego testu. Z zasady jakości danych EIOD wywodzi również wniosek, że jeżeli pracownik zdecyduje się wykonać coroczne badanie lekarskie u wybranego przez siebie lekarza, wyniki tego badania mogą zostać przekazane służbie medycznej instytucji jedynie za dobrowolną i świadomą zgodą podmiotu danych.

2.7.3. Wytyczne w sprawie nadzoru wideo

W dniu 7 lipca 2009 r. EIOD opublikował przeznaczoną do konsultacji wersję wytycznych w sprawie nadzoru wideo. Wszystkie zainteresowane strony poproszono o przedstawienie pisemnych opinii, a w dniu 30 września 2009 r. w Brukseli zorganizowano warsztaty na ten temat. Udział wzięło prawie stu inspektorów ochrony danych, specjalistów ds. bezpieczeństwa, specjalistów ds. nadzoru wideo i technologii informatycznych, jak również przedstawicieli personelu z ponad czterdziestu instytucji i organów UE.

Dzięki warsztatom i procesowi konsultacyjnemu osiągnięto następujące dwa cele: uzyskano

Zastępca Inspektora Giovanni Buttarelli przemawia podczas warsztatów EIOD poświęconych projektowi wytycznych w sprawie nadzoru wideo (Bruksela, 30 września 2009 r.).

informacje zwrotne pozwalające udoskonalić projekt wytycznych i zacieśniono współpracę w celu zapewnienia przestrzegania zasad ochrony danych. Ogólna reakcja na projekt wytycznych była pozytywna. W związku z narastającymi obawami dotyczącymi coraz powszechniejszego wykorzystania nadzoru uczestnicy z zadowoleniem przyjęli fakt, że projekt wytycznych dostarcza praktycznych wskazówek ułatwiających podjęcie decyzji o zastosowaniu urządzeń nadzoru wideo oraz radzenie sobie z zagadnieniami ochrony danych.

Cele i najważniejsze zasady wytycznych w sprawie nadzoru wideo

EIOD zamierzał wydać wspomniane wytyczne na początku 2010 r. w dwóch celach: 1) działania na rzecz ograniczenia powszechności i zapobiegania niekontrolowanemu rozpowszechnianiu się nadzoru wideo, w przypadkach gdy nie jest on uzasadniony; oraz 2) wsparcia instytucji w odpowiedzialnym korzystaniu z nadzoru wideo i wdrażaniu zabezpieczeń, gdy stosowanie nadzoru wideo jest uzasadnione.

Najważniejsze tematy poruszone w wytycznych:
- *Jak wybrać, umiejscowić i skonfigurować system?*
- *Jak długo należy przechowywać nagrania?*
- *Kto powinien mieć dostęp do nagranego obrazu?*
- *Jakie środki bezpieczeństwa należy podjąć, by chronić dane?*
- *Jak informować osoby postronne?*
- *W jaki sposób realizować wnioski o dostęp do danych?*

Wytyczne mają zachęcić do podejmowania decyzji na szczeblu lokalnym w zależności od lokalnych potrzeb bezpieczeństwa, z jednoczesnym uwzględnieniem konkretnych obaw innych zainteresowanych stron, w tym pracowników. Podkreśla się w nich również rozliczalność instytucji, zalecając wprowadzenie formalnej polityki nadzoru wideo oraz przeprowadzanie okresowych audytów w celu zapewnienia i wykazania zgodności z przepisami. Wreszcie stanowią one dla instytucji zachętę do uwzględniania we wdrażanych technologiach oraz praktykach organizacyjnych mechanizmów ochrony prywatności i danych zgodnie z zasadą wbudowanej ochrony prywatności.

Konieczność i proporcjonalność

Wytyczne opierają się na zasadach konieczności i proporcjonalności, co z kolei powinno prowadzić do minimalizacji ilości gromadzonych danych oraz pomóc w powstrzymaniu niekontrolowanego rozprzestrzeniania się kamer bezpieczeństwa. Decyzje o instalacji kamer i sposobie korzystania z nich nie powinny być podejmowane wyłącznie z punktu widzenia potrzeb bezpieczeństwa. Należy zachować równowagę między tymi potrzebami a poszanowaniem podstawowych praw jednostki.

Pytania przed instalacją systemu:
- *Jakie są korzyści wynikające z zastosowania nadzoru wideo?*
- *Czy cel systemu jest jasno określony, wyraźny i zgodny z prawem?*
- *Czy istnieją podstawy prawne dla nadzoru wideo?*
- *Czy potrzebę nadzoru wideo jasno wykazano?*
- *Czy jest to najlepszy sposób osiągnięcia zamierzonego celu?*
- *Czy istnieją mniej inwazyjne alternatywy?*
- *Czy zyski przeważają nad skutkami niekorzystnymi?*

Niezależnie od powyższego ochrona danych nie powinna utrudniać pracy organów ścigania. Potrzeby w zakresie bezpieczeństwa i ochrony danych przedstawiane są często jako przeciwstawne oraz trudne do pogodzenia. Prawa podstawowe i bezpieczeństwo nie muszą się jednak wzajemnie wykluczać. Dzięki pragmatycznemu podejściu opartemu na zasadach selektywności i proporcjonalności systemy nadzoru mogą zaspokajać potrzeby w zakresie bezpieczeństwa przy jednoczesnym poszanowaniu prywatności. Technologie nadzoru powinny być wykorzystywane w sposób ukierunkowany, co zmniejsza do minimum skalę gromadzenia nieistotnych danych. Nie tylko minimalizuje to naruszenie prywatności, ale również pomaga zapewnić lepiej ukierunkowane, a tym samym efektywniejsze wykorzystanie nadzoru w celu rozwiązania problemu bezpieczeństwa. Podsumowując, EIOD dostrzega potrzebę selektywnego podejścia do korzystania z systemów nadzoru, tak aby wskutek działań mniejszości nadmierne ograniczenia nie dotykały reszty społeczeństwa.

Wbudowana ochrona prywatności i rozliczalność

Prywatności i ochrony danych nie można zapewnić wyłącznie przez zadbanie o zgodność z przepisami w poszczególnych obszarach. Gdy tylko jest to możliwe, trzeba stosować działania profilaktyczne: ochrona prywatności musi od samego początku być wbudowana w systemy wykorzystujące technologie informacyjne i komunikacyjne (TIK) oraz

Nadzór wideo musi być wykorzystywany w sposób odpowiedzialny i z zastosowaniem skutecznych zabezpieczeń.

praktyki organizacyjne. Wbudowana ochrona prywatności obejmuje nie tylko planowanie i projekt techniczny systemów TIK, ale również wymaga praktyk organizacyjnych kładących nacisk na rozliczalność i poszanowanie prywatności oraz infrastruktury fizycznej sprzyjającej zachowaniu prywatności. Nadzór wideo jest obszarem, gdzie zasady wbudowanej ochrony prywatności mogą okazać się szczególnie istotne i przydatne.

Systemy nadzoru wideo służące bezpieczeństwu lub innym celom nadzorczym powinny zawsze być projektowane z wykorzystaniem zasady wbudowanej ochrony prywatności, a wymogi ochrony danych powinny stanowić nieodłączny element opracowywania systemu. Systemy przetwarzania danych powinny być projektowane i dobierane pod kątem minimalizacji gromadzenia oraz wykorzystywania danych osobowych. Projektanci systemu powinni również określić dostępne techniki i jak najlepiej je wykorzystać. Kwestiami ochrony danych należy zająć się na wczesnym etapie. Przyczyny tego są oczywiste: w chwili gdy system już działa, trudniej jest wbudować weń rozwiązania sprzyjające ochronie danych, na przykład gwarantujące niezbędny poziom bezpieczeństwa, dające różne poziomy dostępu i zapewniające wiarygodną ścieżkę audytu lub prawa dostępu podmiotów danych.

Rozliczalność oznacza, że odpowiedzialna organizacja (administrator) powinna być w stanie wykazać, iż przestrzega obowiązków w zakresie ochrony danych. Sprzyja to wykorzystaniu ocen wpływu na prywatność i audytów dotyczących ochrony danych oraz prywatności, jak też redukuje znaczenie kontroli organów regulacyjnych, zwiększając wagę aktywnych działań podejmowanych przez samych administratorów. Konieczność wykazania zgodności zainteresowanym stronom i organom regulacyjnym oznacza również, że rozliczalność skutkuje większą przejrzystością – na przykład upublicznieniem polityki nadzoru wideo danej organizacji.

Systemy standardowe a ściślejsza kontrola

Celem wytycznych jest opisanie szczegółowych zabezpieczeń zapewniających ochronę danych w przypadku większości standardowych systemów nadzoru wideo służących typowym celom bezpieczeństwa. Tak więc w większości przypadków nie ma potrzeby przeprowadzania bardziej formalnej i dogłębnej oceny wpływu systemu nadzoru wideo na ochronę danych w instytucji, wprowadzania nowych zabezpieczeń lub przedkładania planów nadzoru do kontroli wstępnej EIOD. Należy po prostu przestrzegać wytycznych i realizować je.

Jednakże gdy proponowany nadzór znacznie zwiększa zagrożenie dla podstawowych praw i słusznych interesów podmiotów nim objętych (w porównaniu do standardowych systemów nadzoru wideo i zabezpieczeń opisanych w wytycznych), przed instalacją i wdrożeniem systemu należy przeprowadzić ocenę wpływu na prywatność i ochronę danych. Celem oceny wpływu jest określenie dodatkowych skutków proponowanego systemu dla prywatności osób fizycznych i innych praw podstawowych oraz ustalenie sposobów minimalizacji

lub uniknięcia negatywnych skutków. Systemy te podlegają kontroli wstępnej i będą w ścisły sposób kontrolowane przez EIOD.

Pod ścisłą kontrolą:
- *monitorowanie pracowników i monitorowanie poszczególnych biur;*
- *ukryty nadzór i wykorzystanie nadzoru wideo w dochodzeniach;*
- *monitorowanie demonstrantów;*
- *zaawansowany i inteligentny nadzór wideo (np. rozpoznawanie twarzy, nadzór o charakterze dynamicznym i prewencyjnym);*
- *systemy połączone;*
- *rejestracja dźwięku oraz telewizja przemysłowa z głośnikami.*

2.8. Eurodac

System Eurodac został utworzony na mocy rozporządzenia Rady (WE) nr 2725/2000 (tzw. rozporządzenie Eurodac), które jest obecnie przedmiotem analizy wraz z rozporządzeniem Dublin II. Eurodac jest obszerną bazą danych odcisków palców osób ubiegających się o azyl i nielegalnych imigrantów w Unii Europejskiej. Celem systemu jest ułatwienie skutecznego stosowania rozporządzenia Dublin II, które wskazuje państwa członkowskie odpowiedzialne za rozpatrzenie wniosków o udzielenie azylu składane przez osoby ubiegające się o międzynarodową ochronę w Unii Europejskiej na mocy konwencji genewskiej.

EIOD powierzono zadanie **nadzoru nad przetwarzaniem danych osobowych w centralnej bazie danych systemu wykorzystywanego przez Komisję** i ich przekazywaniem państwom członkowskim. W ramach tej roli EIOD ściśle współpracuje z organami ochrony danych w państwach członkowskich, które nadzorują przetwarzanie danych na szczeblu krajowym, jak też ich przesyłanie do jednostki centralnej. Przedstawiciele organów ochrony danych i EIOD spotykają się regularnie, by omówić typowe problemy związane z funkcjonowaniem systemu.

Ten **model skoordynowanego nadzoru** stanowi bardzo udany przykład skoordynowanego podejścia do nadzoru nad ochroną danych (zob. rozdz. 4.3).

Działania EIOD w odniesieniu do systemu Eurodac obejmują również konsultacje oraz zadania doradcze wykonywane w ramach przeglądu rozporządzeń Eurodac i Dublin, który jest obecnie omawiany przez instytucje UE. W lutym 2009 r. EIOD wydał dwie opinie w tej sprawie (zob. rozdz. 3.3.2).

3

KONSULTACJE

3.1. Wprowadzenie: przegląd i omówienie pewnych tendencji

W 2009 r. prowadzono ważne działania i zaszły znaczące wydarzenia, które przybliżyły **perspektywę nowych ram prawnych ochrony danych**. Osiągnięcie tego celu będzie dominującym tematem działań EIOD w nadchodzących latach.

Pod koniec 2008 r. na szczeblu UE po raz pierwszy przyjęto ogólne ramy ochrony danych w obszarze współpracy policyjnej i sądowej (decyzja ramowa Rady 2008/977/JHA). W 2009 r. doszło do drugiego ważnego wydarzenia w zakresie prawodawstwa.

Pierwsza modernizacja ram prawnych dotyczących ochrony danych – 25 listopada 2009 r. dyrektywę 2002/58/WE o prywatności i łączności elektronicznej zmieniono dyrektywą 2009/136/WE.

Są to jednak dopiero pierwsze kroki.

Wejście w życie traktatu lizbońskiego oznacza początek nowej ery w zakresie ochrony danych. Artykuł 16 TFUE nie tylko określa indywidualne prawa podmiotu danych, ale również zobowiązuje Parlament Europejski i Radę do zapewnienia ochrony danych we wszystkich obszarach prawa UE.

Innymi słowy, umożliwia on wprowadzenie kompleksowych ram prawnych ochrony danych mających zastosowanie do sektora prywatnego, sektora publicznego w państwach członkowskich oraz instytucji i organów UE.

W zatwierdzonym przez Radę Europejską w grudniu 2009 r. **programie sztokholmskim** – otwarta i bezpieczna Europa dla dobra i ochrony obywateli – zawarto oświadczenie, że Unia musi zagwarantować kompleksową strategię na rzecz ochrony danych w obrębie UE oraz w stosunkach z innymi państwami. W opinii EIOD w sprawie programu sztokholmskiego podkreślono potrzebę nowych ram prawnych, między innymi zastępujących decyzję ramową Rady 2008/977/JHA.

Najważniejszym krokiem w tym kontekście są jednak konsultacje społeczne w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych, organizowane przez DG ds. Sprawiedliwości, Wolności i Bezpieczeństwa.

Te konsultacje społeczne należy traktować jako pierwszy krok w kierunku nowoczesnego i kompleksowego instrumentu prawnego służącego ochronie danych, który w pełni odzwierciedla zmiany wprowadzone przez traktat lizboński, a także zapewni skuteczną ochronę danych osobowych w społeczeństwie informacyjnym.

Wynik wspólnych prac grupy roboczej art. 29 oraz Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości na temat „przyszłość prywatności" został przyjęty

w grudniu 2009 r. przy pełnym poparciu i znaczącym wkładzie EIOD. Dokument ten należy wnikliwie rozważyć, gdyż zawiera on ważne porady europejskich specjalistów ds. ochrony danych dotyczące rozwoju nowoczesnych i kompleksowych ram prawnych, o których mowa powyżej.

W kontekście globalnym warto zauważyć, że podczas 31. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w Madrycie w listopadzie 2009 r. przyjęto uchwałę w sprawie ogólnoświatowych norm dotyczących ochrony danych. Jeżeli chodzi o transatlantycką ochronę danych, podjęto dalsze kroki na rzecz zawarcia porozumienia między UE a USA w sprawie wymiany danych osobowych do celów organów ścigania.

Rok 2009 można również wskazać jako okres, w którym EIOD zaangażował się w dwóch dodatkowych obszarach polityki UE, w których przetwarzanie danych osobowych jest sprawą najwyższej wagi: chodzi tu o wykazy terrorystów i opodatkowanie.

Polityka dotycząca tzw. wykazów terrorystów jest częścią wspólnej polityki zagranicznej i bezpieczeństwa UE, a opodatkowanie jest obszarem, który ze swej natury wiąże się z intensywnym przetwarzaniem danych osobowych oraz współpracą administracyjną, w szczególności w celu zwalczania nadużyć. Położono też większy nacisk na dwie inne dziedziny, mianowicie zdrowie publiczne i transport. Wreszcie EIOD brał oczywiście nadal aktywny udział w różnych działaniach DG ds. Społeczeństwa Informacyjnego oraz DG ds. Sprawiedliwości, Wolności i Bezpieczeństwa.

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 interwencji nie uległo zmianie. Dokument 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 prawodawczych i pokrewnych dokumentów) pozostaje aktualny, chociaż należy go teraz interpretować w świetle traktatu lizbońskiego.

Formalne 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.

Od czasu do czasu zgłaszane 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.

Z EIOD można się konsultować we wszystkich fazach opracowywania polityki i prawodawstwa; wykorzystuje on także różnorodne inne instrumenty wywierania wpływu. Chociaż może to wymagać ścisłej współpracy z instytucjami UE, najważniejszą kwestią jest ochrona jego niezależności i poszanowanie stanowiska wszystkich innych instytucji biorących udział w tym procesie.

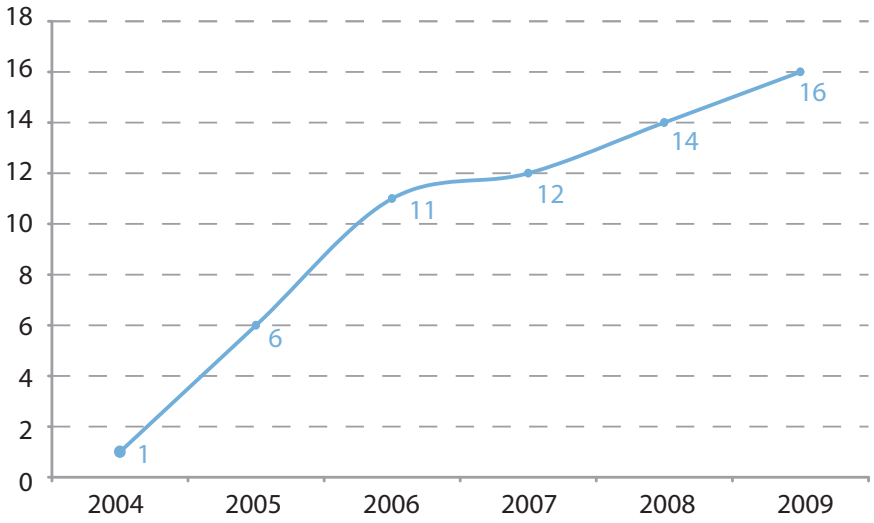
Kontakty z Komisją mają miejsce na różnych etapach opracowywania wniosków, a ich intensywność jest zależna od tematu, a także podejścia służb Komisji. Na przykład w przypadku długoterminowych projektów, takich jak e-sprawiedliwość lub dyskusje na temat zasad zgłaszania przypadków naruszenia bezpieczeństwa, EIOD wnosił wkład w różny sposób na różnych etapach.

Kontakty miały też miejsce w fazie monitorowania dalszych działań, zwłaszcza podczas intensywnych dyskusji i negocjacji w Parlamencie lub Radzie prowadzących do zasadniczych zmian we wniosku Komisji. Przykładami intensywnego zaangażowania EIOD na wielu etapach w 2009 r. były przegląd dyrektywy o prywatności i łączności elektronicznej oraz zmiana rozporządzenia o publicznym dostępie.

Jak stwierdzono powyżej, w 2009 r. perspektywa nowych ram ochrony danych stała się konkretniejsza, a temat ten omawiano na różnych szczeblach i w obrębie różnych sieci. EIOD prezentował swoje stanowisko na wiele sposobów. Ważnymi elementami tych działań była opinia w sprawie programu sztokholmskiego i sprawozdanie grupy roboczej art. 29, ale należy też zwrócić uwagę na inne opinie, np. w sprawie dostępu organów ścigania do systemu Eurodac, jak też wystąpienia, udział w konferencjach

([8]) Dostępny na stronach internetowych EIOD w sekcji „Consultation".

Opinie dotyczące prawodawstwa – ewolucja 2004–2009



i dyskusjach w Parlamencie Europejskim. Jedną z głównych kwestii – potrzebę stworzenia kompleksowych ram, w tym również służących współpracy policyjnej i sądowej – wskazała także jako jeden ze swoich głównych celów komisarz Viviane Reding.

3.2.2. Wyniki w 2009 r.

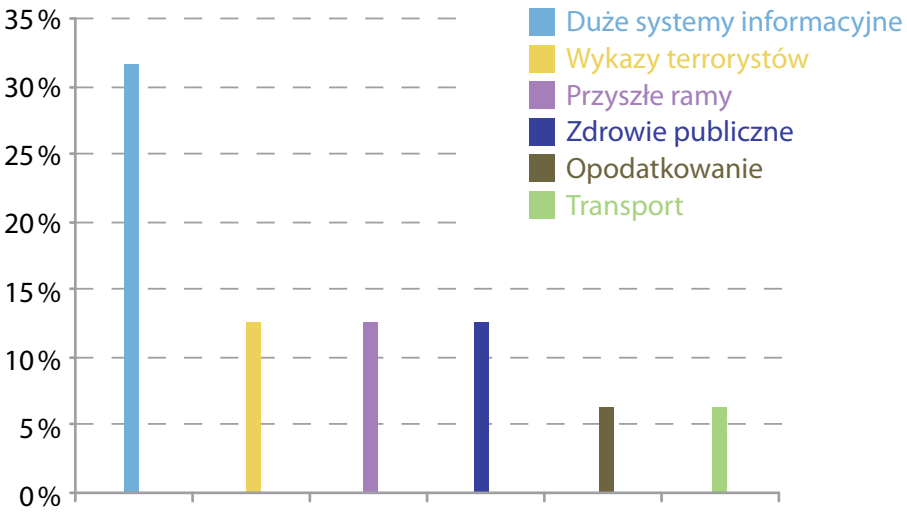
W 2009 r. utrzymywał się systematyczny wzrost liczby opinii konsultacyjnych. EIOD wydał 16 opinii dotyczących różnorodnych tematów.

Opinie te i inne instrumenty interwencyjne stanowiły realizację priorytetów EIOD na 2009 r. zgodnie ze spisem opublikowanym w grudniu 2008 r. Wydanych 16 opinii dotyczyło różnych obszarów polityki UE.

Spis na 2009 r. określał trzy główne obszary zainteresowania: zdrowie publiczne, wolność, bezpieczeństwo i sprawiedliwość oraz społeczeństwo informacyjne. Zdrowie publiczne jest z punktu widzenia EIOD obszarem stosunkowo nowym; ogólne stanowisko sformułowano w opiniach dotyczących dawstwa narządów i nadzoru nad bezpieczeństwem farmakoterapii. W dziedzinie wolności, bezpieczeństwa i sprawiedliwości wiele uwagi poświęcono sytuacji w odniesieniu do zarządzania granicami i do wielkoskalowych systemów informatycznych. Rozwój społeczeństwa informacyjnego był i pozostanie ważnym priorytetem.

Z perspektywy czasu, chociaż EIOD skupił się na głównych priorytetach wymienionych w spisie na 2009 r., konkretne osiągnięcia w tym roku nie pokrywały się w pełni z zamiarami określonymi w tym spisie. Dowodzi to dynamiki zmian w tej dziedzinie. Kwestie, które zostały wskazane na początku roku, nie zawsze okazywały się najbardziej istotne w późniejszych miesiącach. EIOD nie dokonał jednak fundamentalnego zwrotu. Niektóre plany ogłoszone na

Najważniejsze obszary opinii dotyczących prawodawstwa w 2009 r.



początku 2009 r. przyniosą efekty w 2010 r. Przykładem jest tu przedstawiona na początku 2010 r. opinia dotycząca umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA).

3.3. Przestrzeń wolności, bezpieczeństwa i sprawiedliwości

3.3.1. Sytuacja ogólna

W 2009 r. EIOD śledził ze szczególnym zainteresowaniem wydarzenia związane z **programem sztokholmskim**, który zawiera unijną wizję następnego pięciolecia w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych. Program sztokholmski należy uznać za kolejny krok w kierunku budowania przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej.

Współpraca między organami ścigania oraz ogólniej między państwami członkowskimi oraz między państwami członkowskimi a UE w tej dziedzinie wiąże się z gromadzeniem i wymianą danych osobowych na wielką skalę. Ochrona danych osobowych obywateli w ramach współpracy policyjnej i sądowej jest zatem niezwykle istotna, jak EIOD podkreślił w ponad 30 opiniach i komentarzach w tej sprawie. EIOD konsekwentnie podkreślał, że zapewnienie ochrony danych osobowych jest nie tylko sposobem ochrony obywateli, ale również sprzyja efektywnemu egzekwowaniu prawa i wzajemnemu zaufaniu między organami ścigania poszczególnych państw członkowskich.

EIOD wydał opinię w sprawie komunikatu Komisji z dnia 10 czerwca 2009 r., a następnie wniósł aktywny wkład – przez wykonane prace i wystąpienia skierowane do zainteresowanych instytucji – w dyskusje prowadzące do przyjęcia programu na grudniowym posiedzeniu Rady Europejskiej.

EIOD z zadowoleniem przyjął zaakcentowanie w programie ochrony praw podstawowych, a w szczególności ochrony danych osobowych. Podobnie EIOD z zadowoleniem przyjmuje wezwanie do opracowania kompleksowego systemu ochrony danych, który znajduje teraz solidną podstawę prawną w traktacie lizbońskim.

Kompleksowe ramy przyczyniłyby się również do sprawniejszej reakcji na najważniejsze obserwowane ostatnio tendencje oraz do uregulowania tych tendencji:

- *wykładniczy **wzrost ilości informacji cyfrowych** wskutek ewolucji technologii informacyjnych i komunikacyjnych;*
- ***umiędzynarodowienie** wymiany danych osobowych;*
- ***wykorzystanie danych komercyjnych** przez organy ścigania – np. danych zgromadzonych przez przedsiębiorstwa prywatne, takie jak operatorzy telekomunikacyjni, banki, linie lotnicze.*

Zgodnie z programem sztokholmskim UE musi stworzyć kompleksową strategię na rzecz ochrony danych w obrębie UE oraz w relacjach z innymi państwami.

EIOD podkreślił, że przed wprowadzeniem nowych narzędzi służących takiej wymianie instytucje UE powinny zastanowić się nad konsekwencjami z punktu widzenia organów ścigania i obywateli Europy. Ponadto EIOD położył nacisk na znaczenie rozwijania i promowania międzynarodowych standardów w zakresie ochrony danych, jak również zapewnienia, aby dane osobowe były przekazywane do państw trzecich i organizacji tylko wtedy, gdy zapewniona jest ich wystarczająca ochrona.

Program sztokholmski kładzie nacisk na rozwój **europejskiego modelu informacji**, który stanowi godny uznania ruch w kierunku racjonalizacji i opracowania długoterminowej wizji zarządzania danymi osobowymi oraz ich wymiany w dziedzinach wymiaru sprawiedliwości, bezpieczeństwa, azylu i imigracji.

EIOD podkreślił, że ta długoterminowa wizja może być przydatna w uczynieniu wymiany informacji skuteczniejszą przy jednoczesnym zapewnieniu wysokiego poziomu ochrony danych osobowych. Wprowadzenie ochrony prywatności już na początkowym etapie opracowywania architektury systemów informatycznych – „wbudowana ochrona prywatności" (*privacy by design*) lub „domyślna ochrona prywatności" (*privacy by default*) – to ważny krok w realizacji tej długofalowej wizji, ponieważ pomoże to poprawić jakość informacji oraz zapobiec jej nadmiarowi.

EIOD omówił także temat **współdziałania** różnych systemów i baz danych, które nie powinno być zdeterminowane technologią, ale oparte na jasnych i przemyślanych wyborach politycznych. Powinno ono odbywać się przy poszanowaniu oraz zapewnieniu warunków prawnych gromadzenia, wymiany i wykorzystywania danych osobowych.

Obywatele muszą być w stanie określić, jakie dane o nich są gromadzone i do jakich celów są wykorzystywane. Jest to istotne zwłaszcza w przypadku szczególnych kategorii danych, takich jak odciski palców i DNA ([9]).

Nowe technologie będą także wykorzystywane jako narzędzie **usprawnienia współpracy sądowej** w ramach projektu tzw. **e-sprawiedliwości** i innych inicjatyw zmierzających do stworzenia prawdziwej europejskiej przestrzeni sądowej. Elementami tych inicjatyw są połączenia między krajowymi rejestrami, np. rejestrami niewypłacalności, wykorzystanie wideokonferencji w postępowaniach sądowych, a także użycie portali internetowych w celu poprawy dostępu obywateli do wymiaru sprawiedliwości; EIOD przyjmuje je z zadowoleniem, zastrzegając, że przy ich realizacji należy uwzględnić zasady ochrony danych. Część spośród tych narzędzi może również być używana do zapewnienia skuteczniejszej ochrony i łatwiejszego egzekwowania praw dotyczących ochrony danych w całej Europie.

([9]) Wynika to też z warunków sformułowanych przez Europejski Trybunał Praw Człowieka w sprawie S. i Marper, 4 grudnia 2008 r., wnioski nr 30562/04 i 30566/04.

3.3.2. System Eurodac i rozporządzenie dublińskie

Szczególną uwagę należy zwrócić na kwestie prywatności i ochrony danych w systemie dublińskim oraz w systemie Eurodac, który służy do przechowywania i wymiany na dużą skalę cyfrowych odcisków palców osób ubiegających się o azyl oraz innych grup (potencjalnych) imigrantów, co pozwala na określenie państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o azyl. Osoby, które obejmuje swoim zakresem ten system, należą do **jednej z najsłabszych grup społecznych** i napotykają na wielkie trudności, jeżeli chodzi o obronę swoich praw.

Ochrona danych jest również **fundamentalnym czynnikiem sukcesu** systemu Eurodac, a tym samym prawidłowego funkcjonowania systemu dublińskiego. Elementy takie, jak bezpieczeństwo danych, techniczna jakość danych i zgodność konsultacji z prawem, przyczyniają się do sprawnego funkcjonowania systemu Eurodac.

EIOD przyjął dwie powiązane opinie dotyczące wniosku w sprawie zmiany tzw. rozporządzenia Eurodac oraz wniosku w sprawie przekształcenia rozporządzenia dublińskiego, które określa państwo członkowskie UE odpowiedzialne za dany wniosek o azyl.

Wnioski te mają na celu zapewnienie lepszej harmonizacji, wzrostu efektywności i poprawy standardów ochrony w ramach wspólnego europejskiego systemu azylowego. Są one również szczególnie istotne z punktu widzenia EIOD ze względu na jego obecną rolę jako organu nadzorującego system Eurodac.

W swoich opiniach EIOD poparł cele nowelizacji oraz z zadowoleniem przyjął znaczny nacisk położony w obydwu wnioskach na poszanowanie podstawowych praw obywateli państw trzecich i bezpaństwowców. EIOD przedstawił szereg uwag odnoszących się między innymi do przestrzegania praw podmiotów danych, nadzoru nad systemem i mechanizmów wymiany informacji.

Komisja zaproponowała również udostępnienie systemu Eurodac – który ma na celu ułatwienie stosowania rozporządzenia dublińskiego przez porównywanie odcisków palców osób ubiegających się o azyl i nielegalnych imigrantów – organom ścigania do celów zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz wykrywania tych przestępstw i dochodzeń, na warunkach określonych we wnioskach.

EIOD przeanalizował te wnioski z punktu widzenia ich proporcjonalności i zasadności, biorąc za punkt wyjścia konieczność znalezienia właściwej równowagi między potrzebą zapewnienia bezpieczeństwa publicznego i podstawowym prawem do prywatności i ochrony danych zgodnie z art. 8 Europejskiej Konwencji Praw Człowieka (EKPC).

Analiza doprowadziła do wniosku, że nie wykazano konieczności i proporcjonalności wniosków, co stanowi niezbędny element uzasadnienia naruszenia prywatności.

EIOD zalecił ocenę zasadności wniosków w szerszym kontekście, a zwłaszcza:

- tendencji do przyznawania organom ścigania dostępu do danych osobowych osób fizycznych, które nie są podejrzewane o żadne przestępstwo, a dane te zostały zgromadzone w innych celach;
- potrzeby indywidualnej oceny każdego wniosku tego rodzaju;
- potrzeby spójnej, kompleksowej i zorientowanej na przyszłość wizji, o ile to możliwe – związanej z następnym pięcioletnim programem ramowym w dziedzinie sprawiedliwości i spraw wewnętrznych (programem sztokholmskim).

3.3.3. Agencja ds. zarządzania operacyjnego wielkoskalowymi systemami informatycznymi

Komisja zaproponowała pakiet prawodawczy ustanawiający agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

Agencja ta byłaby odpowiedzialna za zarządzanie operacyjne systemem informacyjnym Schengen (SIS II), wizowym systemem informacyjnym (VIS), systemem Eurodac i ewentualnie innymi wielkoskalowymi systemami informatycznymi.

Ponieważ te bazy danych zawierają **znaczne ilości danych osobowych** (np. dane dotyczące paszportów, wiz i odciski palców), a niektóre z nich mają wrażliwy charakter, EIOD przeanalizował wniosek w celu zapewnienia, aby jego **skutki z punktu widzenia prywatności osób fizycznych** zostały w wystarczającym stopniu uwzględnione w akcie prawnym.

EIOD dostrzega korzyści z utworzenia agencji ds. zarządzania operacyjnego niektórymi wielkoskalowymi systemami informatycznymi, ale agencja taka powinna być ustanowiona tylko w przypadku wyraźnego określenia zakresu jej działań i obowiązków.

Utworzenie agencji ds. zarządzania operacyjnego wielkoskalowymi bazami danych musi być oparte na prawodawstwie, które jednoznacznie wskazuje kompetencje i zakres działalności tej agencji. Wyraźne ich określenie zapobiegnie w przyszłości nieporozumieniom co do działania agencji oraz ryzyku rozrastania się jej funkcji. W obecnym kształcie wnioski nie spełniają tych wymagań.

3.3.4. System Informacji Celnej (CIS)

Spójne i kompleksowe podejście do wielkoskalowych systemów informatycznych UE, jak również **efektywny nadzór nad ochroną danych** to warunki konieczne do pomyślnego funkcjonowania tych systemów. Nowe ramy prawne udostępnione przez traktat lizboński oraz likwidacja filarowej struktury prawa UE powinny także posłużyć zapewnieniu większej **spójności** między systemami działającymi uprzednio na bazie prawnej pierwszego i trzeciego filaru. Potrzebna jest również ściślejsza współpraca między organami ochrony danych uczestniczącymi w nadzorowaniu systemów.

W tym kontekście EIOD wydał opinię na temat inicjatywy Republiki Francuskiej na rzecz przyjęcia decyzji Rady w sprawie stosowania technologii informatycznych do potrzeb celnych. W swojej opinii EIOD podkreślił potrzebę zapewnienia jak największej spójności między obydwiema częściami CIS, tj. częścią objętą dawnym pierwszym filarem oraz częścią objętą dawnym trzecim filarem. EIOD wezwał również do poświęcenia w ramach wniosku większej uwagi **konkretnym zabezpieczeniom służącym ochronie danych**, w szczególności w odniesieniu do ograniczenia celu wykorzystania danych wprowadzonych do CIS.

EIOD opowiedział się też za uwzględnieniem we wniosku **skoordynowanego modelu nadzoru**, który zapewni w razie potrzeby spójność z innymi aktami prawnymi regulującymi ustanowienie lub wykorzystanie innych wielkoskalowych systemów informatycznych, gdyż użycie tego modelu jest przewidywane także w przypadku SIS II i VIS.

Zastosowany model nadzoru był ważnym wątkiem dyskusji w Radzie i Parlamencie Europejskim. EIOD poświęcił wiele czasu i energii, argumentując za skoordynowanym modelem. Niestety projekt przyjęty przez Radę nie w pełni odpowiada temu modelowi, daje jednak nowy bodziec do ścisłej i skutecznej współpracy pomiędzy EIOD a krajowymi organami ochrony danych.

3.4. Prywatność w kontekście łączności i technologia

3.4.1. EIOD a dyrektywa o prywatności i łączności elektronicznej

W 2009 r. dyrektywa 2002/58/WE o prywatności i łączności elektronicznej, znana także jako **dyrektywa o e-prywatności**, przeszła ostatni etap procesu przeglądu. Dyrektywa została ostatecznie przyjęta 25 listopada 2009 r. ([10]). Jej nowe przepisy poprawiają ochronę prywatności i danych osobowych wszystkich Europejczyków aktywnych w środowisku internetowym. Wśród szczególnie istotnych udoskonaleń należy wymienić:

- obowiązkowe zgłaszanie naruszeń danych osobowych. Każdy dostawca usług łączności elektronicznej, jak np. dostawca usług internetowych, musi informować osoby fizyczne o wszelkich naruszeniach danych osobowych, które mogą mieć dla nich niekorzystne skutki. Dotyczy to m.in. przypadków, gdy utrata danych osobowych może doprowadzić do kradzieży tożsamości, nadużyć, upokorzenia lub naruszenia dobrego imienia;
- nowe regulacje dotyczące tzw. *cookies* i oprogramowania szpiegowskiego. Zgodnie z nowymi przepisami użytkownikom należy oferować dokładniejsze informacje i łatwiejsze sposoby akceptowania lub odrzucania plików *cookie* przechowywanych w ich urządzeniach końcowych;
- poszerzenie prawa do wszczęcia postępowania sądowego przeciwko spamerom. Osiągnięto to, dając każdej osobie odczuwającej niekorzystne efekty spamu, w tym dostawcom usług internetowych, możliwość wszczęcia skutecznego postępowania sądowego przeciwko spamerom;
- przepisy zwiększające możliwości egzekwowania prawa przez organy ochrony danych.

Na wszystkich etapach procesu legislacyjnego aż do ostatecznego przyjęcia aktu EIOD doradzał decydentom, oferując pomoc w określeniu właściwych rozwiązań. EIOD z dużym zadowoleniem przyjął ostateczną postać przepisów dotyczących obowiązkowego powiadamiania o naruszeniu bezpieczeństwa.

W swojej drugiej opinii prawnej EIOD zawarł m.in. porady na temat najważniejszych cech ram prawnych dotyczących powiadomień o przypadkach naruszenia bezpieczeństwa ([11]).

EIOD z zadowoleniem przyjął szeroką definicję naruszenia bezpieczeństwa, która obejmuje wszelkie naruszenia prowadzące do zniszczenia, utraty, ujawnienia itp. danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób w związku z usługą. Jeżeli chodzi o zdarzenia inicjujące powiadomienie, EIOD sugerował, że powiadomienie w przypadku osób fizycznych powinno być wymagane, jeżeli naruszenie bezpieczeństwa danych *mogłoby mieć niekorzystny wpływ na ich dane osobowe lub prywatność*. Wyjaśnił on powody, dla których zasada ta jest lepszym rozwiązaniem od innych proponowanych; ku jego

([10]) Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz.U. L 337/11 z 18.12.2009.

([11]) Druga opinia z dnia 9 stycznia 2009 r. w sprawie przeglądu dyrektywy 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej), Dz.U. C 128 z 6.6.2009, s. 28.

Komunikacja elektroniczna zawsze zostawia ślady.

zadowoleniu argumentacja ta została przyjęta. Z satysfakcją przyjął też decyzję, by stosowne podmioty były odpowiedzialne za ocenę, czy naruszenie spełnia wspomniane warunki, a więc czy powinno inicjować powiadomienie, czy też nie.

Niestety prawodawca nie postąpił zgodnie z zaleceniem EIOD, aby przepis ten miał zastosowanie do wszystkich administratorów danych, decydując się ograniczyć go do usług łączności elektronicznej świadczonych przez firmy telekomunikacyjne, dostawców usług internetowych, dostawców usług poczty elektronicznej za pośrednictwem stron internetowych itp.

To ograniczenie zakresu wywołało ożywioną dyskusję pomiędzy Parlamentem Europejskim – opowiadającym się za znacznie szerszym zakresem – a Radą i Komisją, które poparły zakres bardziej ograniczony. Choć ostateczny wynik jest niezadowalający, debata skłoniła Komisję do wyrażenia zamiaru obowiązkowego objęcia tym systemem wszystkich administratorów danych w najbliższej przyszłości.

Zmieniona dyrektywa o prywatności i łączności elektronicznej upoważnia Komisję do przyjmowania w porozumieniu z zainteresowanymi stronami oraz z EIOD technicznych środków wykonawczych, tj. szczegółowych środków dotyczących powiadamiania o naruszeniu bezpieczeństwa, w drodze procedury komitetowej. Zapewni to spójne wdrażanie i stosowanie przepisów prawnych dotyczących naruszenia bezpieczeństwa w całej UE, tak aby obywatele korzystali z równie wysokiego poziomu ochrony, a dostawcy usług nie byli obciążani różniącymi się wymogami dotyczącymi powiadamiania.

EIOD zorganizował dwa spotkania w celu wymiany doświadczeń i najlepszych praktyk. Inicjatywa ta powinna być przydatna w związku z przyszłą procedurą komitetową. Pierwsze spotkanie odbyło się w kwietniu 2009 r. i zostało zorganizowane wyłącznie dla organów ochrony danych w ramach inicjatywy londyńskiej. Drugie, skierowane do wszystkich zainteresowanych stron, odbyło się w październiku 2009 r. i zostało zorganizowane wspólnie z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA).

Dyrektywa o prywatności i łączności elektronicznej została przyjęta wraz z innymi dyrektywami, określanymi łącznie jako **pakiet telekomunikacyjny**.

Przepisy dotyczące systemów stopniowanej reakcji (odcinanie od Internetu za trzy wykroczenia) zawarte w dyrektywie 2002/22/WE w sprawie usługi powszechnej i praw użytkowników rodzą obawy dotyczące ochrony danych i prywatności. EIOD poruszył tę kwestię w swoich uwagach z 16 lutego 2009 r., potwierdzając swój sprzeciw wobec systematycznej, aktywnej inwigilacji przestrzegających prawa użytkowników Internetu w celu zwalczania domniemanych naruszeń praw autorskich.

3.4.2. Inteligentne systemy transportowe

EIOD zwrócił szczególną uwagę na innowacje technologiczne w dziedzinie transportu. W celu zmniejszenia zatorów w ruchu drogowym oraz sprawienia, by transport był bezpieczniejszy i bardziej ekologiczny w Europie wdrażane są obecnie tzw. inteligentne systemy transportowe (ITS). Systemy te opierają się zwykle na technologiach lokalizacyjnych, takich jak systemy lokalizacji

Nowoczesna technika umożliwia stałe monitorowanie ruchów pojazdów.

satelitarnej i RFID. Wdrożenie ITS w Europie ma znaczące konsekwencje z punktu widzenia prywatności, zwłaszcza że pozwalają one na śledzenie pojazdu oraz gromadzenie różnorodnych danych związanych z nawykami europejskich użytkowników dróg.

Inteligentne systemy transportowe wykorzystują technologie informacyjne i komunikacyjne (satelitarne, komputerowe, telekomunikacyjne itp.) w odniesieniu do infrastruktury transportowej oraz pojazdów. Przykładem inteligentnego systemu transportowego jest system powiadamiania o wypadkach „e-Call" czy elektroniczny system pobierania opłat za przejazd „e-Toll".

Wypowiadając się na temat planu działania Komisji mającego na celu przyspieszenie i koordynację wdrożenia ITS w Europie, EIOD podkreślił, że należy wnikliwie zająć się kwestiami ochrony prywatności i ochrony danych w celu zapewnienia możliwości funkcjonowania ITS na całym kontynencie.

Ostrzegł też Komisję przed ryzykiem niespójności i fragmentacji wdrożenia, jeśli pewne kwestie nie zostaną ściślej zharmonizowane na szczeblu UE:

- istnieje potrzeba jasnego określenia, czy i które usługi ITS będą świadczone na zasadzie dobrowolnej lub obowiązkowej;
- trzeba określić role poszczególnych stron zaangażowanych w ITS w celu ustalenia, kto jest odpowiedzialny za zapewnienie, aby systemy działały poprawnie z punktu widzenia ochrony danych – tzn. kto jest administratorem danych;
- administratorzy danych świadczący usługi ITS powinni wdrożyć właściwe zabezpieczenia, aby wykorzystanie technologii lokalizacyjnych nie naruszało prywatności. Wykorzystanie urządzeń lokalizacyjnych powinno być ściśle ograniczone do zakresu niezbędnego z punktu widzenia ich celów. Należy zapewnić, aby dane dotyczące lokalizacji nie były udostępniane nieupoważnionym odbiorcom;
- prywatność i ochrona danych powinny zostać uwzględnione na wczesnym etapie projektowania architektury ITS, eksploatacji oraz zarządzania systemami (wbudowana ochrona prywatności);
- administratorzy danych muszą zagwarantować, aby użytkownicy byli odpowiednio informowani o celach i sposobach przetwarzania danych.

3.4.3. Stosowanie dyrektywy w sprawie zatrzymywania danych

Dyrektywa 2006/24/WE w sprawie zatrzymywania danych stanowi narzędzie walki z terroryzmem i innymi poważnymi przestępstwami, zobowiązując dostawców usług i sieci łączności do zatrzymywania danych o ruchu w komunikacji elektronicznej. Została ona przyjęta kilka lat temu pod wielką presją polityczną i rodzi wiele pytań, które utrudniają jej stosowanie.

W związku z tym powołano grupę ekspertów gromadzącą przedstawicieli organów ścigania, branży oraz podmiotów danych, której głównym zadaniem było sformułowanie wytycznych, np. w kwestii tego, do których dostawców dyrektywa ma zastosowanie ze względu na złożoność środowiska usług pocztowych świadczonych za pośrednictwem stron internetowych, dostawców usług tranzytowych, sieci operatorów zewnętrznych itp. EIOD aktywnie uczestniczył w pracach grupy, domagając się, by wszelkie wytyczne były zgodne z zasadami prawa o ochronie danych.

W tym kontekście pojawiło się ciekawe i trudne pytanie: Jakie prawo ma zastosowanie w przypadku łączności, która dotyczy więcej niż jednego państwa członkowskiego, na przykład w przypadku międzynarodowej łączności komórkowej lub transgranicznej łączności internetowej. Problem ten staje się jeszcze bardziej złożony, gdy dostawca przechowuje zatrzymane dane w państwie członkowskim innym niż to, w którym zostały one wytworzone. Grupa zamierza opublikować swoje wnioski w ciągu 2010 r.

3.4.4. RFID

W maju 2009 r. Komisja Europejska przyjęła zalecenie w sprawie wprowadzenia w życie zasad ochrony prywatności i danych w zastosowaniach wykorzystujących identyfikację radiową ([12]). Komisja konsultowała się często z EIOD w trakcie opracowywania zalecenia i większość jego uwag została uwzględniona.

Następnie Komisja Europejska powołała nieformalną grupę roboczą ds. wdrożenia zalecenia RFID; przedstawiciel grupy roboczej art. 29 uczestniczył w dwóch posiedzeniach nieformalnej grupy w 2009 r. Zajmowała się ona m.in. potrzebą wprowadzenia ocen wpływu na prywatność i ochronę danych. Zgodnie z pkt 4 zalecenia ramy takiej oceny zostaną przedłożone do zatwierdzenia grupie roboczej art. 29.

([12]) Zalecenie Komisji C(2009) 3200 wersja ostateczna z 12 maja 2009 r., dostępne pod adresem: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf.

3.4.5. Udział w PR7

RISEPTIS

EIOD dołączył jako obserwator do Rady Doradczej RISEPTIS (badania i innowacje na rzecz bezpieczeństwa, prywatności i wiarygodności w społeczeństwie informacyjnym) ([13]). Ta powołana przez Komisję Europejską grupa doradcza wysokiego szczebla składa się z czołowych podmiotów z kręgów nauki, przemysłu i polityki; jej celem jest stworzenie wizjonerskich wytycznych w sprawie wyzwań politycznych i badawczych w dziedzinie bezpieczeństwa i zaufania w społeczeństwie informacyjnym. EIOD brał czynny udział w posiedzeniach RISEPTIS w 2009 r., udzielając specjalistycznych porad dotyczących zagadnień politycznych, w szczególności w dziedzinie prawa właściwego z punktu widzenia przyszłych i powstających technologii, zasad rozliczalności i odpowiedzialności, jak również koncepcji wbudowanej ochrony prywatności.

Wydany w październiku 2009 r. raport RISEPTIS zatytułowany „Zaufanie w społeczeństwie informacyjnym" zawiera zalecenia odnoszące się do wielu kwestii związanych z wejściem UE w erę cyfrową.

Obejmują one:

- interdyscyplinarne badania, rozwój i wdrażanie technologii;
- inicjatywy mające na celu zaangażowanie zainteresowanych stron z kręgów technicznych, politycznych, prawnych i społeczno-ekonomicznych w działanie na rzecz godnego zaufania społeczeństwa informacyjnego;
- wspólne unijne ramy zarządzania tożsamością i uwierzytelnieniem;
- dalszy rozwój wspólnotowych ram prawnych dotyczących ochrony danych i prywatności;
- działania na dużą skalę z udziałem sektora prywatnego i publicznego, które wykorzystują

([13]) http://www.think-trust.eu/riseptis.html

atuty Europy w dziedzinie komunikacji, badań, studiów prawnych i wartości społecznych;

- współpracę w skali globalnej w celu promowania otwartych standardów i struktur federalnych.

Projekty UE w zakresie badań i rozwoju technologicznego

Po opublikowaniu dokumentu z maja 2008 r. EIOD udzielał również ukierunkowanego wsparcia szeregowi projektów UE w zakresie badań i rozwoju technologicznego w różnych dziedzinach, w tym inteligentnych systemów transportowych, systemów biometrycznych, systemów zdalnego monitoringu oraz e-zdrowia, jak też dostarczał informacji zwrotnych związanych z tymi projektami.

3.5. Globalizacja

3.5.1. Udział w tworzeniu globalnych norm

Wiele zainteresowanych stron, w tym przedstawiciele społeczeństwa obywatelskiego i przemysłu, opowiada się za harmonizacją ram ochrony danych w różnych państwach w celu zagwarantowania pewności prawa i ułatwienia przepływu danych w kontekście międzynarodowym. Podczas Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w Madrycie w listopadzie 2009 r. podjęto konkretne kroki zmierzające do opracowania międzynarodowych norm ochrony danych. Uczestnicy konferencji przyjęli rezolucję wyrażającą zadowolenie z przyjęcia projektu międzynarodowych norm ochrony danych osobowych i prywatności. Normy te stanowią pierwszy krok na drodze do wiążącego dokumentu międzynarodowego. Są one wynikiem intensywnych prac przygotowawczych pod przewodnictwem hiszpańskiego organu ochrony danych, w których aktywną rolę odegrał też EIOD.

Normy zawierają podstawowe zasady ochrony danych; chociaż zasady te są w dużej mierze inspirowane przez europejską dyrektywę o ochronie danych, uwzględniają również inne podejścia do ochrony danych ([14]).

([14]) Np. podejścia krajów OECD i APEC, które różnią się nieco od unijnego.

Oprócz konieczności przestrzegania zasad sprawiedliwości, konieczności, proporcjonalności i przejrzystości wskazują one obowiązki administratorów danych w dziedzinie rozliczalności, jak również podkreślają potrzebę wbudowanej ochrony prywatności. Projektowane normy dają też podmiotom danych prawo dostępu i poprawy danych, a także sądowe i administracyjne środki prawne.

3.5.2. Dane PNR i dialog transatlantycki

Kwestie ochrony danych są jednym z priorytetów rozmów między UE i USA.

Kolejnym aspektem globalizacji jest dialog transatlantycki między Unią Europejską a Stanami Zjednoczonymi w celu ułatwienia wymiany danych osobowych. Przekazywanie danych odbywa się głównie w celu zwalczania terroryzmu i poważnych przestępstw, jak wynika z porozumienia w sprawie przekazywania danych dotyczących przelotu pasażera do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (decyzja Rady z dnia 23 lipca 2007 r.). Zarówno grupa robocza art. 29, jak i EIOD wyrazili obawy co do warunków dotyczących gromadzenia, przetwarzania i przechowywania danych pasażerów ([15]). W 2009 r. podgrupa grupy roboczej art. 29, w pracach której uczestniczy EIOD, monitorowała wykonanie wspomnianej umowy PNR i podniosła wiele kwestii, w szczególności szeroki dostęp przyznany administracji amerykańskiej do danych przetwarzanych przez komputerowe systemy rezerwacyjne oraz brak przeglądu systemu ze strony władz europejskich.

W ogólniejszym kontekście UE i USA prowadzą negocjacje na temat zawarcia porozumienia

([15]) Zob. sprawozdanie roczne EIOD za rok 2008.

Dostęp władz publicznych do danych o transakcjach bankowych podlega ścisłym warunkom.

w sprawie wymiany informacji w szeroko rozumianej dziedzinie egzekwowania prawa. Negocjacje te poskutkowały sporządzeniem kilku sprawozdań tzw. grupy kontaktowej wysokiego szczebla, na temat których EIOD wydał opinię ([16]). W 2009 r. dyskusje koncentrowały się na konkretnych kwestiach, co do których nie osiągnięto pełnej zgody między stronami – w szczególności na administracyjnych i sądowych środkach prawnych przysługujących jednostkom. Strony mają zamiar podjąć dalsze kroki w kierunku osiągnięcia porozumienia w 2010 r. EIOD wniósł wkład w organizowane przez Komisję konsultacje społeczne w sprawie porozumienia.

3.5.3. SWIFT: przekazywanie danych finansowych władzom USA

EIOD uważnie śledził wydarzenia związane z kwestią przekazywania europejskich danych o transakcjach finansowych Departamentowi Skarbu USA w celu zwalczania terroryzmu i jego finansowania. Jest to oczywisty przykład danych osobowych gromadzonych przez firmy komercyjne, które są wykorzystywane do celów egzekwowania prawa w skali ogólnoświatowej.

([16]) Opinia z dnia 11 listopada 2008 r. w sprawie sprawozdania końcowego grupy kontaktowej wysokiego szczebla UE–USA ds. wymiany informacji oraz ochrony prywatności i danych osobowych, Dz.U. C 128 z 6.6.2009, s. 1.

Kiedy wielka sieć przesyłu danych finansowych SWIFT zmieniła swą strukturę w celu przechowywania europejskich danych finansowych na terytorium Europy, Komisja Europejska rozpoczęła negocjacje z władzami USA, aby zawrzeć umowę międzynarodową umożliwiającą im dalszy dostęp do tych danych. EIOD, do którego zwrócono się o konsultacje, wydał kilka uwag, które zostały przesłane do odpowiednich instytucji oraz przedstawione Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych we wrześniu 2009 r.

Według EIOD umowa międzynarodowa powinna zapewnić:

- *zgodność z prawem i proporcjonalność żądań dotyczących przekazania danych, zwłaszcza w świetle naruszającego prywatność charakteru wniosku;*
- *dostępność środków prawnych i możliwość ich skutecznego wykorzystania przez obywateli Europy;*
- *ograniczenie dalszego udostępniania danych innym organom krajowym oraz innym państwom;*
- *możliwość korzystania przez niezależne organy nadzorujące ochronę danych ze swoich uprawnień nadzorczych, w tym dokonywania przeglądu realizacji umowy.*

W listopadzie 2009 r. podpisano umowę przejściową, lecz na mocy nowych przepisów traktatu lizbońskiego Parlament Europejski odmówił swojej zgody. W 2010 r. EIOD będzie nadal doradzać instytucjom UE w celu zagwarantowania, aby europejskie normy ochrony danych osobowych były przestrzegane – zwłaszcza w odniesieniu do jakiejkolwiek nowej umowy, która zastąpi umowę przejściową.

3.5.4. Środki ograniczające w odniesieniu do osób podejrzanych o terroryzm i niektórych państw trzecich

W dwóch opiniach wydanych w 2009 r. EIOD zajął się po raz pierwszy tzw. czarnymi listami terrorystów. Te narzędzia prawne mają służyć zwalczaniu terroryzmu i naruszania praw człowieka przez wprowadzenie środków ograniczających – w szczególności zamrażania aktywów i zakazu podróży – wobec osób fizycznych i prawnych podejrzewanych o związki z organizacjami terrorystycznymi lub niektórymi rządami. Komisja Europejska publikuje i rozpowszechnia czarne listy osób, które podlegają takim środkom ograniczającym.

Europejski Trybunał Sprawiedliwości potwierdził w kilku przypadkach, że wszystkie środki wspólnotowe, nawet wynikające z decyzji ONZ, powinny cechować się poszanowaniem praw podstawowych obowiązujących w UE, w szczególności prawa do obrony i prawa do złożenia wyjaśnień. Trybunał usunął z listy niektóre osoby dlatego, że nie mogły one poznać powodu ich umieszczenia na niej lub też pozostawały na liście przez kilka lat bez formalnego skazania lub trwającego dochodzenia w ich sprawie.

EIOD z zadowoleniem przyjął nowe wnioski Komisji mające na celu pełniejsze poszanowanie praw podstawowych i jednoznaczne uznanie zastosowania rozporządzenia (WE) nr 45/2001 w tej drażliwej politycznie dziedzinie. Zalecił też, aby:

- zapewnić jakość danych dzięki uwzględnieniu postępów w dochodzeniach policji i służb bezpieczeństwa, na których oparte są listy ,oraz przez dokonywanie regularnych przeglądów tych list;
- zapewnić wymienionym na listach osobom odpowiednie informacje oraz prawo dostępu do danych osobowych ich dotyczących;
- niezbędne obostrzenia i ograniczenia dotyczące tych praw zostały wyraźnie określone przepisami prawa, były przewidywalne i proporcjonalne;

EIOD zajmował się tym drażliwym tematem po raz pierwszy.

Czy w bazie danych Eurovigilance muszą być przetwarzane dane osobowe?

- zagwarantować możliwość zaskarżenia, odpowiedzialność i adekwatne odszkodowania w przypadku niezgodnego z prawem przetwarzania danych osobowych.

EIOD będzie nadal śledzić wydarzenia w tej dziedzinie zarówno jako doradca instytucji UE, jak i organ sprawujący nadzór nad przetwarzaniem wspomnianych czarnych list, w sprawie których Komisja Europejska wystosowała pod koniec 2009 r. powiadomienie dotyczące kontroli wstępnej.

3.6. Zdrowie publiczne

UE stworzyła ambitny program poprawy zdrowia obywateli w społeczeństwie informacyjnym i dostrzega wielkie możliwości usprawnienia transgranicznej opieki zdrowotnej dzięki wykorzystaniu technologii informacyjnych. Jest jednak oczywiste, że usprawnienie transgranicznej opieki zdrowotnej dzięki wykorzystaniu technologii informacyjnych niesie istotne implikacje dla ochrony danych osobowych.

Od 2008 r. Komisja przyjmuje lub proponuje konkretne inicjatywy w tej dziedzinie. Komisja opublikowała komunikat w sprawie telemedycyny i zalecenie w sprawie transgranicznej interoperacyjności systemów elektronicznych kart zdrowia. Usprawniła też system wczesnego ostrzegania i reagowania w odniesieniu do chorób zakaźnych oraz zaproponowała przepisy dotyczące praw pacjenta w transgranicznej opiece zdrowotnej, przy przeszczepianiu narządów i nadzorze nad bezpieczeństwem farmakoterapii (wykrywaniu i analizie działań niepożądanych leków).

EIOD wyraził ogólną obawę, że większość z tych tekstów ogranicza się do deklaracji poparcia dla ochrony danych. Wspomina się o kwestii ochrony danych i zamieszcza odniesienia do obowiązujących przepisów dotyczących ochrony danych, nie proponując jednak konkretnych zasad, które by rzeczywiście zapewniły przestrzeganie wymogów ochrony danych oraz zapewniły spójne stosowanie tych reguł przez państwa członkowskie. Wydaje się, że w sektorze opieki zdrowotnej brakuje spójnej wizji ochrony danych.

Można to częściowo tłumaczyć brakiem wiedzy na temat ochrony danych w sektorze zdrowia publicznego, co na szczeblu UE przejawia się niewiedzą odpowiedzialnych jednostek o istnieniu EIOD i o obowiązku konsultowania się z nim. Najbardziej uderzającym przykładem był w tym względzie wniosek w sprawie nadzoru nad bezpieczeństwem farmakoterapii, w którym prawie w ogóle nie wspomniano o ochronie danych i nie skierowano go do konsultacji do EIOD.

EIOD wielokrotnie podkreślał, że dane dotyczące zdrowia zalicza się do wrażliwych kategorii informacji osobistych, a przetwarzanie takich danych jest w zasadzie zabronione. Istnieją wyjątki, na przykład w przypadku diagnostyki medycznej, ale wyjątki te muszą być stosowane w sposób restrykcyjny.

W swojej opinii na temat nadzoru nad bezpieczeństwem farmakoterapii EIOD podkreślił zasadę konieczności i zakwestionował potrzebę przetwarzania danych osobowych w centralnej europejskiej bazie danych EudraVigilance.

W opinii w sprawie przeszczepiania narządów EIOD wyjaśnił pojęcie „anonimizacji". Wyjaśnił, że jeśli identyfikowalność narządów jest zapewniona, co oznacza, że dawcę można zawsze odnaleźć, towarzyszących informacji nie można w żadnym razie uznać za anonimowe. Ponieważ propozycje miały zapewnić jednocześnie identyfikowalność i anonimowość informacji, musiały zostać zmodyfikowane przez położenie nacisku na poufność informacji, a nie jej anonimowość.

EIOD wielokrotnie podkreślał, że zasad ochrony danych nie wprowadza się po to, by utrudniać efektywną współpracę w dziedzinie zdrowia publicznego. Wręcz przeciwnie – gwarancje ochrony danych mają fundamentalne znaczenie dla utrzymania zaufania do zawodu lekarza i służby zdrowia jako takiej.

Europejski Trybunał Praw Człowieka orzekł, że „ochrona danych osobowych, w szczególności danych medycznych, ma fundamentalne znaczenie w kontekście korzystania przez konkretną osobę z jej prawa do poszanowania życia prywatnego i rodzinnego, co gwarantuje art. 8 konwencji". I dalej: „poszanowanie poufności danych na temat zdrowia jest […] kluczowe […] nie tylko [dla poszanowania] poczucia prywatności pacjenta, ale również [dla ochrony] jego zaufania do zawodów związanych ze służbą zdrowia oraz ogólnie do usług zdrowotnych"([17]).

EIOD z zadowoleniem przyjął zaproszenie od Komisji Ochrony Środowiska Naturalnego, Zdrowia Publicznego i Bezpieczeństwa Żywności Parlamentu Europejskiego, które dało mu sposobność do uzasadnienia dwóch wydanych opinii (w sprawie transgranicznej opieki zdrowotnej i przeszczepiania narządów). EIOD wyraził też zadowolenie, że jego sugestie poskutkowały przyjęciem przez Parlament Europejski kilku poprawek, choć jak dotąd żaden z wnioskowanych aktów prawnych nie został przyjęty.

([17]) Zob. Europejski Trybunał Praw Człowieka, 17 lipca 2008 r., I. przeciwko Finlandii (nr wniosku 20511/03), pkt 38.

W związku ze swoimi działaniami w dziedzinie zdrowia publicznego EIOD przyjął zintegrowane podejście do pełnionych funkcji doradczych i nadzorczych.

Konsultacje w sprawie wniosków związanych z nadzorem nad bezpieczeństwem farmakoterapii łączyły się z analizą podjętą na podstawie dokonanego przez Europejską Agencję Leków (EMEA) powiadomienia dotyczącego kontroli wstępnej systemu. Tak samo było w przypadku rozwijanego dalej przez Komisję systemu wczesnego ostrzegania i reagowania w odniesieniu do chorób zakaźnych oraz Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób (ECDC). EIOD zgłosił nieoficjalne uwagi na temat stosownej decyzji Komisji i po otrzymaniu powiadomienia dotyczącego wstępnej kontroli rozpoczął analizę systemu.

3.7. Dostęp publiczny a dane osobowe

3.7.1. Wprowadzenie

Złożone relacje między zasadami UE dotyczącymi publicznego dostępu do dokumentów a ochroną danych są od kilku lat przedmiotem zainteresowania EIOD. W 2009 r. EIOD wziął udział w dyskusji na temat zmian w prawodawstwie UE w sprawie publicznego dostępu do dokumentów oraz interweniował w dotyczących tej materii sprawach toczących się przed Sądem, w tym w sprawie *Bavarian Lager*. Ponadto tematu tego dotyczyło pierwsze wniesione do Sądu odwołanie od decyzji EIOD w sprawie skargi.

3.7.2. Zmiana prawodawstwa UE w sprawie publicznego dostępu do dokumentów

Wysłuchawszy trwających w Parlamencie Europejskim debat dotyczących zmiany prawodawstwa UE w sprawie publicznego dostępu do dokumentów, EIOD streścił poglądy wyrażone w swojej opinii z dnia 30 czerwca 2008 r. w formie krótkich uwag. EIOD podkreślił negatywne konsekwencje niektórych poprawek zgłoszonych w PE dla równowagi między obydwoma prawami. EIOD z zadowoleniem stwierdził, że wynik głosowań na sesji plenarnej dowiódł niemal pełnego poparcia dla jego podejścia.

W komunikacie prasowym wydanym po głosowaniu EIOD oświadczył: „Poprawki te rozjaśniają obraz oraz zapobiegają nadgorliwemu stosowaniu przepisów dotyczących ochrony danych w tym obszarze. Potwierdzają one, że ochrona danych nie jest przeszkodą dla ujawnienia informacji osobistych w przypadkach, w których dana osoba nie ma uzasadnionych powodów do utrzymywania danych w tajemnicy".

EIOD wyjaśnił swoje stanowisko w formie ustnej na forum grupy roboczej Rady ds. informacji. Pomimo wysiłków prezydencji szwedzkiej mających na celu skłonienie Rady do zaakceptowania zmian w drugiej połowie 2009 r., dyskusja w ich sprawie utknęła w miejscu z powodu konfliktu proceduralnego między Komisją a Parlamentem, którego nie udało się jak dotąd rozstrzygnąć.

3.7.3. Odwołanie w sprawie Bavarian Lager

Sprawa *Bavarian Lager* dotyczyła odmowy ujawnienia przez Komisję pięciu nazwisk wymienionych w dokumencie KE. Komisja odwołała się od wyroku Sądu z dnia 8 listopada 2007 r., co doprowadziło do rozprawy w dniu 16 czerwca 2009 r. Podczas tej rozprawy EIOD opowiedział się za utrzymaniem wyroku Sądu. Mimo że w swojej opinii z dnia 15 października 2009 r. rzecznik generalna Eleonor Sharpston również nie zgodziła się z apelacją Komisji, nie podzieliła ona popartego przez EIOD toku rozumowania Sądu. Jako że wniosek wyciągnięty przez rzecznika generalnego opierał się na rozumowaniu, które w ogóle nie było omawiane przez strony, EIOD i Komisja zwrócili się do Sądu o otwarcie procedury ustnej na nowo.

3.7.4. Inne sprawy sądowe dotyczące dostępu publicznego i ochrony danych

Sprawa sądowa *Dennekamp* dotyczyła udzielonej przez Parlament odmowy ujawnienia dokumentów informujących, którzy posłowie do Parlamentu Europejskiego są również członkami dodatkowego systemu emerytalnego. Z prawnego punktu widzenia sprawę tę można uznać za przypadek szczególny sprawy *Bavarian Lager*. Z tego powodu EIOD interweniował w sprawie.

Pierwsze w historii odwołanie od decyzji EIOD wniosła p. Kitou w dniu 3 kwietnia 2009 r. Nie zgodziła się ona z decyzją EIOD, w której stwierdził on, że zasady ochrony danych nie uniemożliwiają podania przez Komisję do wiadomości publicznej, czy pracowała ona w Komisji w danym okresie.

W chwili druku niniejszego sprawozdania rocznego obydwie sprawy pozostawały w toku.

Dwie inne sprawy sądowe związane z omawianym obszarem, które również są w toku, wniósł p. Pachtitis przeciwko Komisji i EPSO – do Sądu oraz do Sądu do spraw Służby Publicznej. Przedmiot tych spraw różni się od przypadków opisanych powyżej, ponieważ skarżący wnioskował o dostęp do **własnych** danych osobowych, którego Komisja odmówiła na podstawie przepisów UE w sprawie publicznego dostępu do dokumentów. W pismach procesowych i podczas rozprawy przed Sądem do spraw Służby Publicznej, która odbyła się w dniu 1 grudnia 2009 r., EIOD twierdził, że wniosek o dostęp powinien był zostać rozpatrzony zgodnie z zasadami ochrony danych i że zasady te powinny były zostać zastosowane w aktywny sposób przez Komisję.

Podczas dyskusji na temat zmiany zasad UE dotyczących publicznego dostępu do dokumentów EIOD argumentował, że obowiązek ten należy zamieścić w preambule do zmienionego dokumentu. Parlament Europejski poparł tę sugestię.

Złożona relacja między tymi dwoma prawami podstawowymi to jeden z obszarów pracy EIOD.

3.8. Inne zagadnienia

3.8.1. System wymiany informacji na rynku wewnętrznym (IMI)

W 2009 r. EIOD w dalszym ciągu aktywnie uczestniczył w rozwoju systemu IMI, który jest być może najbardziej spektakularnym przykładem współpracy administracyjnej poprzez wymianę informacji, jak

też narzędziem dalszej integracji europejskiej. System IMI wszedł do użycia – do końca 2009 r. zarejestrowało się ponad 4500 właściwych organów, podjęto też liczne kroki w celu wbudowania weń zabezpieczeń gwarantujących ochronę danych.

EIOD z zadowoleniem powitał te wysiłki, podkreślając jednak stale znaczenie bardziej kompleksowych ram prawnych funkcjonowania systemu IMI w celu zapewnienia pewności prawa oraz wyższego poziomu ochrony danych – najlepiej w postaci rozporządzenia Rady i Parlamentu.

3.8.2. Inne opinie

EIOD wydał również kilka opinii na tematy, w których ochrona danych nie była zagadnieniem głównym, niemniej kwestia przetwarzania danych osobowych była obecna. Odnosiły się one do wniosku dotyczącego dyrektywy Rady nakładającej na państwa członkowskie obowiązek utrzymywania minimalnych zapasów ropy naftowej lub produktów naftowych, wniosku dotyczącego rozporządzenia Rady ustanawiającego wspólnotowy system kontroli w celu zapewnienia przestrzegania przepisów wspólnej polityki rybołówstwa oraz zalecenia dotyczącego rozporządzenia Rady w sprawie zbierania informacji statystycznych przez Europejski Bank Centralny.

3.9. Spojrzenie w przyszłość

3.9.1. Zmiany technologiczne

Jak wspomniano w sprawozdaniu rocznym EIOD za 2007 r., społeczeństwa informacyjnego nie należy traktować jako środowiska równoległego i wirtualnego, ale w coraz większym stopniu jako złożony, interaktywny świat przenikający się ze światem fizycznym jednostek. Zbliżenie między tymi dwoma światami ułatwia coraz większa liczba pomostów powstających dzięki innowacyjnemu wykorzystaniu technologii istniejących oraz rozwojowi nowych i wyłaniających się technologii. Jest to tendencja naturalna i pożądana, która doprowadzi ostatecznie do pełnej integracji – społeczeństwo informacyjne stanie się po prostu częścią społeczeństwa.

Coraz większa liczba tych pomostów prowadzi jednak do zacierania granic między światami, które nie zawsze są obecnie regulowane przez te same ramy prawne, a tym samym stwarza niepewność prawną, co może podważać zaufanie i być szkodliwe dla rozwoju społeczeństwa informacyjnego.

Poniżej przedstawiono przykłady kilku takich pomostów:

- ***Inteligentna telewizja przemysłowa**: systemy takie są często wykorzystywane w dochodzeniach w sprawie zdarzeń, które miały miejsce w przeszłości, a następnie przy ściganiu sprawców przestępstw. Dzięki oprogramowaniu do rozpoznawania twarzy oraz prywatnym lub publicznym bazom danych, takim jak sieci społecznościowe, rejestrowane w czasie rzeczywistym nagrania telewizji przemysłowej (świat realny) mogą być uzupełniane dodatkowymi danymi pochodzącymi z Internetu (świat cyfrowy).*
- ***Internet przedmiotów**: To ogólne pojęcie jest zdefiniowane w komunikacie Komisji ([18]) z czerwca 2009 r. Te sieci połączonych wzajemnie, opatrzonych etykietami przedmiotów ustanowią niewątpliwie związki między fizycznymi właściwościami przedmiotów (np. ich lokalizacją, sytuacją, czynnościami, zachowaniami, właścicielami) a dotyczącymi ich informacjami internetowymi, które są stale dostarczane za pośrednictwem sieci czujników. W tym nowym środowisku długi cykl życia niektórych przedmiotów opatrzonych etykietami (np. opony, okulary) skonsoliduje te związki, dostarczając z czasem jeszcze dokładniejszych informacji na temat zarówno przedmiotów, jak i ich właścicieli.*
- ***Inteligentna lodówka**: w tym nadużywanym przykładzie urządzenia domowe i kuchenne powiązane są z dostawcami usług. Chociaż aktywne monitorowanie wykorzystania lodówki w gospodarstwie domowym jest uznawane za niedopuszczalne, przetwarzanie danych wygenerowanych przez tę samą lodówkę i przekazywanych dostawcom usług może podlegać odmiennym przepisom.*
- ***Reklama behawioralna w Internecie**: przetwarzanie i łączenie różnorodnych danych dotyczących zachowania osób w Internecie skutkuje precyzyjnymi profilami, które mogą być wykorzystywane w celu przedstawiania ukierunkowanych reklam. Przeglądarki internetowe lub nowe urządzenia komunikacyjne dostarczają danych dotyczących lokalizacji, a informacje o przemieszczeniach związane z innymi urządzeniami, przedmiotami, ludźmi, sklepami itp. mogą w połączeniu z danymi o zachowaniach w Internecie posłużyć stworzeniu kompletnego profilu użytkownika.*

([18]) „Internet przedmiotów – plan działań dla Europy", COM(2009) 278 wersja ostateczna z 18 czerwca 2009 r., http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

Społeczeństwo informacyjne przenika się na każdym kroku z naszym fizycznym światem.

Zlewanie się tych dwóch światów w jednolitą przestrzeń stwarza bez wątpienia nowe wyzwania dla ram prawnych UE dotyczących ochrony prywatności i danych. Celem jest oczywiście pogodzenie środowiska sieciowego i pozasieciowego w ramach zharmonizowanych norm lub przynajmniej uzyskanie większej zgodności między nimi, co może zapobiec podkopaniu zaufania do otwierającej wielkie możliwości epoki cyfrowej.

3.9.2. Wydarzenia polityczne i legislacyjne

W chwili kierowania niniejszego sprawozdania rocznego do druku następują lub nastąpiły już istotne wydarzenia, które określą kontekst polityki i legislacji w 2010 r.:

- *Co najważniejsze, w życie wszedł **traktat lizboński**, zwiększając znaczenie ochrony danych w ramach traktatowych oraz stwarzając potrzebę działań legislacyjnych.*
- ***Program sztokholmski** kładzie znaczny nacisk na ochronę danych. Podkreśla się w nim znaczenie ochrony praw podstawowych w społeczeństwie informacyjnym i uznaje ochronę danych za warunek wstępny wymiany informacji służącej zapewnieniu bezpieczeństwa społeczeństwa.*
- ***Nowa Komisja** rozpoczęła prace ze sporymi ambicjami w dziedzinie ochrony danych i prywatności. Nowa komisarz ds. sprawiedliwości i praw podstawowych wskazuje jako jeden ze swoich priorytetów stworzenie kompleksowych ram ochrony danych.*
- *Nowa Komisja pracuje nad **europejską agendą cyfrową**, w ramach której **niezbędnymi warunkami wstępnymi jest ochrona prywatności i danych**, ze szczególnym naciskiem na przykład na wbudowaną ochronę prywatności.*
- *Następują również istotne zmiany, które umożliwią UE i jej państwom członkowskim skuteczniejsze radzenie sobie z **zewnętrznym wymiarem ochrony danych**, nie tylko w odniesieniu do Stanów Zjednoczonych jako najważniejszej zainteresowanej strony w dziedzinie wymiany danych, ale także w sensie ogólniejszym dzięki dalszemu rozwojowi ogólnoświatowych norm.*

Zmiany te staną się oczywiście bardziej widoczne, gdy nowa Komisja przedstawi szczegółowo swoje plany. Ważnymi dokumentami w tym kontekście będzie plan prac nowej Komisji na 2010 r. oraz plan działań służący realizacji programu sztokholmskiego. EIOD jest oczywiście szczególnie zainteresowany dalszymi działaniami związanymi z konsultacjami społecznymi w sprawie przyszłych ram ochrony danych.

Innymi obszarami, gdzie nowe wydarzenia będą zapewne miały wpływ na przetwarzanie danych osobowych, są różne europejskie mechanizmy w dziedzinie zdrowia publicznego, współpracy w zakresie opodatkowania, transportu (w tym nowe rozwiązania dotyczące monitorowania samochodów) oraz projekt e-sprawiedliwości.

3.9.3. Priorytety na 2010 r.

EIOD określi swoje priorytety na 2010 r. w kontekście rozwoju sytuacji w ciągu roku i będzie kontynuować kierunek działań doradczych obrany w 2009 r. Priorytety zostaną określone w spisie na 2010 r., którego publikacja nastąpi po ogłoszeniu przez Komisję programu prac na 2010 r., co zgodnie z przewidywaniami będzie miało miejsce pod koniec marca tego roku.

4

WSPÓŁPRACA

4.1. Grupa robocza art. 29

Grupę roboczą art. 29 powołano na mocy art. 29 dyrektywy 95/46/WE. Jest to niezależny organ doradczy zajmujący się kwestią ochrony danych osobowych w ramach wspomnianej dyrektywy ([19]). Jej zadania określa art. 30 dyrektywy i można je podsumować w następujący sposób:

- przekazywanie opinii eksperckich w sprawach dotyczących ochrony danych z państw członkowskich do Komisji Europejskiej;
- działanie na rzecz jednolitego stosowania ogólnych zasad dyrektywy we wszystkich państwach członkowskich dzięki współpracy pomiędzy organami nadzorującymi ochronę danych;
- doradzanie Komisji w sprawie wszelkich środków wspólnotowych mających wpływ na prawa i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych;
- formułowanie zaleceń dla ogółu społeczeństwa, w szczególności dla instytucji wspólnotowych w sprawach dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie Europejskiej.

EIOD jest członkiem grupy roboczej art. 29 od początku 2004 r. Artykuł 46 lit. g) rozporządzenia (WE) nr 45/2001 stanowi, że EIOD bierze udział w działalności grupy roboczej. EIOD uważa, że jest to bardzo ważna platforma współpracy z krajowymi organami nadzoru. Jest również oczywiste, że grupa robocza powinna odgrywać fundamentalną rolę w spójnym stosowaniu dyrektywy i w interpretacji jej ogólnych zasad.

W 2009 r. grupa robocza skoncentrowała swoją działalność na elementach określonych w jej programie prac na lata 2008–2009, w szczególności na:

- lepszym wdrożeniu dyrektywy 95/46/WE;
- zapewnieniu ochrony danych w wymianie międzynarodowej;
- zapewnieniu ochrony danych w odniesieniu do nowych technologii;
- zwiększeniu skuteczności działań grupy roboczej art. 29.

Grupa robocza przyjęła pewną liczbę dokumentów w tym zakresie, do których należą:

- **Lepsze wdrożenie dyrektywy 95/46/WE:** wspólny wkład w sprawie przyszłości prywatności w odpowiedzi na konsultacje

([19]) Grupa robocza składa się z przedstawicieli krajowych organów nadzorczych w poszczególnych państwach członkowskich, przedstawiciela organu ustanowionego dla instytucji i organów wspólnotowych (tj. EIOD) oraz przedstawiciela Komisji. Komisja obsługuje również sekretariat grupy roboczej. Krajowe organy nadzorcze Islandii, Norwegii i Liechtensteinu (jako partnerów w ramach EOG) są reprezentowane w roli obserwatorów.

Komisji Europejskiej w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych (WP168).

- **Wymiana międzynarodowa:** Opinia 3/2009 na temat projektu decyzji Komisji w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich, na mocy dyrektywy 95/46/WE (od administratora danych do podmiotu przetwarzającego) (WP161); opinie w sprawie adekwatności Andory (WP166) oraz Izraela (WP165).

- **Nowe technologie:** Opinia w sprawie sieci społecznościowych w Internecie (WP163); opinia w sprawie wniosków zmieniających dyrektywę 2002/58/WE o prywatności i łączności elektronicznej (dyrektywę o prywatności i łączności) (WP159).

Grupa robocza reagowała na rozwój w dziedzinie **nowych technologii** i monitorowała realizację swojej przyjętej w 2008 r. opinii w sprawie **wyszukiwarek**, organizując wysłuchanie dostawców usług wyszukiwania.

Grupa robocza i EIOD kontynuowali ścisłą współpracę w kwestiach związanych z nowymi wyzwaniami w dziedzinie ochrony danych. Oprócz ścisłej współpracy w odniesieniu do **przyszłych ram ochrony danych**, grupa robocza i EIOD sporządzili wspólną odpowiedź w związku z konsultacjami Komisji w sprawie „**skutków wykorzystania skanerów ciała** w dziedzinie ochrony lotnictwa z punktu widzenia praw człowieka, prywatności, godności osobistej, zdrowia i ochrony danych".

EIOD współpracuje również z krajowymi organami nadzoru w stopniu koniecznym dla wykonywania ich obowiązków, w szczególności przez wymianę wszystkich użytecznych informacji i wnioskowanie o pomoc lub udzielanie pomocy w realizacji ich zadań (art. 46 lit. f) ppkt (i) rozporządzenia). Współpraca taka jest podejmowana w konkretnych przypadkach.

Bezpośrednia współpraca z organami krajowymi staje się coraz bardziej istotna w kontekście rozwoju dużych międzynarodowych systemów, takich jak Eurodac, które wymagają skoordynowanego podejścia do kwestii nadzoru (zob. rozdz. 4.3).

4.2. Grupa robocza Rady ds. ochrony danych

W ostatnich latach, podczas urzędowania kolejnych prezydencji, grupa robocza Rady ds. ochrony danych stanowiła dla państw członkowskich forum służące omawianiu kwestii ochrony danych w ramach dawnego „pierwszego filaru". W 2009 r. grupa robocza zebrała się tylko raz, podczas prezydencji czeskiej. EIOD wykorzystał tę okazję, aby zaprezentować przedstawicielom państw członkowskich ogólne informacje o swojej działalności.

Ze względu na brak ogólnych inicjatyw legislacyjnych dotyczących ochrony danych w tym obszarze grupa robocza nie wykorzystywała w pełni swojego potencjału. Działając jednak jako platforma wymiany informacji i aktywnie wspomagając inne podmioty swoją wiedzą, grupa robocza może odgrywać konstruktywną rolę w rozwoju kompleksowych ram prawnych dotyczących ochrony danych, co EIOD przyjąłby z zadowoleniem.

Prezydencja hiszpańska przewiduje kolejne spotkanie grupy roboczej w marcu 2010 r.

4.3. Skoordynowany nadzór nad Eurodac

Skuteczny nadzór nad Eurodac opiera się na ścisłej współpracy pomiędzy krajowymi organami ochrony danych i EIOD. Złożona z przedstawicieli krajowych organów ochrony danych oraz EIOD grupa ds. koordynowania nadzoru nad systemem Eurodac („grupa") zebrała się w 2009 r. trzykrotnie.

Drugie sprawozdanie z kontroli

Jednym z najważniejszych osiągnięć grupy w tym roku było przyjęcie w czerwcu drugiego sprawozdania z kontroli. Sprawozdanie to przedstawia ustalenia i zalecenia oparte na odpowiedziach otrzymanych od wszystkich państw członkowskich. Jednym z celów tych działań jest wniesienie wartościowego wkładu w trwający przegląd systemu dublińskiego i Eurodac (zob. również rozdz. 3.3.2).

Dwiema głównymi kwestiami, które podlegały kontroli grupy, było prawo do informacji osób ubiegających się o azyl oraz metody oceny wieku młodych osób ubiegających się o azyl. Sprawozdanie wysłano do najważniejszych zainteresowanych problemem instytucji UE, jak również do organizacji

międzynarodowych i pozarządowych działających w dziedzinie azylu oraz imigracji.

Prawo do informacji

Bez jasnych i łatwo dostępnych informacji osoby objęte działaniem systemu Eurodac nie są w stanie korzystać ze swoich praw w zakresie ochrony danych.

Kontrola wykazała, że informacje dla osób ubiegających się o azyl o ich prawach i sposobie wykorzystania ich danych są zazwyczaj niekompletne, w szczególności w zakresie konsekwencji zdejmowania odcisków palców oraz prawo dostępu do własnych danych i ich poprawiania. Zakres dostępnych informacji znacznie różni się w zależności od państwa członkowskiego, a w praktykach wobec osób ubiegających się o azyl i nielegalnych imigrantów zaobserwowano znaczne różnice.

W związku z tym w sprawozdaniu zalecono, aby państwa członkowskie poprawiły jakość udostępnianych informacji dotyczących ochrony danych. Informacje te powinny uwzględniać prawo dostępu do danych i ich poprawiania, a także procedury korzystania z tego prawa. Ponadto organy odpowiedzialne za udzielanie azylu powinny zapewnić takie same informacje zarówno cudzoziemcom ubiegającym się o azyl, jak i nielegalnym imigrantom, oraz formułować je w wyraźny i zrozumiały sposób. Szczególny nacisk należy położyć na zapewnienie widoczności i dostępności informacji. Dodatkowo państwa członkowskie powinny promować współpracę oraz wymianę doświadczeń między właściwymi organami krajowymi, zachęcając grupę roboczą do badania tej kwestii, i docelowo wypracować zharmonizowane praktyki.

Ocena wieku osób ubiegających się o azyl

Zgodnie z rozporządzeniem Eurodac w przypadku dzieci w wieku 14 lat i starszych powinny być zdejmowane odciski palców. Występują jednak często problemy z określeniem wieku dziecka, które nie ma przy sobie żadnych wiarygodnych dokumentów tożsamości, tak więc na szczeblu krajowym stosowane są różne metody.

Kontrola przeprowadzona przez grupę koncentrowała się zarówno na metodach oceny wieku osób ubiegających się o azyl (w tym też naruszających prywatność badaniach lekarskich), jak i na samej procedurze badań.

W jednym z wniosków stwierdzono, że metody określania wieku osób ubiegających się o azyl powinny być wyraźnie określone i podane do publicznej wiadomości. Zasugerowano, że w celu wsparcia harmonizacji Komisja powinna dokonać ogólnej oceny (uwzględniając aspekty medyczne i etyczne) wiarygodności różnych metod oceny wieku wykorzystywanych w państwach członkowskich,

Ponadto osoba ubiegająca się o azyl powinna mieć prawo wnioskowania o drugą opinię w sprawie wyników medycznych i wniosków z nich płynących bez ponoszenia kosztów. Przy podejmowaniu decyzji dotyczących statusu prawnego osoby ubiegającej się o azyl organy odpowiedzialne za udzielanie azylu powinny brać pod uwagę margines błędu obecny w przypadku niektórych badań lekarskich.

4.4. Trzeci filar

EIOD kontynuował współpracę ze wspólnymi organami nadzorczymi, które zajmują się zagadnieniami Schengen, Europolu, Eurojustu i Systemu Informacji Celnej oraz z Grupą Roboczą ds. Policji i Wymiaru Sprawiedliwości powołaną przez europejską konferencję rzeczników ochrony danych w celu monitorowania rozwoju sytuacji w zakresie ochrony danych w dziedzinie egzekwowania prawa oraz reagowania na zachodzące wydarzenia.

Współpraca ze wspólnymi organami nadzorczymi koncentrowała się na wymianie informacji oraz działaniu na rzecz spójności i usprawnienia nadzoru nad ochroną danych, zwłaszcza w związku z wejściem w życie traktatu lizbońskiego. Grupę Roboczą ds. Policji i Wymiaru Sprawiedliwości można uznać za nieformalne uzupełnienie grupy roboczej art. 29 w obszarach, w których brakuje jej kompetencji, w szczególności dawnego „trzeciego filaru". Jako członek grupy EIOD aktywnie uczestniczył w jej działalności:

- wnosząc wkład w debatę na temat programu sztokholmskiego;
- oceniając wpływ decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej, ze szczególnym uwzględnieniem sposobów zagwarantowania zharmonizowanego podejścia do wdrożenia na szczeblu krajowym;

- monitorując wdrażanie Konwencji Rady Europy o cyberprzestępczości – pierwszej umowy międzynarodowej określającej wspólną politykę ochrony społeczeństwa przed przestępstwami popełnianymi za pośrednictwem Internetu lub innych sieci komputerowych;

- wyrażając głębokie zaniepokojenie, zgodnie z opinią EIOD, w związku z wnioskiem Komisji, aby umożliwić dostęp do systemu Eurodac w celach związanych z egzekwowaniem prawa;

- sporządzając rejestr dotyczący współpracy i nadzoru w obszarze egzekwowania prawa w UE, który został następnie przyjęty przez europejską konferencję;

- monitorując i udoskonalając istniejące umowy dwustronne oraz wielostronne między państwami europejskimi i pozaeuropejskimi w dziedzinie współpracy policyjnej i sądowej w sprawach karnych, w tym walki z terroryzmem;

- śledząc wydarzenia związane z umową międzynarodową z USA w sprawie przekazywania danych z komunikatów finansowych do celów programu śledzenia środków finansowych należących do terrorystów, jak i z szerszą debatą w sprawie ustanowienia transatlantyckich zasad ochrony danych;

- wnosząc wkład we wspólny dokument na temat przyszłości ochrony danych w Europie w odpowiedzi na konsultacje społeczne zainicjowane przez Komisję Europejską.

W celu zapewnienia spójności działań europejskich organów ochrony danych grupa współpracowała ściśle z grupą roboczą art. 29, nawiązując również do stanowisk przyjmowanych przez EIOD.

4.5. Konferencja europejska

Przedstawiciele organów ochrony danych z państw członkowskich Unii Europejskiej i Rady Europy spotykają się co roku na wiosennej konferencji w celu omówienia spraw będących przedmiotem wspólnego zainteresowania oraz wymiany informacji i doświadczeń na różne tematy. **Europejska Konferencja Rzeczników Ochrony Danych Osobowych odbyła się w Edynburgu w dniach 23 i 24 kwietnia 2009 r.**

Uczestnicy konferencji skupili się na potrzebie dokonania **przeglądu europejskich ram ochrony danych**. W związku z tym tematem zorganizowano cztery sesje:

- prezentacja projektu sprawozdania sporządzonego przez RAND Europe na zlecenie biura brytyjskiego Komisarza ds. Informacji i zatytułowanego „Przegląd unijnej dyrektywy w sprawie ochrony danych", w związku z którym EIOD zgłosił uwagi;

- sesja pod hasłem: Czy w ogóle potrzebujemy reform? Inne spojrzenie na zalety i wady dyrektywy 95/46/WE;

- sesja zatytułowana: Jakie powinny być cele regulacji w odniesieniu do osób fizycznych, społeczeństwa i organów regulacyjnych?

- sesja poświęcona międzynarodowemu kontekstowi regulacji.

Podczas konferencji przyjęto deklarację na temat przywództwa i przyszłości ochrony danych w Europie, w której podkreślono rolę organów ochrony danych w toczącej się debacie. Uczestnicy konferencji przyjęli także uchwałę w sprawie umów dwustronnych między państwami członkowskimi UE a państwami trzecimi w obszarze współpracy policyjnej i sądowej w sprawach karnych.

Konferencja stanowiła również okazję do przedstawienia sprawozdania z odbywających się co pół roku warsztatów poświęconych rozpatrywaniu spraw, podczas których pracownicy europejskich organów ochrony danych wymieniają koncepcje dotyczące najlepszych praktyk. W 2009 r. warsztaty odbyły się w Pradze (Czechy) i Limassol (Cypr). Kolejne warsztaty zostaną zorganizowane w Brukseli na wiosnę 2010 r.

Następna konferencja europejska, organizowana przez czeski organ ochrony danych, odbędzie się w Pradze w dniach 29 i 30 kwietnia 2010 r.

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

Peter Hustinx przemawia podczas Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności (Madryt, 4–6 listopada 2009 r.).

roku **Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności została zorganizowana przez hiszpański organ ochrony danych w Madrycie w dniach 4–6 listopada 2009 r.** i przyciągnęła ponad tysiąc uczestników – najwięcej jak dotychczas. Jej temat przewodni brzmiał: „Prywatność – dziś jest jutrem".

Dyskusje podczas sesji plenarnych dotyczyły następujących tematów:

- Społeczeństwo pod nadzorem? Dążenie do równowagi między bezpieczeństwem a prywatnością;
- Quo vadis, Internecie?
- Prywatność a odpowiedzialność biznesu;
- Ochrona prywatności osób niepełnoletnich: misja priorytetowa;
- Wbudowana ochrona prywatności;
- Dążenie do globalnych regulacji chroniących prywatność: wnioski i strategie.

Jedną z głównych kwestii poruszonych podczas konferencji była ochrona danych jako strategiczny element działalności biznesowej i międzynarodowej wymiany danych w zglobalizowanym świecie. Konferencja stanowiła sposobność, by zaobserwować rosnące zapotrzebowanie ze strony zainteresowanych podmiotów, w tym społeczeństwa obywatelskiego i przemysłu, dotyczące wprowadzenia zharmonizowanych, ponadpaństwowych ram ochrony danych. W tym duchu uczestnicy konferencji przyjęli rezolucję wyrażającą zadowolenie z opracowania projektu międzynarodowych norm ochrony danych osobowych i prywatności. Normy te są wynikiem intensywnych rocznych prac przygotowawczych koordynowanych przez hiszpański organ ochrony danych i stanowią pierwszy krok na drodze do opracowania wiążącego dokumentu międzynarodowego.

Kolejny problem, który został szczegółowo omówiony w Madrycie, to systemy nadzoru, zwłaszcza bazujące na cechach ludzkiego ciała (np. danych biometrycznych), które są coraz częściej wykorzystywane w życiu codziennym.

W konferencji uczestniczyli zarówno Inspektor, jak i jego zastępca. Inspektor przewodniczył sesji zatytułowanej „Ustalanie prawa właściwego w zglobalizowanym świecie", a podczas równoległej sesji na temat „Życie prywatne w pracy?" głos zabrał jego zastępca.

Następna konferencja odbędzie się w Jerozolimie w dniach 27–29 października 2010 r.

4.7. Inicjatywa londyńska

Podczas 28. międzynarodowej konferencji w Londynie w listopadzie 2006 r. przedstawiono oświadczenie zatytułowane „Informowanie o ochronie danych i czynienie jej skuteczniejszą", które spotkało się z ogólnym poparciem organów ochrony danych z całego świata. Była to wspólna inicjatywa prezesa francuskiego organu ochrony danych (CNIL), brytyjskiego komisarza ds. informacji oraz EIOD (zwana odtąd „inicjatywą londyńską"). Jako jeden z architektów inicjatywy EIOD będzie aktywnie uczestniczyć w monitorowaniu związanych z nią działań wraz z krajowymi organami ochrony danych ([20]).

W kontekście inicjatywy londyńskiej zorganizowano wiele warsztatów w celu wymiany doświadczeń i najlepszych praktyk w różnych dziedzinach, takich jak komunikacja, egzekwowanie prawa, planowanie strategiczne oraz zarządzanie organami ochrony danych.

W kwietniu 2009 r. EIOD zorganizował w Brukseli warsztaty dla organów ochrony danych w celu wymiany najlepszych praktyk w zakresie reakcji na naruszenia bezpieczeństwa. Te zamknięte warsztaty dostarczyły też materiału dla seminarium na ten sam temat z udziałem innych zainteresowanych stron, zorganizowanego przez EIOD wraz z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA) w siedzibie Parlamentu Europejskiego w październiku 2009 r.

4.8. Organizacje międzynarodowe

W listopadzie 2009 r. EIOD rozpoczął wraz z Europejskim Instytutem Uniwersyteckim (EUI) przygotowania do trzeciej edycji warsztatów na temat ochrony danych w organizacjach międzynarodowych, które odbędą się wiosną 2010 r. we Florencji.

W rezultacie przyjętej w 2003 r. na konferencji międzynarodowej w Sydney ([21]) rezolucji w sprawie ochrony danych i organizacji międzynarodowych, EIOD wraz z Radą Europy, OECD i Europejskim Urzędem Patentowym zorganizował już wcześniej dwa warsztaty w Genewie (2005) i Monachium (2007). Zwolnione ze stosowania prawa krajowego organizacje międzynarodowe w wielu przypadkach nie posiadają ram prawnych ochrony danych. Ich udział we wspomnianych wydarzeniach wskazuje na ich rosnące zainteresowanie zarówno ochroną danych osobowych, jak i zapewnieniem przestrzegania jej zasad.

Podczas kolejnych warsztatów EIOD zamierza skupić dyskusję na następujących kwestiach:

- zarządzanie ochroną danych w organizacjach międzynarodowych;
- przestrzeganie zasad w praktyce, zwłaszcza w zakresie zarządzania danymi dotyczącymi zasobów ludzkich;
- wyzwania technologiczne oraz odpowiednie środków bezpieczeństwa;
- wykorzystanie danych biometrycznych na granicach i do celów zapewnienia bezpieczeństwa wewnętrznego.

([20]) Zob. Sprawozdanie roczne 2006, pkt 4.5 i 5.1.

([21]) http://www.privacyconference2008.org/adopted_resolutions/5-SYDNEY2003/SYDNEY-EN4.pdf

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 ogóle. Ma to tym większe znaczenie, że EIOD jest instytucją ustanowioną niedawno i dlatego świadomość jego roli na szczeblu UE musi być dalej zwiększana. W początkowych latach funkcjonowania EIOD skupiał swoje działania przede wszystkim na tym celu, co generalnie poskutkowało zwiększeniem widoczności jego urzędu. Wzrost wskaźników, takich jak liczba wniosków od obywateli UE o udzielenie informacji, pytań ze strony mediów, odbiorców biuletynu, zaproszeń do wystąpienia na konferencjach oraz osób odwiedzających stronę internetową, jednoznacznie wskazuje, że EIOD stał się ważnym punktem odniesienia w dziedzinie ochrony danych.

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 formułowanie polityki (Komisja, Rada i Parlament), która może mieć wpływ na ochronę danych osobowych; funkcji współpracy z krajowymi organami nadzoru, jak też różnymi organami nadzorczymi w dziedzinie bezpieczeństwa i wymiaru sprawiedliwości.

Podnoszenie świadomości i poprawienie komunikacji w istotnych kwestiach dotyczących ochrony danych było również ważnym celem inicjatywy londyńskiej (zob. rozdz. 4.7). Jednym z istotnych rezultatów pierwszych warsztatów w tym kontekście było utworzenie (z udziałem EIOD) sieci specjalistów ds. komunikacji. Organy ochrony danych wykorzystują tę sieć w celu wymiany najlepszych praktyk oraz realizacji określonych projektów, takich jak podejmowanie wspólnych działań przy okazji istotnych wydarzeń.

Działania komunikacyjne w 2009 r. były ukierunkowane głównie na usprawnienie i rozwój narzędzi informacyjnych oraz komunikacyjnych stworzonych w pierwszych latach funkcjonowania instytucji w celu skuteczniejszego komunikowania się oraz dotarcia zarówno do administracji UE, jak i ogółu społeczeństwa.

W swoich wystąpieniach w ciągu roku (zob. załącznik G) Inspektor oraz jego zastępca poświęcili wiele czasu i wysiłku na wyjaśnianie misji EIOD i podnoszenie świadomości na temat ochrony danych oraz innych konkretnych kwestii.

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 dostosować się do rozmaitych ograniczeń i wymogów.

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 podmioty danych, 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 głównie na działaniu organów ochrony danych na szczeblu krajowym oraz wykorzystywaniu ośrodków informacyjnych i punktów kontaktowych.

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.

Polityka językowa

Polityka komunikacyjna EIOD musi również uwzględniać szczególną dziedzinę działalności jego instytucji. Problematyka ochrony danych może być postrzegana jako skomplikowana i niejasna dla laika, a zatem język używany w komunikacji 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 w związku z tym stałe wysiłki służące skorygowaniu nadmiernie „legalistycznego" wizerunku kwestii ochrony danych.

W przypadku odbiorców bardziej wyspecjalizowanych (np. media, specjaliści w zakresie ochrony danych, zainteresowane podmioty UE) stosowanie terminów technicznych i prawnych jest bardziej celowe. Dlatego też może być konieczne przekazywanie tych samych wiadomości przy użyciu innej formy i stylu w zależności od potrzeb odbiorców docelowych.

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

Peter Hustinx podczas wywiadu z dziennikarzem.

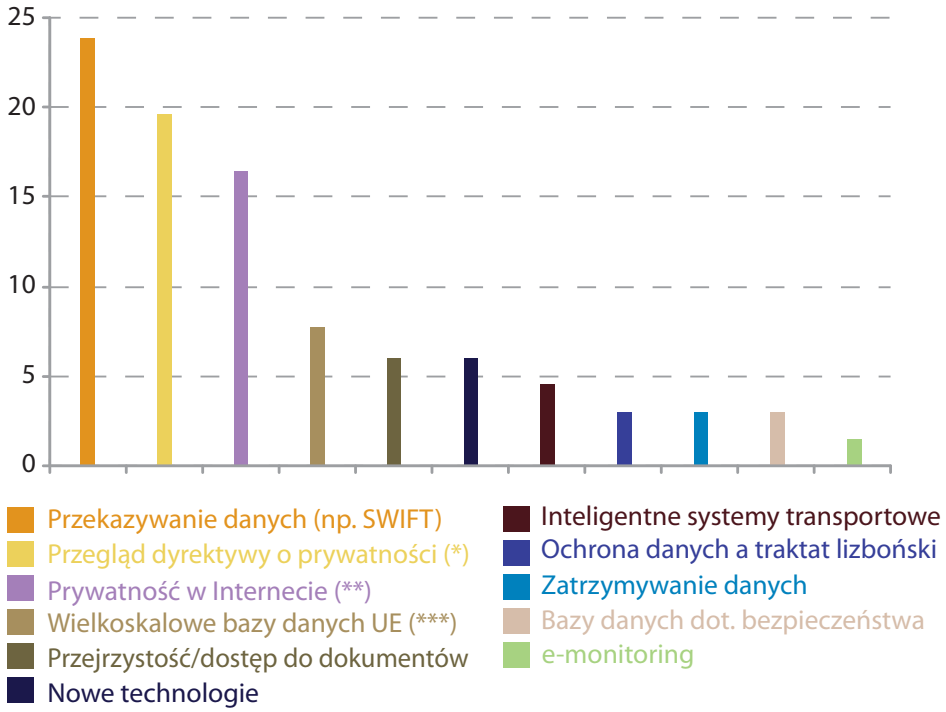
wyjaśniających tło wydarzeń oraz konferencji prasowych. Częste odpowiadanie na pytania ze strony mediów sprzyja dodatkowym regularnym kontaktom z nimi.

W 2009 r. służba prasowa wydała 14 **komunikatów prasowych.** Większość z nich odnosiła się do nowych opinii w sprawie aktów prawnych mających istotne znaczenie z punktu widzenia ogółu społeczeństwa. Dotyczyły one m.in. przeglądu dyrektywy o prywatności i łączności, publicznego dostępu do dokumentów UE, nowego programu sztokholmskiego w dziedzinie sprawiedliwości i spraw wewnętrznych, inteligentnych systemów transportowych w transporcie drogowym, dostępu organów ścigania do systemu Eurodac oraz nowej agencji do spraw wielkoskalowych systemów informatycznych.

Komunikaty prasowe publikowane są w językach angielskim i francuskim na stronie internetowej EIOD oraz w prowadzonej przez Komisję Europejską międzyinstytucjonalnej bazie komunikatów prasowych RAPID. Są one rozsyłane do regularnie aktualizowanej grupy dziennikarzy i zainteresowanych podmiotów. 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, organizacji pozarządowych, instytucji uniwersyteckich oraz przedsiębiorstw z branży informatycznej.

W 2009 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 belgijskiej. Zaowocowało to wieloma artykułami w prasie krajowej, międzynarodowej i unijnej oraz w publikacjach i na stronach internetowych specjalizujących się w zagadnieniach technologii informacyjnych, jak również wywiadami w radiu i telewizji (np. dla francusko-niemieckiej stacji telewizyjnej ARTE, radia holenderskiego oraz szwedzkiej i holenderskiej telewizji). Wywiady dotyczyły spraw ogólnych, takich jak europejskie bezpieczeństwo danych, tendencje do rozpowszechniania się nadzoru oraz obecne i nadchodzące wyzwania w dziedzinie ochrony prywatności i danych. Omawiano także kwestie bardziej szczegółowe, w tym nową umowę SWIFT między UE a USA, paszporty biometryczne i bazy odcisków palców, nowy wymóg powiadamiania o naruszeniach bezpieczeństwa danych w zmienionej dyrektywie o prywatności i łączności, a także wpływ traktatu lizbońskiego na ochronę danych.

Najważniejsze tematy pytań prasy w 2009 r.



(*) Włączając nową regulację dotyczącą naruszenia danych

(**) Włączając wyszukiwarki, nowe aplikacje online oraz portale społecznościowe

(***) Głównie Eurodac, CIS i VIS

Media regularnie zadają EIOD pytania, prosząc zwykle o komentarze, wyjaśnienia lub informacje. W 2009 r. uwaga mediów skupiała się głównie na kwestii przekazywania danych (np. debata w sprawie nowej umowy SWIFT), przeglądzie dyrektywy o prywatności i łączności (w szczególności nowy przepis dotyczący obowiązku powiadamiania o naruszeniach bezpieczeństwa), obawach związanych z prywatnością w Internecie, m.in. w kontekście wyszukiwarek, nowych aplikacji i sieci społecznościowych, oraz wielkoskalowych bazach danych UE. Istotnymi kwestiami dla prasy były też dostęp do dokumentów UE i nowe technologie (np. RFID i chmury obliczeniowe).

5.4. Wnioski o udzielenie informacji i porad

Liczba wniosków o udzielenie informacji lub pomocy otrzymanych od obywateli pozostawała w 2009 r. dość stabilna (174 wnioski w porównaniu do 180 w 2008 r.). Wnioski te pochodzą od wielu różnych osób i podmiotów – zainteresowanych stron funkcjonujących w ramach UE lub aktywnych w dziedzinie ochrony 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 ochrony prywatności lub potrzebujących pomocy w związku z napotkanymi problemami z tej dziedziny. Wnioski takie są przesyłane głównie na ogólny adres poczty elektronicznej EIOD.

Pierwsza kategoria wniosków otrzymanych w 2009 r. dotyczy skarg od obywateli UE, których EIOD nie jest władny rozpatrywać. Skargi te odnosiły się w większości do domniemanych naruszeń ochrony danych przez krajowe przedsiębiorstwa lub władze publiczne, strony internetowe niezarządzane przez UE lub internetowe sieci społecznościowe. Inne dotyczyły domniemanego naruszenia prywatności podczas krajowych postępowań sądowych oraz odwołań od orzeczeń krajowych organów 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 organu, którym jest zazwyczaj krajowy organ ochrony danych właściwego państwa członkowskiego.

Najważniejsze tematy publicznych wniosków o informacje w 2009

Druga kategoria wniosków otrzymanych w 2009 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 odpowiednim organem ds. ochrony danych oraz w stosownych przypadkach – z jednostką ds. 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 prawodawstwa UE w zakresie ochrony danych, działalności EIOD, transgranicznych przepływów danych, zawartych w traktacie lizbońskim nowych przepisów o ochronie danych oraz obaw związanych z ochroną danych w kontekście wykorzystania skanerów ciała na lotniskach.

5.5. Wizyty studyjne

W ramach wysiłków zmierzających do 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. Na przykład w październiku 2009 r. biuro EIOD odwiedziła grupa europejskich i pochodzących spoza Europy studentów prawa z francuskiego Uniwersytetu Grenoble; podczas wizyty przedstawiono rolę i działalność biura oraz omawiano zagadnienia ochrony danych w związku z walką z terroryzmem. Wśród innych grup należy wymienić austriackich słuchaczy studiów MBA w dziedzinie zarządzania instytucjami publicznymi i studentów z uniwersytetu w Tilburgu w Holandii.

W celu dotarcia do młodszych odbiorców urząd EIOD zaprosił również grupę uczniów szkół średnich z Austrii, z którymi pracownicy omawiali szczególnie interesujące ich kwestie ochrony danych, np. związane z sieciami społecznościowymi oraz ochroną osób niepełnoletnich w Internecie.

5.6. Internetowe narzędzia informacyjne

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 trakcie działalności EIOD (opinie dotyczące kontroli wstępnych i wnioski odnoszące się do prawodawstwa UE, priorytety robocze, publikacje, przemówienia i głosy w dyskusji wyrażane w formie pisemnej, komunikaty prasowe, biuletyny oraz informacje na temat wydarzeń itp.).

Zawartość strony

W 2009 r., oprócz aktualizacji związanej z powołaniem Inspektora i jego zastępcy na drugą kadencję EIOD, udostępniono nowe narzędzia informacyjne, aby wyjść naprzeciw oczekiwaniom odwiedzających i podwyższyć poziom wiedzy o działalności instytucji. Opublikowano m.in. słowniczek terminów związanych z ochroną danych osobowych oraz sekcję poświęconą pytaniom i odpowiedziom.

Przeprowadzono też gruntowną aktualizację wszystkich stron witryny przed wprowadzeniem w 2010 r. wersji niemieckojęzycznej oprócz istniejących: angielskiej i francuskiej. Trwa również rozbudowa sekcji często zadawanych pytań, gdzie znajdą się ukierunkowane odpowiedzi przeznaczone dla różnych odbiorców (np. pracowników instytucji UE, odwiedzających, kandydatów do pracy w instytucjach i organach wspólnotowych).

Planowane są dalsze usprawnienia strony internetowej, które będą obejmować udostępnienie internetowego formularza skarg, uruchomienie rejestru powiadomień oraz zmiany na stronie głównej w celu lepszego wyeksponowania najnowszych informacji na temat działalności EIOD.

Zmiany techniczne oraz ruch

W ramach trwających wysiłków na rzecz 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 2009 r. łącznie 92 884 użytkowników, w tym ponad 8000 miesięcznie w styczniu, marcu, kwietniu, październiku i listopadzie. Po stronie głównej najczęściej odwiedzano strony dotyczące kontaktu, nadzoru i konsultacji, chociaż popularne były też aktualności, publikacje i wydarzenia. Statystyki pokazują, 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.

Biuletyn

Biuletyn EIOD pozostaje skutecznym narzędziem służącym informowaniu o bieżących działaniach Inspektora oraz zwróceniu uwagi na nowości na stronie internetowej. Dostarcza on wiadomości na temat najnowszych opinii EIOD dotyczących wniosków prawodawczych UE i kontroli wstępnych. Zawiera też informacje o nadchodzących konferencjach i innych wydarzeniach w terenie oraz o ostatnich wystąpieniach Inspektora i jego zastępcy. Biuletyny dostępne są na stronie internetowej EIOD, gdzie można również zamówić ich subskrypcję.

W 2009 r. opublikowano pięć wydań biuletynu EIOD; ukazywały się one średnio co dwa miesiące. Biuletyn wydawany jest w języku angielskim i francuskim; na 2010 r. planowana jest też wersja niemieckojęzyczna.

Liczba subskrybentów wzrosła z 880 pod koniec 2008 r. do ok. 1200 pod koniec 2009 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.

Wyraźny, systematyczny wzrost liczby subskrybentów sprawił, że konieczne stało się ulepszenie publikacji i uczynienie jej przystępniejszą przez nadanie jej wyglądu, który byłby bardziej przyjazny dla odbiorcy. Pierwsze wydanie nowej wersji biuletynu opublikowano w październiku 2009 r.

5.7. Publikacje

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. 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 podmioty danych, 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.

Inspektor i zastępca przedstawili streszczenie sprawozdania rocznego EIOD za rok 2008 Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego w dniu 16 kwietnia 2009 r.

Broszura informacyjna

W kontekście drugiej kadencji EIOD (2009–2014) w 2009 r. została opracowana nowa broszura informacyjna. Broszura ta, skierowana do ogółu społeczeństwa, zawiera informacje na temat kompetencji i obowiązków EIOD, praw podmiotów danych, roli inspektorów ochrony danych oraz procedury składania skargi do EIOD. Zawiera także wytyczne i krótkie wyjaśnienia dotyczące najważniejszych aspektów roli EIOD oraz ochrony danych osobowych w administracji UE.

W 2010 r. zostaną opracowane zestawienia tematyczne dotyczące konkretnych zagadnień w dziedzinie ochrony danych w celu dostarczenia ukierunkowanych informacji zarówno ogółowi społeczeństwa, jak i zainteresowanym stronom.

5.8. Wydarzenia zwiększające świadomość

Uczestnictwo w imprezach promocyjnych stanowi dla EIOD doskonałą sposobność do krzewienia wiedzy na temat praw przysługujących podmiotom danych oraz obowiązków instytucji i organów Wspólnoty w zakresie prywatności i ochrony danych.

Dzień Ochrony Danych

Państwa członkowskie Rady Europy oraz instytucje i organy europejskie obchodziły 28 stycznia 2009 r. trzeci Europejski Dzień Ochrony Danych. Data ta upamiętnia rocznicę uchwalenia Konwencji Rady

Stoisko EIOD w siedzibie Komisji Europejskiej podczas Dnia Ochrony Danyc.

Europy o ochronie danych osobowych (Konwencji nr 108) – pierwszego wiążącego prawnie instrumentu międzynarodowego dotyczącego ochrony danych, który przyjęto w 1981 r.

EIOD skorzystał 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 Parlamencie Europejskim, Komisji Europejskiej oraz w siedzibie Rady funkcjonowało z tej okazji przez trzy kolejne dni stoisko informacyjne. EIOD przedstawiał swoją rolę nadzorczą, konsultacyjną i związaną ze współpracą, jak też osiągnięcia i bieżącą działalność swojego urzędu. Stoisko EIOD zorganizowano we współpracy z inspektorami ochrony danych odpowiednich instytucji, którzy również przedstawili swoje działania. Dystrybuowano różne publikacje przedstawiające rolę EIOD i jego pracę, a odwiedzający mieli okazję sprawdzić swoją wiedzę na temat ochrony danych w krótkim quizie.

Podczas następnego Dnia Ochrony Danych celem będzie dalszy rozwój tej działalności, w szczególności przez wykorzystanie materiałów wideo, a także dywersyfikacja działań w tym zakresie, tak aby skuteczniej dotrzeć do personelu UE i innych zainteresowanych stron.

Dzień Otwarty UE

W dniu 9 maja 2009 r. biuro EIOD uczestniczyło, jak co roku, w zorganizowanym w Parlamencie Europejskim w Brukseli Dniu Otwartym instytucji Unii Europejskiej.

Stoisko EIOD działało w głównym gmachu Parlamentu Europejskiego, a pracownicy biura odpowiadali 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.

6

ADMINISTRACJA, BUDŻET I PERSONEL

6.1. Wprowadzenie

Pierwsza kadencja Inspektora i jego zastępcy zakończyła się w styczniu 2009 r. Po wyborach, które odbyły się w 2008 r., Rada i Parlament Europejski powołały na pięcioletnią kadencję nowy zespół.

Aby stworzyć rezerwę wysoko wyspecjalizowanych pracowników, EIOD ogłosił ogólny konkurs w zakresie ochrony danych organizowany przez Europejski Urząd Doboru Kadr (EPSO). Lista rezerwowa zostanie podana do wiadomości latem 2010 r.

Administracja instytucji jest stopniowo rozbudowywana zgodnie z ustalanymi corocznie priorytetami, z uwzględnieniem jej potrzeb i wielkości.

EIOD przyjął nowe przepisy wewnętrzne niezbędne do prawidłowego funkcjonowania instytucji.

Usprawniono dodatkowo współpracę z innymi instytucjami – Parlamentem Europejskim, Radą i Komisją Europejską, co pozwoliło osiągnąć znaczne korzyści skali.

6.2. Budżet

Budżet na 2009 r. przyjęty przez władzę budżetową wyniósł 6 663 026 euro. Oznacza to wzrost w porównaniu z 2008 r., głównie z racji dodatkowych stanowisk, zmiany na stanowisku Inspektora i jego następcy oraz zwiększenia powierzchni biurowej niezbędnego w związku z rozwojem instytucji.

Oprócz wynagrodzeń i wydatków związanych z budynkami znaczna część budżetu przeznaczana jest na tłumaczenia. Opinie EIOD na temat wniosków prawodawczych są tłumaczone na 23 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.

W swoim sprawozdaniu dotyczącym roku budżetowego 2008 Europejski Trybunał Obrachunkowy stwierdził, że audyt nie skutkował żadnymi uwagami.

Komisja Europejska nadal udzielała EIOD wsparcia, zwłaszcza w zakresie rachunkowości, księgowy Komisji pełni bowiem także rolę księgowego EIOD. EIOD stosuje w zakresie wykonania budżetu wewnętrzny regulamin Komisji. Jego zasady mają zastosowanie do instytucji, w których nie ustalono szczegółowego regulaminu.

6.3. Zasoby ludzkie

Jeśli chodzi o zadania w zakresie zarządzania personelem, EIOD korzysta ze skutecznej pomocy służb Komisji Europejskiej.

6.3.1. Rekrutacja

Rosnąca widoczność instytucji oznacza większe obciążenie pracą, a także poszerzenie zakresu zadań. Na kwestię znacznego wzrostu obciążenia

pracą w 2009 r. zwrócono uwagę w poprzednich rozdziałach. W tym kontekście istotne znaczenie mają zasoby ludzkie. EIOD postanowił ograniczyć tempo rozrastania się instytucji, decydując się na wzrost kontrolowany, tak aby nowi pracownicy zostali w pełni przeszkoleni oraz by mogli zintegrować się z resztą zespołu.

EIOD korzysta z usług świadczonych przez Europejski Urząd Doboru Kadr (EPSO) i uczestniczy w pracach jego zarządu, obecnie w charakterze obserwatora. We współpracy z EPSO EIOD ogłosił ogólny konkurs w zakresie ochrony danych w celu pozyskania wysoko wyspecjalizowanych pracowników. Lista rezerwowa zostanie podana do wiadomości latem 2010 r.

Jeżeli chodzi o oprogramowanie służące do zarządzania zasobami ludzkimi (głównie w związku z wyjazdami służbowymi, urlopami i szkoleniami), Komisja zawiesiła wdrażany uprzednio projekt rozwoju takiej aplikacji i opracowała system SYSPER2, który zostanie udostępniony na potrzeby EIOD przed końcem 2010 r.

6.3.2. Program stażowy

Realizacja programu stażowego rozpoczęła się w 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 dwoje stażystów.

Oprócz programu zasadniczego opracowano też specjalne warunki umożliwiające przyjmowanie studentów i doktorantów na krótkoterminowe staże bezpłatne. Ta część programu oferuje studentom możliwość prowadzenia badań związanych z tematyką pisanych prac. Program ten jest realizowany zgodnie z procesem bolońskim i wiąże się z obowiązkiem odbycia przez wspomnianych studentów stażu w trakcie nauki. Uczestnictwo w takim stażu jest możliwe tylko w wyjątkowych przypadkach i po spełnieniu rygorystycznych kryteriów przyjęcia.

Wszyscy stażyści, zarówno odbywający staże płatne, jak i bezpłatne, wnieśli wkład w zadania teoretyczne oraz praktyczne urzędu, zdobywając zarazem cenne doświadczenie.

Na podstawie podpisanych w 2005 i 2008 r. umów o gwarantowanym poziomie usług EIOD korzysta z pomocy administracyjnej biura ds. staży Dyrekcji Generalnej ds. Edukacji i Kultury Komisji Europejskiej, które 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 organów ochrony danych z różnych państw 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 ekspertom krajowym zapoznanie się z problematyką ochrony danych w UE.

Aby pozyskać ekspertów krajowych, EIOD kontaktuje się bezpośrednio z krajowymi organami ochrony danych. Stałe przedstawicielstwa państw członkowskich są również informowane o programie i proszone o pomoc w wyszukaniu właściwych kandydatów.

6.3.4. Struktura organizacyjna

Struktura organizacyjna EIOD nie uległa zmianie od 2004 r.: jedna sekcja – licząca obecnie 8 osób – jest odpowiedzialna za administrację, personel i budżet; pozostali pracownicy, w tym niewielki zespół koordynatorów odpowiedzialnych za stronę operacyjną, zajmują się dwiema głównymi dziedzinami – nadzorem oraz konsultacjami. Niewielki zespół ds. informacji jest kierowany przez rzecznika prasowego. Wszyscy pracownicy podlegają bezpośrednio Inspektorowi, jego zastępcy oraz dyrektorowi sekretariatu.

To ostatnie stanowisko utworzono pod koniec 2009 r., czyniąc tym samym pierwszy krok w kierunku restrukturyzacji organizacji planowanej na 2010 r.

6.3.5. Szkolenia

Celem wewnętrznej polityki szkoleń pozostawały w 2009 r. poszerzanie i poprawa wiedzy oraz kompetencji pracowników, co pozwoli im skuteczniej wnosić wkład w realizację celów instytucji.

Pracownicy EIOD mają dostęp do szkoleń organizowanych na szczeblu międzyinstytucjonalnym. Ponadto niektórzy pracownicy uczestniczyli w profesjonalnych szkoleniach zewnętrznych, aby doskonalić swoją wiedzę w dziedzinie ochrony danych.

Plan szkoleń na 2009 r., obejmujący potrzeby pracowników zidentyfikowane na podstawie ankiety, odnosił się do najważniejszych obszarów kształcenia określonych w ogólnych wytycznych załączonych do decyzji wewnętrznej dotyczącej szkoleń.

Istotną część całkowitej liczby dni przeznaczonej na szkolenia w 2009 r. stanowiły kursy językowe. Duża frekwencja potwierdza zasadę, że nauka języków w EIOD powinna służyć przede wszystkim poprawie skuteczności wykonywania zadań oraz potrzebom związanym z pracą zawodową, w tym oczywiście – harmonijnej integracji nowych pracowników.

EIOD uczestniczył w dalszym ciągu w pracach międzyinstytucjonalnych komitetów: międzyinstytucjonalnej grupy roboczej Europejskiej Szkoły Administracji, międzyinstytucjonalnej grupy ds. oceny szkoleń Europejskiej Szkoły Administracji, międzyinstytucjonalnego komitetu ds. szkoleń językowych itp. Celem było wypracowanie wspólnego podejścia w sektorze, gdzie potrzeby są zasadniczo podobne w różnych instytucjach i możliwe jest osiągnięcie korzyści skali.

W 2009 r. 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.

Podpisano również z EAS umowy o poziomie usług, co umożliwia pracownikom EIOD wytypowanym do uzyskania certyfikatów wzięcie udziału w obowiązkowych szkoleniach na potrzeby procedury certyfikacji.

6.3.6. Działania socjalne

Inspektor i jego zastępca osobiście witają nowych pracowników. Pracownicy ci spotykają się ze swoim mentorem, a także z członkami działu administracyjnego, którzy udzielają im informacji na temat specyficznych procedur instytucji oraz przekazują przewodnik administracyjny EIOD. Inspektor podpisał z Komisją umowę o współpracy w celu ułatwienia integracji nowych współpracowników, 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.

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; rozpoczęto też analizę kwestii dobrego samopoczucia w pracy.

Dialog społeczny w ramach biura EIOD musiał niestety zostać tymczasowo wstrzymany z powodu rezygnacji Komitetu Pracowniczego i nieukonstytuowania się nowego. Organizowano jednak działania socjalne poza biurem.

EIOD w dalszym ciągu rozwijał współpracę międzyinstytucjonalną w zakresie opieki nad dziećmi: dzieci pracowników EIOD mogą korzystać ze żłobków, opieki pozaszkolnej oraz rekreacyjnych ośrodków opieki dziennej Komisji, jak również ze szkół europejskich.

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.

W 2009 r. kontynuowano ocenę ryzyka w działalności EIOD w celu zaprojektowania systemu zarządzania ryzykiem umożliwiającego identyfikację i ocenę ryzyka związanego z działalnością instytucji, a w razie potrzeby przeciwdziałanie mu.

EIOD przyjął do wiadomości roczne sprawozdanie z działalności i związane z nim poświadczenie wiarygodności podpisane przez intendenta delegowanego. Ogólnie rzecz biorąc, EIOD uważa, że funkcjonujące mechanizmy kontroli wewnętrznej

dają wystarczającą pewność co do legalności i prawidłowości działań, za które instytucja jest odpowiedzialna.

6.4.2. Audyt wewnętrzny

Audytor wewnętrzny Komisji został mianowany audytorem wewnętrznym EIOD.

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

W 2009 r. otrzymano i przyjęto sprawozdanie dotyczące działań podjętych po kontroli przeprowadzonej w grudniu 2008 r. przez Służbę Audytu Wewnętrznego. W sprawozdaniu potwierdzono zdolność mechanizmu kontroli wewnętrznej EIOD do zapewnienia wystarczającej pewności realizacji celów instytucji, chociaż wskazano również pewne aspekty wymagające poprawy. Niektóre z zaleceń już zrealizowano, pozostałe będą natomiast wdrażane stopniowo wraz z ewolucją zadań EIOD.

6.4.3. Bezpieczeństwo

Pod koniec 2008 r. EIOD przyjął decyzję w sprawie obowiązujących środków bezpieczeństwa. Decyzja ta obejmuje środki odnoszące się do zarządzania informacjami poufnymi i bezpieczeństwa systemów informatycznych, a także bezpieczeństwa i higieny pracy oraz bezpieczeństwa budynków. W 2009 r. zorganizowano sesję informacyjną w celu podniesienia poziomu wiedzy związanej z bezpieczeństwem oraz zapewnienia, aby pracownicy byli świadomi obowiązujących środków bezpieczeństwa.

6.4.4. Inspektor ochrony danych

W 2009 r. trwały prace nad wewnętrznym wdrożeniem przepisów rozporządzenia (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych i o swobodnym przepływie takich danych.

Wystosowano też kolejne powiadomienia do inspektora ochrony danych w związku ze wskazanymi w spisie EIOD operacjami przetwarzania dotyczącymi danych osobowych. W przypadkach podlegających powiadomieniu dotyczącemu kontroli wstępnej wdrożono uproszczoną procedurę uwzględniającą szczególną sytuację EIOD. Stworzono rejestr powiadomień.

Udział w spotkaniach sieci inspektorów ochrony danych pozwala inspektorowi ochrony danych EIOD uczestniczyć w wymianie doświadczeń i omawianiu wspólnych problemów.

6.5. Infrastruktura

Zgodnie z porozumieniem o współpracy administracyjnej siedziba EIOD znajduje się w budynku Parlamentu Europejskiego, który wspiera ponadto EIOD w zakresie technologii informatycznych i infrastruktury.

EIOD 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 EIOD korzysta ze współpracy międzyinstytucjonalnej w zakresie wielu zagadnień dotyczących administracji. Współpraca ta jest dla EIOD bardzo wartościowa ze względu na zwiększenie wydajności i uzyskiwane korzyści skali. Pozwala również uniknąć dublowania infrastruktury administracyjnej oraz ograniczyć bezcelowe wydatki administracyjne, a jednocześnie zapewnia zarządzanie usługami publicznymi na wysokim poziomie.

Na tej podstawie w 2009 r. kontynuowano współpracę międzyinstytucjonalną z różnymi dyrekcjami generalnymi Komisji (DG ds. Personelu i Administracji; DG ds. Budżetu; Służbą Audytu Wewnętrznego; DG ds. Edukacji i Kultury), Biurem Administracji i Rozliczania Należności Indywidualnych, z różnymi służbami Parlamentu Europejskiego (ds. technologii informacyjnych – w szczególności w związku z pracami nad nową wersją strony internetowej EIOD, jak również w zakresie wyposażenia pomieszczeń, ochrony budynków, druku, poczty, sprzętu telefonicznego, zaopatrzenia itd.) oraz z Radą Europejską (w zakresie tłumaczeń).

Z Biurem Administracji i Rozliczania Należności Indywidualnych podpisano umowę o poziomie

usług dotyczącą pewnych czynności, w tym ustalania, obliczania i wypłaty kwot związanych z uprawnieniami indywidualnymi obecnych oraz byłych pracowników, jak też zwrotu środków za wyjazdy służbowe, wydatków związanych z opieką zdrowotną i wydatków ekspertów.

Na podstawie pozytywnej oceny w styczniu 2010 r. umowę przedłużono o dwa lata do stycznia 2012 r. W styczniu 2010 r. zakończył się okres obowiązywania umowy z Radą Europejską dotyczącej usług tłumaczeniowych. Nową umowę podpisano z Centrum Tłumaczeń dla Organów Unii Europejskiej, które od 2010 r. przejmie zadania związane z tłumaczeniem.

Obowiązujące umowy o poziomie usług są regularnie aktualizowane. W listopadzie 2009 r. EIOD podpisał nową umowę o poziomie usług z Europejską Szkołą Administracji (EAS) w sprawie programu szkolenia pracowników w związku z procedurą certyfikacji.

Bezpośredni dostęp do niektórych aplikacji finansowych Komisji z biura EIOD ułatwiał współpracę oraz wymianę informacji między jednostkami Komisji i EIOD.

Trwająca współpraca z Parlamentem Europejskim zapewniała konserwację strony internetowej EIOD i pozwoliła rozszerzyć jej funkcjonalność.

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.

EIOD jest członkiem licznych międzyinstytucjonalnych komitetów i grup roboczych, w tym Comité de Gestion Assurances maladies (CGAM), Comité de Préparation pour les Questions Statutaires (CPQS), Comité du Statut, międzyinstytucjonalnej grupy roboczej ds. EAS, międzyinstytucjonalnej grupy ds. oceny szkoleń oraz międzyinstytucjonalnego komitetu ds. szkoleń językowych. Udział w nich pomógł zwiększyć rozpoznawalność EIOD wśród innych instytucji i zachęcał do wymiany dobrych praktyk.

6.6.2. Przepisy wewnętrzne

Trwał proces przyjmowania nowych przepisów wewnętrznych niezbędnych do prawidłowego funkcjonowania instytucji. Przyjęto też nowe ogólne przepisy wykonawcze do regulaminu pracowniczego.

W przypadku gdy przepisy te odnoszą się do obszarów, w których EIOD korzysta z pomocy Komisji, są one podobne do uregulowań Komisji, choć uwzględniają też pewne specyficzne cechy urzędu EIOD.

W pierwszym dniu pracy nowi pracownicy otrzymują przewodnik administracyjny, który zawiera wszystkie przepisy wewnętrzne EIOD i szczegóły dotyczące instytucji. Dokument ten jest regularnie uaktualniany.

Przyjęto też nowy przewodnik dotyczący wyjazdów służbowych oparty na przewodniku KE.

W 2009 r. przyjęto trzy decyzje wewnętrzne odnoszące się do okresu próbnego w przypadku urlopu rodzicielskiego lub ze względów rodzinnych, urlopu dla kobiet karmiących piersią i urlopu w przypadku ciężkiej choroby dziecka.

EIOD jest stosunkowo młodą instytucją i rozwija się szybko. W związku z tym przepisy i procedury odpowiednie w pierwszych latach działalności mogą okazać się mniej przydatne w przyszłości, w warunkach bardziej rozbudowanej i złożonej struktury. Dlatego też obowiązujące zasady zostaną poddanie ocenie po dwóch latach od ich przyjęcia i mogą ulec zmianie.

6.6.3. Zarządzanie dokumentami

Przy wsparciu służb Parlamentu Europejskiego w styczniu 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.

7

GŁÓWNE CELE 2010

W 2009 r. podjęto pierwsze kroki na rzecz dokonania strategicznej oceny ról i zadań EIOD w celu określenia głównych kierunków rozwoju na najbliższe cztery lata. Spowoduje to konsekwencje w różnych obszarach, zwłaszcza jednak w zakresie nadzoru i organizacji wewnętrznej. Zmiany w innych dziedzinach będą miały charakter bardziej stopniowy, zgodnie z opisem w niniejszym sprawozdaniu rocznym.

Na 2010 r. określono główne cele wymienione poniżej. Wyniki ich realizacji zostaną przedstawione w przyszłym roku.

- Wspieranie sieci inspektorów ochrony danych

EIOD będzie nadal wspierać inspektorów ochrony danych, zwłaszcza w niedawno utworzonych agencjach, zachęcając ich do wymiany wiedzy fachowej i najlepszych praktyk, w tym również w stosownych przypadkach do wdrożenia standardów zawodowych w celu zwiększenia skuteczności ich działań.

- Rola kontroli wstępnych

EIOD położy większy nacisk na wdrażanie zaleceń wydanych w opiniach dotyczących kontroli wstępnych oraz zapewni właściwe monitorowanie podjętych działań. Szczególną uwagę będzie się nadal zwracać na kontrolę wstępną operacji przetwarzania danych wspólnych dla większości agencji.

- Wytyczne horyzontalne

EIOD będzie nadal opracowywać i udostępniać wytyczne w sprawie istotnych kwestii. Zostaną opublikowane wytyczne w sprawie nadzoru wideo, dochodzeń administracyjnych i postępowań dyscyplinarnych, jak też przepisów wykonawczych dotyczących zadań i obowiązków inspektorów ochrony danych.

- Polityka kontroli

EIOD opublikuje obszerne zasady dotyczące monitorowania oraz egzekwowania przestrzegania przepisów w zakresie ochrony danych w instytucjach i organach. Będą one obejmować opis wszystkich właściwych środków określenia i zapewnienia zgodności z zasadami ochrony danych oraz metod wykształcenia odpowiedzialności instytucjonalnej za prawidłowe zarządzanie danymi.

- Zakres konsultacji

EIOD będzie nadal wydawać we właściwym terminie opinie lub uwagi dotyczące wniosków prawodawczych oraz zapewni podjęcie właściwych dalszych działań w stosownych dziedzinach. Szczególną uwagę zwróci na plan działań zmierzających do wdrożenia programu sztokholmskiego.

- Przegląd ram prawnych

EIOD przyzna priorytet wypracowaniu kompleksowych ram prawnych w zakresie ochrony danych obejmujących wszystkie dziedziny polityki UE i zapewniających skuteczną ochronę danych w praktyce; będzie też w miarę potrzeb wnosić w stosownych przypadkach wkład w debatę publiczną.

- Agenda cyfrowa

EIOD zwróci szczególną uwagę na agendę cyfrową Komisji we wszystkich dziedzinach, które mają oczywisty wpływ na ochronę danych. Wesprze przy tym zdecydowanie zasadę wbudowanej ochrony prywatności oraz jej wdrożenie w praktyce.

- Działania informacyjne

EIOD będzie nadal udoskonalać swoje internetowe narzędzia informacyjne (stronę internetową i biuletyn elektroniczny) w celu lepszego zaspokajania potrzeb odwiedzających. Zostaną też opracowane nowe publikacje tematyczne („zestawienia").

- Organizacja wewnętrzna

EIOD dokona zmian struktury organizacyjnej swojego sekretariatu w celu zapewnienia skuteczniejszej i efektywniejszej realizacji poszczególnych zadań. Najważniejsze informacje o nowej strukturze zostaną opublikowane na stronie internetowej.

- Zarządzanie zasobami

EIOD będzie kontynuować działania w zakresie zasobów finansowych i ludzkich oraz usprawniania innych procesów wewnętrznych. Szczególną uwagę zwróci na potrzebę zapewnienia dodatkowej powierzchni biurowej i stworzenia systemu obiegu spraw.

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 nadzorczy.

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 zapoczątkowano na początku lat siedemdziesiątych XX w. 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 ([22]). 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 opierała się 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 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 „dobrych rządów". Zasadniczą częścią tej ochrony jest niezależny nadzór.

Rozporządzenie (WE) nr 45/2001

Przyglądając się uważniej rozporządzeniu, należy po pierwsze odnotować, że ma ono zastosowanie do „przetwarzania danych osobowych przez instytucje i organy wspólnotowe, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu". Od chwili wejścia w życie traktatu lizbońskiego oznacza to, że instytucje i organy UE, które dotychczas były „instytucjami i organami wspólnotowymi", podlegają nadzorowi EIOD i muszą respektować jego uprawnienia. Nie jest jasne, czy zakres rozporządzenia jest szerszy i obejmuje też częściowo dawny „trzeci filar".

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

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 wrażliwych, informacje przekazywane podmiotowi danych, prawa podmiotu danych, 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.

Ciekawym aspektem tego rozporządzenia jest zobowiązanie instytucji i organów wspólnotowych 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 kilku lat. Oznacza to, że pomimo braku organu nadzoru 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. rozdz. 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 nadzoru i obejmują wysłuchiwanie i badanie skarg, prowadzenie innych dochodzeń, informowanie administratorów danych oraz podmiotów danych, 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 prawodawczych 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 nadzoru oraz organami nadzoru działającymi w obrębie dawnego „trzeciego filara". 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 nadzoru 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 – Wyciąg z 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

ARES	zaawansowany system kartotek
CCL	wspólny wykaz przechowywanej dokumentacji
CCTV	telewizja przemysłowa
CdT	Centrum Tłumaczeń dla Organów Unii Europejskiej
Cedefop	Europejskie Centrum Rozwoju Kształcenia Zawodowego
CFCA	Wspólnotowa Agencja Kontroli Rybołówstwa
CIS	system informacji celnej
KR	Komitet Regionów
CPCS	system współpracy w zakresie ochrony konsumentów
CPVO	Wspólnotowy Urząd Ochrony Odmian Roślin
CRS	komputerowy system rezerwacji
DG JLS	Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa
DG ADMIN	Dyrekcja Generalna ds. Personelu i Administracji
DG EAC	Dyrekcja Generalna ds. Edukacji i Kultury
DG EMPL	Dyrekcja Generalna ds. Zatrudnienia, Spraw Społecznych i Równości Szans
DG INFSO	Dyrekcja Generalna ds. Społeczeństwa Informacyjnego i Mediów
DIGIT	Dyrekcja Generalna ds. Informatyki
DPA	organ ochrony danych
DPC	koordynator ds. ochrony danych (wyłącznie w Komisji Europejskiej)
DPO	inspektor ochrony danych
EAS	Europejska Szkoła Administracji
WE	Wspólnoty Europejskie
ETO	Europejski Trybunał Obrachunkowy
EBC	Europejski Bank Centralny
ETS	Europejski Trybunał Sprawiedliwości
ECRIS	europejski system przekazywania informacji z rejestrów karnych
EKES	Europejski Komitet Ekonomiczno-Społeczny
EFSA	Europejski Urząd ds. Bezpieczeństwa Żywności
EBI	Europejski Bank Inwestycyjny
EMPL	Komisja Zatrudnienia i Spraw Socjalnych Parlamentu Europejskiego
ENISA	Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji
EKPC	europejska konwencja praw człowieka
EMEA	Europejska Agencja Leków
EMCDDA	Europejskie Centrum Monitorowania Narkotyków i Narkomanii
EMSA	Europejska Agencja ds. Bezpieczeństwa na Morzu
EPSO	Europejski Urząd Doboru Kadr
ETF	Europejska Fundacja Kształcenia
UE	Unia Europejska
EUMC	Europejskie Centrum Monitorowania Rasizmu i Ksenofobii
Eurofound	Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy
EWS	system wczesnego ostrzegania
FIDE	baza danych rejestru celnego dla celów identyfikacyjnych
7PR	siódmy program ramowy

FRA	Agencja Praw Podstawowych Unii Europejskiej
IAS	Służba Audytu Wewnętrznego
IGC	konferencja międzyrządowa
IMI	system wymiany informacji na rynku wewnętrznym
IMS	usługa zarządzania tożsamością
WCB	Wspólne Centrum Badawcze
JSB	wspólny organ nadzorczy
LIBE	Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego
MoU	protokół ustaleń
NSA	krajowa władza bezpieczeństwa
OECD	Organizacja Współpracy Gospodarczej i Rozwoju
OHC	Centrum Zdrowia w Miejscu Pracy
UHRW	Urząd Harmonizacji Rynku Wewnętrznego
OLAF	Europejskie Biuro ds. Zwalczania Nadużyć Finansowych
PEP	osoba zajmująca eksponowane stanowisko polityczne
PMO	Biuro Administracji i Rozliczania Należności Indywidualnych w Komisji Europejskiej
PNR	dane dotyczące przelotu pasażera
B&R	badania i rozwój
RFID	identyfikacja radiowa
SIS	system informacyjny Schengen
SOC	Centrum Usługowo-Operacyjne
s-TESTA	bezpieczne transeuropejskie usługi telematyczne między administracjami
SWIFT	Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych
TFUE	Traktat o funkcjonowaniu Unii Europejskiej
Trzeci filar	współpraca policyjna i sądowa w sprawach karnych
TIM	system zarządzania czasem
VIS	wizowy system informacyjny
WP 29	grupa robocza art. 29
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
Europejski Trybunał Obrachunkowy (ETO)	Jan KILB	Data-Protection@eca.europa.eu
Europejski Komitet Ekonomiczno-Społeczny (EKES)	Maria ARSENE	Data.Protection@eesc.europa.eu
Komitet Regionów (KR)	Petra CANDELLIER	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)	Giuseppina LAURITANO	Giuseppina.Lauritano@edps.europa.eu
Europejski Bank Centralny (EBC)	Frederik MALFRÈRE	DPO@ecb.int
Europejskie Biuro 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 (Eurofound)	Markus GRIMMEISEN	MGR@eurofound.europa.eu
Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA)	Cecile MARTEL	Cecile.Martel@emcdda.europa.eu
Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu

>>>

ORGANIZACJA	IMIĘ I NAZWISKO	E-MAIL
Europejska Agencja ds. Bezpieczeństwa na Morzu (EMSA)	Małgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.europa.eu
Europejskie Centrum Rozwoju Kształcenia Zawodowego (Cedefop)	Spyros ANTONIOU	Spyros.Antoniou@cedefop.europa.eu
Agencja Wykonawcza ds. Edukacji, Kultury i Sektora Audiowizualnego (EACEA)	Hubert MONET	eacea-data-protection@ec.europa.eu
Europejska Agencja ds. Bezpieczeństwa Zdrowia w Pracy (OSHA)	Terry TAYLOR	Taylor@osha.europa.eu
Wspólnotowa Agencja Kontroli Rybołówstwa (CFCA)	Clara FERNANDEZ/ Rieke ARNDT	cfca-dpo@cfca.europa.eu
Organ Nadzoru Europejskiego GNSS (GSA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Europejska Agencja Kolejowa (ERA)	Guido STÄRKLE	Dataprotectionofficer@era.europa.eu
Agencja Wykonawcza ds. Zdrowia i Konsumentów (EAHC)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC)	Elisabeth ROBINO	Elisabeth.Robino@ecdc.europa.eu
Europejska Agencja Środowiska (EEA)	Gordon McINNES	Gordon.McInnes@eea.europa.eu
Europejski Fundusz Inwestycyjny (EIF)	Jobst NEUSS	J.Neuss@eif.org
Europejska Agencja ds. Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych (Frontex)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
Europejska Agencja Bezpieczeństwa Lotniczego (EASA)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Agencja Wykonawcza ds. Konkurencyjności i Innowacyjności (EACI)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Agencja Wykonawcza ds. Transeuropejskiej Sieci Transportowej (TEN-T EA)	Elisa DALLE MOLLE	Elisa.Dalle-Molle@ec.europa.eu
Europejska Agencja Chemikaliów (ECHA)	Minna HEIKKILA	Minna.Heikkila@echa.europa.eu
Agencja Wykonawcza Europejskiej Rady ds. Badań Naukowych (ERCEA)	Donatella PIATTO	Donatella.Piatto@ec.europa.eu
Agencja Wykonawcza ds. Badań Naukowych (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu
Fuzja dla Energii (Europejskie Wspólne Przedsięwzięcie na rzecz Realizacji Projektu ITER i Rozwoju Energii Termojądrowej)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu

>>>

ORGANIZACJA	IMIĘ I NAZWISKO	E-MAIL
Wspólne przedsięwzięcie SESAR	Daniella PAVKOVIC	Daniella.PAVKOVIC@sesarju.eu
Wspólne przedsięwzięcie ARTEMIS	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Wspólne przedsięwzięcie „Czyste niebo”	Silvia POLIDORI	Silvia.Polidori@cleansky.eu
Inicjatywa w zakresie leków innowacyjnych (ILI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Wspólne przedsięwzięcie na rzecz ogniw paliwowych i technologii wodorowych	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu

Załącznik E – Wykaz opinii wydanych w wyniku kontroli wstępnej

Procedury oceny – EMEA

Opinia z dnia 18 grudnia 2009 r. w sprawie procedur oceny wyników Europejskiej Agencji Leków (sprawa 2007-421)

Stanowiska indywidualne – Parlament

Opinia z dnia 17 grudnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie stanowisk indywidualnych (sprawa 2009-650)

Procedura oceny – Rada

Opinia z dnia 15 grudnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury oceny urzędników Rady (sprawa 2009-042)

Wybór dyrektora EIGE – Parlament

Opinia z dnia 8 grudnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wyboru Dyrektora Europejskiego Instytutu ds. Równości Kobiet i Mężczyzn (EIGE) (sprawa 2008-785)

System zarządzania jakością danych EudraVigilance – EMEA

Opinia wyrażona w piśmie z dnia 7 grudnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu zarządzania jakością danych EudraVigilance (sprawa 2009-740)

Zarządzanie urlopami – EFSA

Opinia z dnia 1 grudnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania urlopami w EFSA (sprawa 2009-455)

Mobilność wewnętrzna – Europejski Bank Inwestycyjny

Opinia z dnia 18 listopada 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie mobilności wewnętrznej (sprawa 2009-253)

Sprawdzanie zapisów w systemie Flexitime – Rada

Opinia z dnia 12 listopada 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie sprawdzania zapisów w systemie Flexitime pod względem danych o dostępie fizycznym (sprawa 2009-477)

Postępowania administracyjne i procedury dyscyplinarne – EKES

Opinia z dnia 18 listopada 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie postępowań administracyjnych i procedur dyscyplinarnych (sprawa 2008-569)

360-stopniowa ocena inteligencji emocjonalnej w EAS – Komisja

Opinia z dnia 30 października 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie 360-stopniowej oceny inteligencji emocjonalnej w EAS (Europejskiej Szkole Administracji) (sprawa 2009-100)

Ubezpieczenia posłów – Parlament

Opinia z dnia 30 października 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie ubezpieczeń posłów (sprawa 2009-434)

„e-wyniki" – Europejski Bank Inwestycyjny

Opinia z dnia 19 października 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie e-wyników (sprawa 2008-379)

Korzystanie z list rezerwowych – Trybunał Obrachunkowy

Opinia z dnia 5 października 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie korzystania z list rezerwowych i list umiejętności w odniesieniu do naboru urzędników, pracowników tymczasowych i kontraktowych (sprawa 2008-433)

Zarządzanie Centrum Dziecka (CPE) – Komisja

Opinia z dnia 29 września 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania Centrum Dziecka (CPE) – żłobek i świetlica: system informacyjny Loustic i dokumentacja medyczna (Luksemburg) (sprawa 2009-089)

System służący zapewnieniu bezpieczeństwa – Parlament

Opinia z dnia 29 września 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu służącego zapewnieniu bezpieczeństwa (sprawa 2009-225)

Selekcja pracowników stałych i czasowych – Rada

Opinia z dnia 28 września 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie selekcji pracowników stałych i czasowych w Sekretariacie Generalnym Rady Unii Europejskiej (sprawa 2009-197)

Selekcja i nabór pracowników czasowych i kontraktowych – FRA

Opinia z dnia 24 września 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie selekcji i naboru przez FRA pracowników czasowych i kontraktowych (sprawa 2008-589)

Rada Dyscyplinarna – Komisja

Opinia z dnia 21 września 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie Rady Dyscyplinarnej (sprawa 2009-087)

Ubezpieczenie wypadkowe – Rada

Opinia z dnia 14 września 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przetwarzania danych odnoszącego się do ubezpieczenia wypadkowego (sprawa 2009-257)

Baza danych EudraVigilance – EMEA

Opinia z dnia 7 września 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie bazy danych EudraVigilance (sprawa 2008-402)

Ocena prezesa i wiceprezesa – CPVO

Opinia z dnia 28 lipca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny prezesa i wiceprezesa CPVO (sprawy 2009-355 i 2009-356)

Niepełny wymiar godzin – Komitet Regionów

Opinia z dnia 28 lipca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wniosków o pracę w niepełnym wymiarze godzin (sprawa 2009-396)

Niepełny wymiar godzin – EKES

Opinia z dnia 24 lipca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wniosków o pracę w niepełnym wymiarze godzin (sprawa 2009-322)

Nabór – Trybunał Obrachunkowy

Opinia z dnia 23 lipca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedur naboru urzędników, pracowników tymczasowych i kontraktowych (sprawa 2008-313)

Przesłuchania desygnowanych komisarzy – Parlament

Opinia z dnia 3 lipca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przesłuchań desygnowanych komisarzy (sprawa 2009-0332)

Ocena szkoleń – Europejski Bank Centralny

Opinia z dnia 1 lipca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny szkoleń (sprawa 2009-220)

Procedury zaproszenia do składania ofert – EKES

Opinia z dnia 30 czerwca 2009 r. w sprawie procedur zaproszenia do składania ofert oraz zarządzania kontraktami (sprawa 2009-323)

Zarządzanie czasem i nieobecnościami – ECDC

Opinia z dnia 22 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania czasem i nieobecnościami (sprawa 2009-072)

Selekcja kierownictwa średniego szczebla i doradców – Komisja

Opinia z dnia 17 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie selekcji kierownictwa średniego szczebla i doradców w Komisji (sprawa 2008-751)

Rekrutacja personelu kontraktowego – Komitet Regionów

Opinia z dnia 16 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rekrutacji personelu kontraktowego (sprawa 2008-696)

Rekrutacja urzędników – Komitet Regionów

Opinia z dnia 16 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rekrutacji urzędników (sprawa 2008-694)

Rekrutacja personelu czasowego – Komitet Regionów

Opinia z dnia 16 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rekrutacji personelu czasowego (sprawa 2008-695)

Dokumenty dostarczane podczas rekrutacji – Komisja

Opinia z dnia 5 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie dokumentów dostarczanych podczas rekrutacji (sprawa 2008-755)

Szczegółowe deklaracje o braku konfliktu interesów – EFSA

Opinia z dnia 5 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie postępowania z rocznymi i szczegółowymi deklaracjami o braku konfliktu interesów (sprawa 2008-737)

Administracja stażami – Komisja

Opinia z dnia 5 czerwca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie administracji stażami (sprawa 2008-485)

Bezpieczeństwo pracy w WCB – Komisja

Opinia z dnia 20 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania bezpieczeństwem pracy w Instytucie Zdrowia i Ochrony Konsumentów w Isprze Wspólnego Centrum Badawczego (sprawa 2008-541)

Hurtownia danych – Komisja

Opinia z dnia 19 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przetwarzania danych osobowych w hurtowni danych DG ENTR (sprawa 2008-487)

Zapobieganie nękaniu – Parlament

Opinia z dnia 19 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zapobiegania nękaniu (sprawa 2008-477)

Wnioski i rekrutacja stażystów – EMEA

Opinia z dnia 18 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wniosków i rekrutacji stażystów (sprawa 2008-730)

Procedura awansu – CdT

Opinia z dnia 18 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury awansu (sprawa 2009-018)

Służba Mediacji – Komisja

Opinia z dnia 18 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie Służby Mediacji Komisji Europejskiej (sprawa 2009-010)

TFlow i PROFIL – Parlament

Opinia z dnia 8 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie operacji przetwarzania TFlow i PROFIL (sprawa 2009-069)

Procedury rekrutacji personelu w niektórych agencjach wspólnotowych

Opinia z dnia 7 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedur rekrutacji personelu (sprawa 2009-287)

Ocena i sprawozdawczość na temat okresu próbnego – EFSA

Opinia z dnia 6 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny i sprawozdawczości na temat okresu próbnego (sprawa 2009-030)

Elastyczny czas pracy – Trybunał Sprawiedliwości

Opinia z dnia 6 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie elastycznego czasu pracy (sprawa 2007-437)

Coroczny dialog – ETF

Opinia z dnia 4 maja 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie corocznego dialogu w ETF (sprawa 2009-168)

Nagrywanie głosu w WCB-IE – Komisja

Opinia z dnia 29 kwietnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie nagrywania głosu w Instytucie Energii Wspólnego Centrum Badawczego (WCB-IE) (sprawa 2008-014)

Dane medyczne dzieci uczęszczających do żłobków międzyinstytucjonalnych – Komisja

Opinia z dnia 27 kwietnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania danymi medycznymi dzieci uczęszczających do międzyinstytucjonalnych żłobków i przedszkoli administrowanych przez OIB (sprawa 2009-088)

Procedury selekcyjne dotyczące oddelegowania ekspertów krajowych – FRA

Opinia z dnia 27 kwietnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedur selekcyjnych dotyczących oddelegowania ekspertów krajowych (sprawa 2008-747)

Młodsi eksperci w delegacjach – Komisja

Opinia z dnia 22 kwietnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie młodszych ekspertów w delegacjach (sprawa 2008-754)

Wcześniejsza emerytura – EKES

Opinia z dnia 1 kwietnia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie corocznych działań dotyczących wcześniejszego przejścia na emeryturę bez ograniczenia praw emerytalnych (sprawa 2008-719)

Staże strukturalne – Komisja

Opinia z dnia 30 marca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie stażów strukturalnych (sprawa 2008-760)

Uchylenie immunitetu jurysdykcyjnego oraz nietykalność pomieszczeń i archiwów Komisji – Komisja

Opinia z dnia 25 marca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie uchylenia immunitetu jurysdykcyjnego oraz nietykalności pomieszczeń i archiwów Komisji (sprawa 2008-645)

Zarządzanie informacjami przesłanymi przez OLAF – Komisja

Opinia z dnia 23 marca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania informacjami przesłanymi przez OLAF na mocy protokołu ustaleń (sprawa 2009-011)

Procedura zakończenia okresu próbnego – Komisja

Opinia z dnia 10 marca 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury zakończenia okresu próbnego (sprawa 2008-720)

Elastyczny czas pracy – ETF

Opinia z dnia 26 lutego 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury ETF – elastyczny czas pracy (sprawa 2008-697)

Grupa ds. poradnictwa dla personelu i przywracania na stanowisko – Rada

Opinia z dnia 23 lutego 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie grupy ds. poradnictwa dla personelu i przywracania na stanowisko (sprawa 2008-746)

Pracownicy czasowi – Wspólnotowy Urząd Ochrony Odmian Roślin

Opinia z dnia 20 lutego 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie angażowania i wykorzystywania pracowników czasowych (sprawa 2008-315)

Wcześniejsza emerytura – Parlament

Opinia z dnia 18 lutego 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury wcześniejszego przejścia na emeryturę bez ograniczenia praw emerytalnych (sprawa 2008-748)

ART: narzędzie uzgadniania audytu –Trybunał Obrachunkowy

Opinia z dnia 9 lutego 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie narzędzia uzgadniania audytu ART (sprawa 2008-239)

Zagrożenia dla interesów Komisji pod względem kontrwywiadu, zwalczania terroryzmu – Komisja

Opinia z dnia 26 stycznia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zagrożeń dla interesów Komisji pod względem kontrwywiadu, zwalczania terroryzmu (sprawa 2008-440)

Zdolność do pracy w trzecim języku przed pierwszym awansem – Parlament

Opinia z dnia 21 stycznia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny zdolności personelu do pracy w trzecim języku przed pierwszym awansem (sprawa 2008-690)

Sprawozdanie dotyczące okresu próbnego – Parlament

Opinia z dnia 21 stycznia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie sprawozdania dotyczącego okresu próbnego (sprawa 2008-604)

Komitet ds. Inwalidztwa – Rada

Opinia z dnia 16 stycznia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury Komitetu ds. Inwalidztwa (sprawa 2008-626)

Szkolenia SYSLOG – Komisja

Opinia z dnia 16 stycznia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania szkoleniami centralnymi i lokalnymi przy wykorzystaniu SYSLOG (sprawa 2008-481)

Zarządzanie żłobkiem – Rada

Opinia z dnia 15 stycznia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania żłobkiem Sekretariatu Generalnego Rady i opłat (sprawa 2007-441)

Wcześniejsza emerytura –Trybunał Obrachunkowy

Opinia z dnia 9 stycznia 2009 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie corocznych działań dotyczących wcześniejszego przejścia na emeryturę bez ograniczenia praw emerytalnych (sprawa 2008-552)

Załącznik F – Wykaz opinii w sprawie wniosków prawodawczych

Środki ograniczające w odniesieniu do Somalii i in.

Opinia z dnia 16 grudnia 2009 r. na temat różnych wniosków ustawodawczych nakładających określone środki ograniczające wobec Somalii, Zimbabwe, Korei Północnej oraz Gwinei

Agencja ds. wielkoskalowych systemów informatycznych

Opinia z dnia 7 grudnia 2009 r. na temat wniosku dotyczącego rozporządzenia ustanawiającego agencję ds. zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz na temat wniosku w sprawie decyzji Rady powierzającej tej agencji zadania dotyczące zarządzania operacyjnego systemami SIS II i VIS w zastosowaniu tytułu VI Traktatu UE

Zwalczanie oszustw w dziedzinie podatku od wartości dodanej

Opinia z dnia 30 października 2009 r. w sprawie wniosku dotyczącego rozporządzenia Rady w sprawie współpracy administracyjnej oraz zwalczania oszustw w dziedzinie podatku od wartości dodanej (przekształcenie)

Dostęp organów ścigania do systemu EURODAC

Opinia z dnia 7 października 2009 r. w sprawie wniosków dotyczących dostępu organów ścigania do systemu EURODAC

Środki ograniczające w odniesieniu do Al-Kaidy i talibów

Opinia z 28 lipca 2009 r. w sprawie wniosku dotyczącego rozporządzenia Rady zmieniającego rozporządzenie (WE) nr 881/2002 wprowadzające niektóre szczególne środki ograniczające skierowane przeciwko niektórym osobom i podmiotom związanym z Osamą bin Ladenem, siecią Al-Kaida i talibami, Dz.U. C 276 z 17.11.2009, s. 1

Inteligentne systemy transportowe

Opinia z dnia 22 lipca 2009 r. w sprawie komunikatu Komisji w sprawie planu działania na rzecz wdrażania inteligentnych systemów transportowych w Europie oraz towarzyszącego mu wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady ustanawiającej ramy wdrażania inteligentnych systemów transportowych w dziedzinie transportu drogowego oraz ich interfejsów z innymi rodzajami transportu

„Program sztokholmski" – przestrzeń wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli

Opinia z dnia 10 lipca 2009 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli, Dz.U. C 276 z 17.11.2009, s. 8

Nadzór nad bezpieczeństwem farmakoterapii

Opinia z dnia 22 kwietnia 2009 r. w sprawie wniosku dotyczącego rozporządzenia oraz dyrektywy w sprawie nadzoru nad bezpieczeństwem farmakoterapii, Dz.U. C 229 z 23.9.2009, s. 19

Wykorzystanie technologii informacyjnej dla potrzeb celnych

Opinia z dnia 20 kwietnia 2009 r. na temat inicjatywy Republiki Francuskiej na rzecz przyjęcia decyzji Rady w sprawie stosowania technologii informatycznych do potrzeb celnych, Dz.U. C 229 z 23.9.2009, s. 12

Zbieranie informacji statystycznych przez Europejski Bank Centralny

Opinia z dnia 8 kwietnia 2009 r. na temat zalecenia w sprawie rozporządzenia Rady zmieniającego rozporządzenie (WE) nr 2533/98 dotyczące zbierania informacji statystycznych przez Europejski Bank Centralny, Dz.U. C 192 z 15.8.2009, s. 1

Przeszczepy organów

Opinia z dnia 5 kwietnia 2009 r. na temat wniosku dotyczącego dyrektywy w sprawie norm jakości i bezpieczeństwa narządów ludzkich do przeszczepów, Dz.U. C 192 z 15.8.2009, s. 6

Wspólna polityka rybołówstwa

Opinia z dnia 4 marca 2009 r. w sprawie wniosku dotyczącego rozporządzenia Rady ustanawiającego wspólnotowy system kontroli w celu zapewnienia przestrzegania przepisów wspólnej polityki rybołówstwa, Dz.U. C 151 z 3.7.2009, s. 11

Azyl: rozporządzenie Eurodac

Opinia z dnia 18 lutego 2009 r. w sprawie wniosku na temat rozporządzenia dotyczącego ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr […/…] (ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca) [COM(2008) 825], Dz.U. C 229 z 23.9.2009, s. 6

Azyl: rozporządzenie dublińskie

Opinia z dnia 18 lutego 2009 r. w sprawie wniosku dotyczącego rozporządzenia ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca [COM(2008) 820 wersja ostateczna], Dz.U. C 229 z 23.9.2009, s. 1

Minimalne zapasy ropy naftowej i produktów naftowych

Opinia z dnia 3 lutego 2009 r. na temat wniosku dotyczącego dyrektywy Rady nakładającej na państwa członkowskie obowiązek utrzymywania minimalnych zapasów ropy naftowej lub produktów naftowych, Dz.U. C 128 z 6.6.2009, s. 42

Druga opinia w sprawie prywatności i łączności elektronicznej

Druga opinia z dnia 9 stycznia 2009 r. w sprawie przeglądu dyrektywy 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. C 128 z 6.6.2009, s. 28

Załącznik G – Wystąpienia Inspektora i jego zastępcy

Inspektor oraz jego zastępca poświęcali wiele czasu i wysiłku, by wyjaśnić swoje zadania oraz propagować wiedzę o ochronie danych w ogóle, a także o szeregu konkretnych zagadnień, występując publicznie i podejmując podobne formy aktywności w różnych instytucjach oraz państwach członkowskich w ciągu całego roku.

Inspektor często uczestniczył w posiedzeniach Komisji Parlamentu Europejskiego ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) lub w podobnych wydarzeniach. W dniu 5 marca wystąpił podczas wysłuchania dotyczącego wyzwań dla praw podstawowych w Internecie. W dniu 16 kwietnia przedstawił wraz z zastępcą główne tematy sprawozdania rocznego EIOD za rok 2008. W dniu 27 kwietnia mówił o trwających pracach nad zmianą rozporządzenia nr 1049/2001 w sprawie publicznego dostępu do dokumentów. W dniu 22 lipca przedstawił opinię EIOD na temat komunikatu Komisji w sprawie programu sztokholmskiego. W dniu 3 września wystąpił na wspólnym posiedzeniu komisji LIBE i ECON w sprawie umowy przejściowej UE–USA dotyczącej SWIFT. W dniu 29 września zastępca Inspektora wystąpił na posiedzeniu komisji LIBE w sprawie wykorzystania technologii informacyjnych do potrzeb celnych. W dniu 30 marca na posiedzeniu komisji ENVI Parlamentu Europejskiego mówił o kwestiach ochrony danych w odniesieniu do wniosku dotyczącego dyrektywy w sprawie transplantacji organów.

Inspektor uczestniczył także w innych spotkaniach z Parlamentem Europejskim. W dniu 22 stycznia wystąpił w komisji TRAN podczas wysłuchania w sprawie inteligentnych systemów transportowych. W dniu 28 stycznia wziął udział w obchodach Dnia Ochrony Danych w Parlamencie. W dniu 10 lutego przedstawił opinię EIOD na temat praw pacjenta w transgranicznej opiece zdrowotnej w Komisji ENVI. W dniu 29 września przemawiał na posiedzeniu Europejskiego Stowarzyszenia ds. Prywatności we współpracy z różnymi posłami do Parlamentu Europejskiego.

W dniu 26 stycznia Inspektor wziął udział w obchodach Dnia Ochrony Danych w Stałym Przedstawicielstwie Rzeczypospolitej Polskiej w Brukseli. W dniu 5 marca wystąpił na forum Rady o pracach nad zmianą rozporządzenia nr 1049/2001 w sprawie publicznego dostępu do dokumentów. W dniu 23 marca wypowiadał się na forum grupy roboczej Rady ds. ochrony danych o priorytetach w dziedzinie nadzoru i konsultacji. W dniu 6 lipca wygłosił przemówienie na temat potrzeby stworzenia strategii UE ds. zarządzania informacjami na pierwszym posiedzeniu grupy roboczej Rady ds. wymiany informacji podczas prezydencji szwedzkiej. W dniu 15 lipca zastępca Inspektora wystąpił na posiedzeniu grupy roboczej Rady w sprawie projektu e-sprawiedliwości oraz połączenia rejestrów niewypłacalności. W dniu 7 grudnia w Stałym Przedstawicielstwie Zjednoczonego Królestwa w Brukseli Inspektor wziął udział w wysłuchaniu przed komisją Izby Gmin na temat ochrony danych i egzekwowania prawa. W dniu 28 października zastępca Inspektora wygłosił przemówienie w parlamencie krajowym Berlina podczas obchodów 30-lecia ochrony danych i 10-lecia wolności słowa w Niemczech.

W dniu 26 marca zastępca Inspektora wystąpił na forum Europejskiego Komitetu Ekonomiczno-Społecznego podczas wysłuchania w sprawie wdrażania inteligentnych systemów transportowych w Ostrawie. W dniu 28 kwietnia Inspektor przedstawił strategiczne zagadnienia w zakresie ochrony danych na posiedzeniu RISEPTIS – Rady Doradczej Komisji ds. badań i innowacji na rzecz bezpieczeństwa, prywatności i wiarygodności w społeczeństwie informacyjnym. W dniu 12 maja przemawiał na posiedzeniu Komitetu SISVIS na temat bezpieczeństwa danych. W dniu 14 maja wygłosił przemówienie podczas konferencji Komisji poświęconej ocenie dyrektywy w sprawie zatrzymywania danych. W dniu 20 maja Inspektor i jego zastępca wystąpili podczas zorganizowanej przez Komisję konferencji poświęconej ochronie danych. W dniu 14 września zastępca Inspektora wystąpił na forum Europejskiego Komitetu Ekonomiczno-Społecznego podczas wysłuchania w sprawie sieci społecznościowych w Brukseli. W dniu 16 września zastępca Inspektora przemawiał podczas konferencji zorganizowanej przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) w Heraklionie. W dniu 30 września zastępca Inspektora wystąpił podczas warsztatów EIOD poświęconych nadzorowi wideo w instytucjach i organach Wspólnoty. W dniu 13 maja przemawiał w sprawie ochrony danych w obrębie instytucji i organów UE podczas 12. spotkania międzyagencyjnej sieci prawnej (IALN) zorganizowanego przez Urząd Harmonizacji Rynku Wewnętrznego (OHIM) w Alicante. W dniu 4 kwietnia przemawiał na międzynarodowej konferencji w sprawie wolności informacji i ochrony danych w Viareggio. W dniu

23 października Inspektor i jego zastępca wzięli udział w zorganizowanym przez EIOD we współpracy z ENISA seminarium w sprawie naruszeń bezpieczeństwa danych.

W dniu 16 stycznia Inspektor przemawiał na temat ochrony danych w kontekście systemu schengeńskiego i dublińskiego na uniwersytecie we Fryburgu (Szwajcaria). W dniu 17 stycznia przemawiał na dorocznej konferencji w sprawie komputerów, prywatności i ochrony danych w Brukseli. W dniu 27 stycznia przemawiał na konferencji w sprawie ochrony danych i egzekwowania prawa w Instytucie Clingendael w Hadze. W dniu 11 lutego omawiał wyzwania stojące obecnie przed europejską ochroną danych podczas konferencji TEPSA w Brukseli. W dniu 19 lutego wystąpił na konferencji e-Health 2009 w Pradze. W dniu 27 lutego wystąpił przed radą doradczą ds. e-administracji w Hadze. W dniu 19 marca wystąpił na konferencji PES dotyczącej Internetu w Atenach. W dniu 26 marca wystąpił podczas londyńskiej konferencji Brytyjskiego Stowarzyszenia Bankowców. W dniu 3 listopada zastępca Inspektora mówił na temat najnowszych wydarzeń w zakresie ochrony danych na szczeblu europejskim podczas warsztatów FIDE (Hiszpańskiej Fundacji ds. Badania Prawa i Przedsiębiorczości) w Madrycie. W dniu 14 grudnia wygłosił przemówienie programowe w sprawie ochrony danych i kodeksów postępowania na Uniwersytecie Florenckim, a 17 kwietnia mówił o e-monitoringu w miejscu pracy w Alma Graduate School w Bolonii.

W dniu 28 kwietnia zastępca Inspektora wygłosił przemówienie na temat prywatności i bezpieczeństwa w Centrum Studiów nad Polityką Europejską w Brukseli. W dniu 8 maja Inspektor wystąpił na konferencji dotyczącej Internetu przedmiotów w Brukseli. W dniu 18 maja przemawiał na konferencji w sprawie ochrony danych w UE w Brukseli. W dniu 21 maja wygłosił przemówienie podczas wiosennej konferencji Austriackiej Komisji Prawników w Weissenbach am Attersee. W dniu 8 czerwca przemawiał na XI konferencji w sprawie ochrony i bezpieczeństwa danych w Berlinie. W dniu 19 czerwca zastępca Inspektora wziął udział w wiedeńskiej konferencji europejskich organów sądowych dotyczącej nadzoru i ochrony praw podstawowych. W dniu 23 czerwca (prywatność i bezpieczeństwo na szczeblu światowym) i 10 września (sprawy przed Trybunałem Sprawiedliwości dotyczące ochrony danych) przemawiał podczas dwóch konferencji włoskiej Najwyższej Rady Sądowniczej (CSM), w których brali udział sędziowie i prokuratorzy.

W dniu 8 września Inspektor wygłosił przemówienie na seminarium „Przejrzystość i jasny język prawny w UE" zorganizowanym przez prezydencję szwedzką w Sztokholmie. W dniu 21 września wystąpił na konferencji dotyczącej rządów i informatyzacji w Antwerpii. W dniu 24 września odwiedził słowacki organ ochrony danych w Bratysławie. W dniu 8 października przemawiał podczas 35. rocznicy holenderskiej sekcji Międzynarodowej Komisji Prawników (NJCM) w Hadze. W dniach 8 i 9 października Inspektor oraz jego zastępca wzięli udział w warsztatach dotyczących ochrony danych w postępowaniu karnym w Strasburgu. W dniu 13 października Inspektor przemawiał na posiedzeniu Grupy Roboczej OECD ds. Bezpieczeństwa Informacji i Prywatności w Paryżu. W dniu 14 października wystąpił na konferencji dotyczącej bezpieczeństwa i prywatności w Oslo. W dniu 26 października przemawiał podczas lunchu zorganizowanego przez Towarzystwo Belgijsko-Holenderskie (BENEV) w Brukseli. W dniu 28 października przemawiał na konferencji Missing Children Europe w Brukseli.

W dniu 2 listopada Inspektor wystąpił podczas warsztatów na temat wbudowanej ochrony prywatności w Madrycie. W dniu 3 listopada zwracał się do konferencji organizacji społeczeństwa obywatelskiego w Madrycie. W dniu 12 listopada przemawiał podczas poświęconego programowi sztokholmskiemu seminarium zorganizowanego przez Fundację Roberta Schumana w Brukseli oraz podczas konferencji BEUC dotyczącej prywatności konsumentów w Brukseli. W dniu 20 listopada wygłosił przemówienie podczas ogólnokrajowej holenderskiej konferencji poświęconej prywatności w Amsterdamie. W dniu 2 grudnia mówił o kwestiach e-zdrowia podczas konferencji zorganizowanej przez Friends of Europe w Brukseli. W dniu 3 grudnia mówił na temat inteligentnych systemów transportowych podczas IX konferencji spedytorów w Brukseli.

Zarówno Inspektor, jak i jego zastępca rozwijali również relacje transatlantyckie. W dniu 12 marca Inspektor przemawiał podczas szczytu IAPP poświęconego prywatności w Waszyngtonie. W dniu 26 maja zastępca Inspektora wygłosił przemówienie podczas pierwszego europejsko-iberoamerykańskiego seminarium poświęconego ochronie danych w Cartagena de Indias w Kolumbii. W dniach 16–18 listopada Inspektor i zastępca wzięli udział w Safe Harbor Conference zorganizowanej w Waszyngtonie przez amerykański Departament Handlu.

Załącznik H – Skład sekretariatu EIOD

Monique LEENS-FERRANDO
Dyrektor sekretariatu (od listopada 2009 r.)

• Nadzór

Sophie LOUVEAUX *Administrator – radca prawny* *Koordynator ds. kontaktów z inspektorami ochrony danych i kontroli wstępnych*	Manuel GARCIA SANCHEZ *Ekspert krajowy – specjalista ds. technologii (do października 2009 r.)*
	Delphine HAROU *Asystent ds. nadzoru*
Zsuzsanna BELENYESSY *Administrator / radca prawny*	John-Pierre LAMB *Ekspert krajowy (od października 2009 r.)*
Isabelle CHATELIER *Administrator – radca prawny*	Xanthi KAPSOSIDERI *Asystent ds. nadzoru*
Eva DIMOVNÉ KERESZTES *Administrator – radca prawny* *Koordynator ds. kontroli (do października 2009 r.)*	Sylvie PICARD *Asystent ds. nadzoru*
Jarosław LOTARSKI *Administrator – radca prawny* *Koordynator ds. skarg*	Kim Thien LÊ *Asystent ds. sekretariatu*
Maria Veronica PEREZ ASINARI *Administrator – radca prawny* *Koordynator ds. środków administracyjnych*	Pierre FALLER *Stażysta (od kwietnia do lipca 2009 r.)*
Tereza STRUNCOVA *Administrator – radca prawny*	Evangelia MESAIKOU *Stażystka (od marca do lipca 2009 r.)*
Michaël VANFLETEREN *Administrator – radca prawny*	Eleni ATHERINOU *Stażystka (od października 2009 r.)*
Athena BOURKA *Ekspert krajowy – specjalista ds. technologii (do października 2009 r.)*	Mathias POCS *Stażysta (od października 2009 r.)*

• Polityka i informacja

Hielke HIJMANS *Administrator – radca prawny* *Koordynator ds. konsultacji i postępowań sądowych*	Roberto LATTANZI *Ekspert krajowy (od października 2009 r.)*
Rosa BARCELO *Administrator – radca prawny*	Martine BLONDEAU (*) *Asystent ds. dokumentacji*
Laurent BESLAY *Administrator – specjalista ds. technologii* *Koordynator ds. bezpieczeństwa i technologii*	Francisco Javier MOLEÓN GARCIA *Asystent ds. dokumentacji*
Katarzyna CUADRAT-GRZYBOWSKA *Administrator – radca prawny*	Andrea BEACH *Asystent ds. sekretariatu*
Bénédicte HAVELANGE *Administrator – radca prawny* *Koordynator ds. wielkoskalowych systemów informatycznych i polityki dotyczącej granic*	Anna-Maria VANHOYE *Asystent ds. sekretariatu* *(od października 2009 r.)*
Herke KRANENBORG *Administrator / radca prawny*	Vasiliki MYLONA *Stażystka (od marca do lipca 2009 r.)*
Anne-Christine Lacoste *Administrator – radca prawny* *Koordynator ds. grupy roboczej art. 29*	Mario Viola DE Azevedo CUNHA *Stażystka (od marca do lipca 2009 r.)*
Alfonso SCIROCCO *Administrator – radca prawny*	Maria-Grazia PORCEDDA *Stażystka (od października 2009 r.)*
Nathalie VANDELLE (*) *Administrator – rzecznik prasowy* *Koordynator zespołu ds. informacji*	

(*) Zespół ds. informacji.

• Sekcja personelu, budżetu i administracji

Monique LEENS-FERRANDO
Kierownik sekcji (do października 2009 r.)

• Zasoby ludzkie

Giuseppina LAURITANO *Administrator – kwestie regulaminowe* *Specjalista ds. audytu i ochrony danych*	Guido CAGNONI *Stażysta (od marca 2009 r. do lipca 2009 r.)*
Vittorio MASTROJENI *Asystent ds. zasobów ludzkich*	Livia HARSEU *Stażystka (od października 2009 r.)*
Anne LEVÊCQUE *Asystent ds. zasobów ludzkich*	

• Budżet i finanse

Tonny MATHIEU *Administrator ds. finansowych* *(do października 2009 r.)*	Maria SANCHEZ LOPEZ *Asystent ds. finansów i księgowości*
Raja ROY *Asystent ds. finansów i księgowości*	

• Administracja

Anne-Françoise REYNDERS *Asystent ds. działań socjalnych, infrastruktury i administracji*

EIOD i jego zastępca z personelem.

Europejski Inspektor Ochrony Danych

Sprawozdanie roczne 2009

Luksemburg: Urząd Publikacji Unii Europejskiej

2011 — 110 str. — 21 x 29,7 cm

ISBN 978-92-95073-08-1
doi:10.2804/12320

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)

EUROPEJSKY INSPEKTOR
OCHRONY DANYCH

QT-AA-10-001-PL-N

Europejski Inspektor Ochrony Danych

www.edps.europa.eu

ISBN 978-92-95073-08-1

Urząd Publikacji