

Sprawozdanie za **2008**



URZĄD PUBLIKACJI UNII
EUROPEJSKIEJ



Sprawozdanie za **2008 r.**



URZĄD PUBLIKACJI UNII
EUROPEJSKIEJ

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, 2009

ISBN 978-92-95073-17-3

doi: 10.2804/89741

© Photos: Sylvie Picart-Longrée et iStockphoto

© Wspólnoty Europejskie, 2009

Powielanie materiałów dozwolone pod warunkiem podania źródła.

WYDRUKOWANO NA PAPIERZE BIAŁYM BEZCHLOROWYM

Spis treści

Podręcznik użytkownika	7
Określenie misji	9
Przedmowa	11
1. Bilans i perspektywy	13
1.1. Ogólny przegląd 2008 roku	13
1.2. Wyniki w 2008 roku	15
1.3. Cele na 2009 rok	15
2. Nadzór	17
2.1. Wprowadzenie	17
2.2. Inspektorzy ochrony danych	17
2.3. Kontrole wstępne	19
2.3.1. Podstawa prawna	19
2.3.2. Procedura	19
2.3.3. Analiza ilościowa	21
2.3.4. Główne zagadnienia w sprawach dotyczących kontroli <i>ex-post</i>	25
2.3.5. Główne zagadnienia we właściwych kontrolach wstępnych	31
2.3.6. Konsultacje dotyczące potrzeby przeprowadzenia kontroli wstępnej	34
2.3.7. Powiadomienia niepodlegające kontroli wstępnej lub wycofane	35
2.3.8. Dalsze działania po wydaniu opinii dotyczących kontroli wstępnej	36
2.3.9. Wnioski i przyszłość	37
2.4. Skargi	37
2.4.1. Wprowadzenie	37
2.4.2. Sprawy uznane za dopuszczalne	38
2.4.3. Sprawy niedopuszczalne: główne przyczyny niedopuszczalności	42
2.4.4. Współpraca z Europejskim Rzecznikiem Praw Obywatelskich	43
2.4.5. Dalsze prace w dziedzinie skarg	44
2.5. Polityka w zakresie kontroli	44
2.5.1. Wiosna 2007 roku i okres późniejszy	44
2.5.2. Kontrole	45
2.6. Środki administracyjne	48
2.6.1. Nowy wzór zaświadczenia lekarskiego	48
2.6.2. Dostęp do dokumentów	48
2.6.3. Szczególne kategorie danych: prawo właściwe	49
2.6.4. Wniosek o kopię pełnej dokumentacji medycznej urzędnika wydany przez sąd	49
2.6.5. Zatrzymywanie danych o karach dyscyplinarnych związanych z danymi	50
2.6.6. Przepisy wykonawcze do rozporządzenia (WE) nr 45/2001	51
2.6.7. Skargi rozpatrywane przez Europejskiego Rzecznika Praw Obywatelskich	51
2.7. Nadzór wideo	51
2.7.1. Wytyczne	51
2.7.2. Kontrola wstępna	52
2.7.3. Skarga	52
2.7.4. Inne wnioski	53
2.8. Eurodac	53

3. Konsultacje	54
3.1. Wprowadzenie	54
3.2. Ramy polityki i priorytety	55
3.2.1. Realizacja polityki konsultacyjnej	55
3.2.2. Spis zamierzeń na rok 2008	56
3.2.3. Spis zamierzeń na rok 2009	57
3.3. Opinie prawne	58
3.3.1. Uwagi ogólne	58
3.3.2. Poszczególne opinie	59
3.4. Uwagi	65
3.5. Interwencje przed Trybunałem	66
3.6. Inne rodzaje działań	67
3.6.1. E prywatność	67
3.6.2. PNR	68
3.6.3. Wdrożenie SIS i polityka dotycząca granic	68
3.6.4. Konferencja na temat ochrony danych i egzekwowania prawa (Trewir)	68
3.6.5. Badania i rozwój technologiczny w UE	69
3.6.6. Połączenie <i>Google / DoubleClick</i> a kwestie ochrony danych	70
3.6.7. Udział w grupach ekspertów	71
3.6.8. Wypadki morskie	71
3.6.9. Choroby zakaźne	72
3.6.10. Wspólnotowy kodeks celny oraz numer w systemie rejestracji i identyfikacji podmiotów gospodarczych (numer EORI)	72
3.7. Nowe zjawiska	72
3.7.1. Interakcje z technologią	72
3.7.2. Nowe wydarzenia w polityce i prawodawstwie	75
4. Współpraca	77
4.1. Grupa robocza art. 29	77
4.2. Grupa Robocza Rady ds. Ochrony Danych	78
4.3. Skoordynowany nadzór nad systemem Eurodac	79
4.4. Trzeci filar	80
4.5. Konferencja europejska	81
4.6. Konferencja międzynarodowa	81
4.7. Inicjatywa londyńska	82
4.8. Organizacje międzynarodowe	83
5. Komunikacja	84
5.1. Wprowadzenie	84
5.2. Aspekty działań informacyjnych	85
5.3. Przemówienia	86
5.4. Kontakty z mediami	89
5.5. Prośby o udzielenie informacji	90
5.6. Wizyty studyjne	91
5.7. Internetowe narzędzia informacyjne	91
5.8. Publikacje	93
5.9. Przedsięwzięcia zwiększające świadomość	93
5.10. Priorytety na rok 2009	94

6. Administracja, budżet i personel	95
6.1. Wprowadzenie	95
6.2. Budżet	95
6.3. Zasoby ludzkie	96
6.3.1. Rekrutacja	96
6.3.2. Program stażowy	96
6.3.3. Program dla oddelegowanych ekspertów krajowych	97
6.3.4. Struktura organizacyjna	97
6.3.5. Dialog społeczny	97
6.3.6. Szkolenia	97
6.3.7. Działania socjalne	98
6.3.8. Protokół w sprawie przywilejów i immunitetów Wspólnot Europejskich	98
6.4 Funkcje kontrolne	98
6.4.1. Kontrola wewnętrzna	98
6.4.2. Audyt wewnętrzny	99
6.4.3. Bezpieczeństwo	99
6.4.4. Inspektor ochrony danych	99
6.5. Infrastruktura	99
6.6. Otoczenie administracyjne	99
6.6.1. Pomoc administracyjna i współpraca międzyinstytucjonalna	99
6.6.2. Przepisy wewnętrzne	100
6.6.3. Zarządzanie dokumentami	101
6.7. Cele na rok 2009	101
Załącznik A – Ramy prawne	103
Załącznik B – Wyciąg z rozporządzenia (WE) nr 45/2001	105
Załącznik C – Wykaz skrótów	107
Załącznik D – Lista inspektorów ochrony danych (DPO)	109
Załącznik E – Czas trwania kontroli wstępnej w poszczególnych sprawach i instytucjach	111
Załącznik F – Wykaz opinii wydanych w wyniku kontroli wstępnej	115
Załącznik G – Wykaz opinii w sprawie wniosków prawodawczych	123
Załącznik H – Skład sekretariatu EIOD	125
Załącznik I – Wykaz porozumień administracyjnych i decyzji	127

Podręcznik użytkownika

Bezpośrednio po tekście podręcznika użytkownika zamieszczono określenie misji i przedmowę przygotowaną przez Petera Hustinx, Europejskiego Inspektora Ochrony Danych (zwanego dalej Inspektorem).

Rozdział 1 – Bilans i perspektywy przedstawia ogólny przegląd działań Inspektora. Rozdział ten prezentuje również wyniki osiągnięte w 2008 roku i przedstawia główne cele na rok 2009.

Rozdział 2 – Nadzór obszernie opisuje działania realizowane w celu zapewnienia wykonywania przez instytucje i organy Wspólnoty obowiązków związanych z ochroną danych oraz monitorowania w tym kontekście tych instytucji i organów. Po ogólnym przeglądzie przedstawiono rolę inspektorów ochrony danych (DPO) w administracji UE. W rozdziale tym przedstawia się analizę kontroli wstępnych (zarówno w ujęciu ilościowym, jak i merytorycznym), skargi, politykę kontroli oraz porady dotyczące środków administracyjnych, którymi zajmowano się w roku 2008. Ponadto zawiera sekcję dotyczącą e-monitoringu i nadzoru wideo oraz aktualizację informacji na temat nadzoru nad systemem Eurodac.

Rozdział 3 – Konsultacje obejmuje działania Inspektora dotyczące jego funkcji doradczej, koncentrując się na opiniach wydawanych na temat wniosków prawodawczych i dokumentów pokrewnych, jak również na wpływie, jaki wywierają one w coraz liczniejszych dziedzinach. Rozdział ten zawiera także analizę tematów horyzontalnych: przedstawia się w nim pewne nowe kwestie technologiczne i podkreśla się nowe wydarzenia w dziedzinie polityki i prawodawstwa.

Rozdział 4 – Współpraca opisuje działania realizowane w ramach kluczowych forów, takich jak grupa robocza art. 29 ds. ochrony danych, w ramach wspólnych organów nadzoru „trzeciego filaru”, a także podczas europejskich oraz międzynarodowych konferencji na temat ochrony danych osobowych.

Rozdział 5 – Komunikacja przedstawia działania i osiągnięcia Inspektora w zakresie informacji i komunikacji, w tym prace serwisu prasowego oraz komunikację zewnętrzną z mediami. Stanowi również przegląd wykorzystania różnych narzędzi komunikacji, takich jak strona internetowa, biuletyny, materiały informacyjne i imprezy służące zwiększeniu świadomości.

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

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

Dostępne **jest również** streszczenie niniejszego sprawozdania; jego celem jest przedstawienie – w skróconej formie – najważniejszych wydarzeń w działalności Inspektora w 2008 roku.

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

Papierowe kopie sprawozdania rocznego, jak również jego streszczenia, można zamówić bezpłatnie w księgarni UE (www.bookshop.europa.eu) lub u Inspektora. Dane kontaktowe znajdują się na naszej stronie internetowej w dziale „Kontakt” (*Contact*).

Określenie misji

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

Inspektor jest odpowiedzialny za:

- monitorowanie i zapewnienie przestrzegania przepisów rozporządzenia (WE) nr 45/2001⁽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 wspólnotowym we wszystkich sprawach związanych z przetwarzaniem danych osobowych. Obejmuje to konsultacje w sprawie wniosków prawodawczych i monitorowanie nowych wydarzeń, które mają wpływ na ochronę danych osobowych („konsultacje”);
- współpracę z krajowymi instytucjami nadzoru oraz organami nadzoru w ramach „trzeciego filaru” UE z myślą o poprawie spójności w dziedzinie ochrony danych osobowych („współpraca”).

Zgodnie z powyższym Inspektor stawia sobie za cel prowadzenie strategicznych działań służących:

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

⁽¹⁾ Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

Przedmowa



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

Niniejsze sprawozdanie obejmuje rok 2008 jako czwarty pełny rok działalności Inspektora 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.

Sprawozdanie to zamyka również pierwszą kadencję Inspektora i daje sposobność do podsumowania rozwoju tej instytucji od czasu jej ustanowienia. Niezależna kontrola przewidziana w art. 286 Traktatu WE i potwierdzona jako ogólna zasada w art. 8 ust. 3 Karty praw podstawowych Unii Europejskiej oraz w traktacie lizbońskim stanowi niezwykle ważny warunek skutecznej ochrony danych osobowych w praktyce.

Podstawowe prawa i wolności, takie jak poszanowanie życia prywatnego i ochrona danych osobowych, mogą stać się rzeczywistością jedynie wtedy, gdy są one przestrzegane w praktyce, zarówno w systemach informacyjnych instytucji i organów wspólnotowych, jak i przy przyjmowaniu nowych przepisów i polityk wpływających na ochronę danych osobowych. Działania Inspektora stanowią przydatną inicjatywę w obydwu dziedzinach.

Niniejsze sprawozdanie dowodzi, że zarówno w dziedzinie nadzoru, jak i konsultacji osiągnięto wielkie postępy. Rozwija się przestrzeganie przepisów o ochronie danych i zasad jej dotyczących, istnieją jednak nadal poważne wyzwania. Najbardziej znaczącym z nich jest zakres, w którym działa Inspektor, w porównaniu do sytuacji początkowej, kiedy to zaczynał praktycznie od zera.

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

Pragnę także przekazać szczególne podziękowania – po pierwsze, Joaquínowi Bayo Delgado, który był doskonałym zastępcą Inspektora, charakteryzującym się wielkim zaangażowaniem, zmysłem praktycznym i umiejętnością pracy w zespole, a po drugie – naszym pracownikom. Nieprzeciętne zalety naszego personelu nadal walnie przyczyniały się do skuteczności naszych działań.

Na koniec, na tym etapie właściwe jest podziękowanie Parlamentowi Europejskiemu i Radzie za ich zaufanie wyrażające się ponownym powołaniem mnie na drugą kadencję i za powołanie Giovanniego Buttarellego na stanowisko nowego zastępcy Inspektora.

Peter Hustinx
Europejski Inspektor Ochrony Danych

1. Bilans i perspektywy

1.1. Ogólny przegląd 2008 roku

Działalność Europejskiego Inspektora Ochrony Danych (Inspektora) w roku 2008 były oparte na tej samej strategii ogólnej jak poprzednio, ale nadal rozszerzała się ona zarówno w odniesieniu do skali, jak i zakresu. Poprawiła się także możliwość zarówno skutecznego, jak i sprawnego działania Inspektora.

Ramy prawne ⁽²⁾, wewnątrz których działa Inspektor, zakładają liczne zadania i uprawnienia umożliwiające rozróżnienie między trzema głównymi funkcjami. Funkcje te nadal służą jako strategiczne platformy działań Inspektora i są odzwierciedlone w określeniu jego misji:

- funkcja „nadzorczą” polegająca na monitorowaniu i zapewnianiu poszanowania przez instytucje i organy wspólnotowe ⁽³⁾ istniejących zabezpieczeń prawnych podczas przetwarzania danych osobowych;
- funkcja „konsultacyjna” polegająca na udzielaniu instytucjom i organom wspólnotowym porad we wszystkich stosownych kwestiach, w szczególności w sprawie wniosków prawodawczych, mających wpływ na ochronę danych osobowych;
- funkcja „współpracy” z krajowymi instytucjami nadzoru oraz organami nadzoru w ramach „trzeciego filaru” UE obejmująca współpracę policyjną i sądową w sprawach karnych z myślą o poprawie spójności w dziedzinie ochrony danych osobowych.

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

⁽³⁾ Pojęcia „instytucje” i „organy” pojawiające się w rozporządzeniu (WE) 45/2001 stosowane są w całym sprawozdaniu. Obejmuje to również agencje wspólnotowe. Pełny wykaz znajduje się na stronie: http://europa.eu/agencies/community_agencies/index_en.htm

Funkcje te zostaną szerzej omówione w rozdziałach 2, 3 i 4 niniejszego sprawozdania rocznego, w których przedstawiono główne działania Inspektora i postępy osiągnięte w 2008 roku. Znaczenie informacji na temat tych działań oraz waga przekazywania tych informacji w pełni uzasadniają ich oddzielne potraktowanie w rozdziale 5 dotyczącym komunikacji. Większość tych działań opiera się na skutecznym zarządzaniu zasobami finansowymi, ludzkimi i innymi, co zostanie omówione w rozdziale 6.

Podstawowe prawo do poszanowania życia prywatnego oraz ochrona danych osobowych, przewidziane w Karcie praw podstawowych Unii Europejskiej i w traktacie lizbońskim, odnoszą się w coraz większym stopniu zarówno do osób fizycznych, jak i do instytucji, a także do społeczeństwa jako całości. W świecie, który coraz szerzej wykorzystuje technologie informacyjne i komunikacyjne, prawa te mają za zadanie umożliwienie każdemu uczestnictwa bez obaw, że informacje o jego życiu prywatnym i dane osobowe zostaną bezprawnie ujawnione. Zatem poszanowanie prywatności i ochrona danych osobowych mają także za zadanie stworzenie zaufania do zaawansowanych technologii.

Jednak nie dzieje się to samo z siebie ani wyłącznie za pomocą przepisów prawa. Wymaga to systematycznego wprowadzania w życie praktycznych zabezpieczeń prywatności, przełożenia ogólnych przepisów i zasad na konkretne ustalenia techniczne i organizacyjne umożliwiające stosowanie prawidłowych zabezpieczeń w codziennej rzeczywistości. Zakłada się przy tym także, że osoby odpowiedzialne za ten proces wprowadzania w życie i przekładania są dostatecznie świadome potrzeby czynienia tego i mogą być rozliczane z osiągnięcia wymaganych rezultatów w odpowiednim czasie.

Mając to na uwadze, Inspektor działa w celu propagowania kultury ochrony danych wewnątrz instytucji i organów, w ramach której przestrzeganie przepisów i zasad ochrony danych jest postrzegane jako oczywiste. Jako organ kontrolny Inspektor stawia sobie za cel wzbudzenie poczucia odpowiedzialności przez mierzenie postępów i ustalanie, w razie potrzeby, wartości docelowych, jednak bez niepotrzebnego narzucania rozwiązań. Inspektor pracuje także nad wprowadzeniem poszanowania zasad ochrony danych do prawodawstwa i polityki UE, gdy jest to zasadne. Jako doradca Inspektor dąży do tego, by określić przypadki, w których we wnioskach prawodawczych i nowych politykach odpowiednio uwzględniono te zasady, oraz przypadki, w których należy dokonać poprawek, by uwzględnić te wymagania. We współpracy z krajowymi organami nadzorczymi i organami w „trzecim filarze” Inspektor działa w celu poprawienia spójności w ochronie danych osobowych w UE jako całości.

Inspektor od samego początku podkreślał, że wiele polityk UE jest uzależnionych od zgodnego z prawem przetwarzania danych osobowych oraz że skuteczną ochronę danych osobowych, jako jedną z podstawowych wartości leżących u podstaw polityk UE, należy postrzegać jako warunek ich powodzenia. Inspektor będzie nadal działał w tym ogólnym duchu; z zadowoleniem stwierdza również, że takie działania spotyka się z coraz większym poparciem.

Kontrole wstępne nadal były głównym aspektem nadzoru w roku 2008, w którym wydano więcej opinii niż kiedykolwiek przedtem. Podczas gdy większość instytucji i organów czyni zadowalające postępy w rozwijaniu przestrzegania rozporządzenia (WE) nr 45/2001, nacisk nadzoru przenosi się teraz na monitorowanie realizacji zaleceń z kontroli wstępnych i na poprawianie poziomu przestrzegania przepisów w agencjach. Inspektor zakończył także pierwszą serię kontroli na miejscu w różnych instytucjach i organach, by zmierzyć poziom przestrzegania przepisów w praktyce. Nadal rosła całkowita liczba skarg, przy czym skarg dopuszczalnych było mniej niż poprzednio, ale ogólnie były one bardziej złożone. Przeprowadzono także dalsze prace w konsultacji nad środkami administracyjnymi i nad rozwinięciem doradztwa horyzontalnego. Sieć wewnętrznych inspektorów ochrony danych osiągnęła pełen zakres i jest nadal istotną podstawą skutecznej kontroli (zob. rozdział 2).

W roku 2008 Inspektor udzielił jeszcze więcej porad i przedłożył opinie dotyczące jeszcze większej liczby

wniosków legislacyjnych. Rozszerzył zakres działań na większą ilość obszarów polityki i na wszystkie etapy procedury legislacyjnej, tj. od najwcześniejszej fazy tworzenia polityki, wydając opinie o zielonych księgach czy reagując na wnioski o nieformalne konsultacje, aż po rozmowy w Parlamencie i Radzie na różnych etapach, łącznie z końcowym etapem procedury pojednawczej. Większość opinii Inspektora nadal dotyczyła kwestii związanych z przestrzenią wolności, bezpieczeństwa i sprawiedliwości, ale sporego znaczenia nabrały również inne obszary polityki, takie jak e-prywatność, publiczny dostęp do dokumentów czy transgraniczna opieka zdrowotna. Ponadto Inspektor opublikował dokument strategiczny dotyczący prac badawczych w UE oraz rozwoju technologii i brał udział w coraz większej liczbie interwencji sądowych (zob. rozdział 3).

We współpracy z krajowymi organami nadzoru nadal koncentrowano się na roli grupy roboczej art. 29, co zaowocowało przyjęciem nowego programu prac zakładającym cztery główne kierunki strategiczne i kilkoma sukcesami w pierwszym roku jej działania. Inspektor nadal kładł także nacisk na skoordynowany nadzór nad systemem Eurodac jako takim, a także w kontekście oczekiwanych w niedalekiej przyszłości podobnych systemów informacyjnych na wielką skalę. W związku ze sprawami z zakresu „trzeciego filaru” potrzeba ścisłej współpracy stała się bardzo wyraźna. Na koniec, nadal uwagę przyciągała współpraca na innych forach międzynarodowych, w tym w ramach „inicjatywy londyńskiej” dotyczącej podnoszenia świadomości ochrony danych i czynienia jej bardziej skuteczną (zob. rozdział 4).

Informacja i komunikacja nie tylko stanowią istotne sposoby podnoszenia świadomości, lecz są także podstawowymi warunkami skuteczności Inspektora w dziedzinie nadzoru, konsultacji i współpracy. Dlatego też w ciągu roku poświęcono wiele uwagi poprawie dotychczasowych usług, co zaowocowało dobrymi postępami, zwłaszcza w odniesieniu do strony internetowej Inspektora, w kategoriach treści i dostępności a dalsze ulepszenia są przewidziane (zob. rozdział 5).

Zarządzanie zasobami ludzkimi, finansowymi i innymi w gestii Inspektora zmieniło się znacznie od czasu tworzenia nowej instytucji w pierwszych latach działania, przez konsolidację i zwiększenie skali działalności, do sytuacji, w której stopniowe ulepszenia przyniosły stabilność i większą sprawność oraz skuteczność w różnych obszarach (zob. rozdział 6).

1.2. Wyniki w 2008 roku

W sprawozdaniu rocznym z 2007 roku wspomniano, że na 2008 rok wybrano następujące cele główne. Większość z tych celów została w pełni lub częściowo zrealizowana.

• **Wspieranie sieci DPO**

Inspektor nadal silnie wspierał inspektorów ochrony danych i zachęcał ich do dalszej wymiany wiedzy fachowej i najlepszych wzorców. Szczególną uwagę poświęcono inspektorom w niedawno utworzonych agencjach, m.in. na specjalnym posiedzeniu zwołanym w celu omówienia kwestii dotyczących nowych agencji i poinformowania inspektorów o ostatnich wydarzeniach.

• **Rola kontroli wstępnych**

Wydano rekordową liczbę opinii dotyczących kontroli wstępnej, choć w odniesieniu do większości instytucji i organów prace związane z zamknięciem kontroli wstępnej prowadzonych operacji przetwarzania danych nie są jeszcze zakończone. Większy nacisk położono na realizację zaleceń. Wyniki kontroli wstępnych i dalsze działania powierzono inspektorom i innym właściwym stronom.

• **Wytyczne horyzontalne**

Opracowano – początkowo z myślą o ułatwieniu kontroli wstępnych w agencjach – wytyczne w sprawie istotnych kwestii wspólnych dla większości instytucji i organów (np. rekrutacja personelu, przetwarzanie danych dotyczących zdrowia). Wytyczne te zostaną wkrótce udostępnione wszystkim zainteresowanym stronom. W grudniu 2008 roku zorganizowano seminarium poświęcone przekazywaniu informacji o najnowszych wydarzeniach w dziedzinie nadzoru innym zainteresowanym stronom w UE.

• **Ocena zgodności**

Inspektor nadal sprawdzał postępy w przestrzeganiu przepisów rozporządzenia (WE) nr 45/2001 przez wszystkie instytucje i organy; sprawozdanie na ten temat zostanie przedstawione do połowy 2009 roku. Oprócz tego ogólnego przeglądu Inspektor przeprowadził pierwszą serię kontroli w różnych instytucjach i organach, aby sprawdzić przestrzeganie przepisów dotyczących konkretnych obszarów. Na stronie internetowej Inspektora opublikowane zostaną niedługo założenia ogólnej polityki kontroli.

• **Systemy na dużą skalę**

Inspektor w dalszym ciągu pracuje wraz z krajowymi organami nadzoru nad skoordynowanym nadzorem systemu Eurodac i wdrożeniem programu prac

przyjętego w tym celu. Wynik tych działań zostanie udostępniony w ciągu roku 2009. Inspektor poczynił również pierwsze kroki w kwestii innych obszernych systemów, takich jak SIS II i VIS.

• **Opinie na temat prawodawstwa**

Inspektor wydał rekordową liczbę opinii lub uwag do wniosków dotyczących nowych aktów prawnych lub powiązanych dokumentów odnoszących się do dziedzin bardziej różnorodnych niż kiedykolwiek wcześniej i zapewnił stosowny wkład we wszystkie etapy procedury legislacyjnej. Spis priorytetów śledzono przez cały rok i aktualizowano w miarę potrzeby.

• **Traktat lizboński**

Szczegółowej analizie poddano wpływ traktatu lizbońskiego na dziedzinę ochrony danych osobowych, ale wejście tego traktatu w życie zależy od ostatecznej jego ratyfikacji przez kilka państw członkowskich. Analiza ta wskazała, że traktat ma – ze względów instytucyjnych i merytorycznych – wielki potencjalny wpływ, a jego wejście w życie stworzyłoby duże możliwości poprawy ochrony danych.

• **Informacje dostępne na stronie internetowej**

Informacje dostępne na stronie internetowej Inspektora zostały ulepszone, zarówno dzięki uaktualnieniu i rozwinięciu jej zawartości, jak i poprawie jej dostępności. Dalsze ulepszenia są spodziewane w ciągu 2009 roku; jednym z nich będzie elektroniczny biuletyn.

• **Regulamin wewnętrzny**

Dokonano znacznych postępów w przygotowywaniu regulaminu wewnętrznego obejmującego poszczególne funkcje i działania Inspektora; w toku są również prace nad wewnętrznymi podręcznikami proceduralnymi opisującymi najważniejsze czynności. Wyniki tych prac wraz praktycznymi narzędziami dla zainteresowanych stron zostaną zamieszczone na stronie internetowej Inspektora w 2009 roku.

• **Zarządzanie zasobami**

Zarządzanie zasobami finansowymi i ludzkimi zostało skonsolidowane lub było przedmiotem dalszych prac, a inne wewnętrzne procedury zostały udoskonalone. Poprawione zostały również funkcjonalność i skuteczność kontroli wewnętrznej.

1.3. Cele na 2009 rok

W latach poprzednich ta część sprawozdania rocznego była także wykorzystywana do przedstawienia ogólnego zarysu planów na przyszłość. Tym razem można oczekiwać zarówno kontynuacji, jak i zmian.

Pierwszy rok nowej kadencji Inspektora przy częściowej zmianie składu instytucji to właściwy moment, by podsumować potrzeby ewentualnych korekt. W roku tym dokonana zostanie zatem strategiczna ocena kompetencji i zadań Inspektora oraz wyznaczone zostaną główne ścieżki rozwoju na następne cztery lata. Refleksja ta zbiegnie się z innymi nowymi elementami w zewnętrznym środowisku Inspektora, takimi jak wyzwania związane z nową kadencją Parlamentu Europejskiego, powołaniem nowej Komisji Europejskiej, możliwym wejściem w życie traktatu lizbońskiego, innymi nowymi długoterminowymi strategiami politycznymi i ramami prawnymi oraz z łącznym wpływem powyższych czynników na ochronę danych. Inspektor zamierza w tym zakresie zająć wyraźne stanowisko i w następnym sprawozdaniu rocznym poinformuje o wnioskach wyciągniętych w tej nowej sytuacji.

Na rok 2009 wybrano następujące główne cele, nie przesądzając wyniku wspomnianej strategicznej refleksji. Wyniki osiągnięte w trakcie ich realizacji także zostaną również przedstawione w sprawozdaniu w przyszłym roku.

- **Wsparcie sieci DPO**

Inspektor nadal będzie silnie wspierał inspektorów ochrony danych, zwłaszcza działających w niedawno utworzonych agencjach, i zachęcał ich do dalszej wymiany wiedzy fachowej i najlepszych wzorców w celu poprawy skuteczności ich działań.

- **Rola kontroli wstępnych**

Inspektor zamierza zakończyć kontrole wstępne operacji przetwarzania danych przeprowadzanych w większości instytucji i organów oraz kłaść coraz większy nacisk na realizację zaleceń. Szczególna uwaga zostanie poświęcona kontrolom wstępnym wspólnych dla większości agencji operacji przetwarzania danych.

- **Wytyczne horyzontalne**

Inspektor będzie nadal opracowywał wytyczne związane z ważnymi kwestiami dotyczącymi większości instytucji i organów i będzie je powszechnie udostępniał. Opublikowane zostaną wytyczne na temat nadzoru wideo, co pozwoli również na skupienie uwagi na sytuacjach, które wiążą się z konkretnymi zagrożeniami.

- **Rozpatrywanie skarg**

Inspektor opublikuje również ramy polityczne dotyczące rozpatrywania skarg, aby poinformować wszystkie zaangażowane strony o stosownych procedurach, w tym o kryteriach pozwalających

zdecydować o ewentualnej potrzebie wszczęcia dochodzenia w związku ze złożonymi do niego skargami.

- **Polityka kontroli**

Inspektor będzie kontynuował mierzenie postępów w wykonywaniu rozporządzenia (WE) nr 45/2001, któremu będą towarzyszyć różnego rodzaju kontrole we wszystkich instytucjach i organach; coraz częściej będą przeprowadzane kontrole na miejscu. Zostaną opublikowane wytyczne polityki kontroli dotyczące poszczególnych procedur.

- **Zakres konsultacji**

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

- **Program sztokholmski**

Inspektor zamierza poświęcić szczególną uwagę przygotowaniu nowego pięcioletniego programu politycznego dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który ma zostać przyjęty przez Radę Europejską pod koniec 2009 roku. Jako jeden z głównych warunków zostanie uwypuklona potrzeba skutecznych zabezpieczeń służących ochronie danych.

- **Działania informacyjne**

Inspektor będzie w dalszym ciągu podnosił jakość i skuteczność narzędzi informatycznych on-line (strony internetowej i elektronicznego biuletynu) i oceniał inne działania informacyjne, a w razie potrzeby również nadawał im nowocześniejszy charakter.

- **Regulamin wewnętrzny**

Inspektor przyjmie i opublikuje regulamin wewnętrzny potwierdzający lub wyjaśniający praktyki obowiązujące w odniesieniu do różnych spoczywających na nim zadań i wykonywanych przez niego czynności. Praktyczne narzędzia dla zainteresowanych podmiotów będą dostępne na stronie internetowej.

- **Zarządzanie zasobami**

Inspektor będzie dalej konsolidował i rozwijał działania związane z zasobami finansowymi i ludzkimi; udoskonali również inne wewnętrzne procedury. Szczególną uwagę zwróci na długofalową rekrutację personelu, potrzebę uzyskania dodatkowej przestrzeni biurowej i rozwijanie systemu zarządzania sprawami.

2. Nadzór

2.1. Wprowadzenie

Zadaniem Europejskiego Inspektora Ochrony Danych jest niezależny nadzór nad przeprowadzonymi przez instytucje lub organy wspólnotowe operacjami przetwarzania danych, które w całości lub częściowo wchodzą w zakres prawa wspólnotowego (z wyjątkiem Trybunału Sprawiedliwości działającego w ramach swych kompetencji sądowych). Rozporządzenie (WE) nr 45/2001 („rozporządzenie”) określa i przyznaje szereg obowiązków i uprawnień umożliwiających Inspektorowi sprawowanie nadzoru.

Kontrola wstępna czynności przetwarzania nadal była głównym aspektem nadzoru w ciągu roku 2008, będąc wyraźnym rezultatem powiadomień otrzymanych po tzw. działaniu z wiosny 2007 roku (zob. sekcje 2.3.3 i 2.5.1). Zadanie to obejmuje analizę działań instytucji i organów w dziedzinach, które mogą stwarzać konkretne zagrożenia dla osób, których dane dotyczą, zgodnie z art. 27 rozporządzenia (WE) 45/2001. Inspektor dokonał kontroli wstępnej istniejących oraz planowanych operacji przetwarzania w najważniejszych kategoriach. Opinie Inspektora pozwalają administratorom danych dostosowywać przeprowadzane przez nich operacje przetwarzania danych w taki sposób, aby były one zgodne z rozporządzeniem. Inspektor dysponuje również innymi metodami, takimi jak rozpatrywanie skarg, prowadzenie dochodzeń i kontroli oraz udzielanie porad dotyczących środków administracyjnych.

Jeśli chodzi o uprawnienia nadane Inspektorowi, w 2008 roku, podobnie jak w latach poprzednich, nie było konieczne wydanie żadnego nakazu, ostrzeżenia ani zakazu, jako że administratorzy danych wykonywali zalecenia Inspektora lub wyrażali



Zastępca Inspektora Joaquín Bayo Delgado – odpowiedzialny za zespół ds. nadzoru

zamiar ich wykonania, podejmując niezbędne kroki. Szybkość reakcji różni się w poszczególnych przypadkach. Inspektor systematycznie śledzi wykonywanie zaleceń.

2.2. Inspektorzy ochrony danych

W rozporządzeniu przewiduje się, że przynajmniej jedna osoba powinna być mianowana na inspektora ochrony danych (DPO) (art. 24 ust. 1 rozporządzenia). Niektóre instytucje wyznaczyły również zastępcę DPO. Komisja wyznaczyła także DPO dla Europejskiego Urzędu ds. Zwalczenia Nadużyć Finansowych (OLAF, jedna z dyrekcji generalnych Komisji) oraz koordynatora ds. ochrony danych (DPC) w każdej z pozostałych dyrekcji generalnych, w celu koordynowania wszystkich aspektów ochrony danych w danej dyrekcji generalnej.

Od kilku lat DPO spotykają się regularnie w celu wymiany wspólnych doświadczeń i omawiania zagadnień horyzontalnych. Ta nieformalna sieć okazała się być przydatnym narzędziem współpracy. Funkcjonowała ona także w 2008 roku.



Inspektorzy ochrony danych na swoim 21. zebraniu w Brukseli (26 czerwca 2008 r.)

„Kwartet DPO” składający się z DPO z czterech instytucji (Parlamentu Europejskiego, Rady Unii Europejskiej, Komisji Europejskiej i Centrum Tłumaczeń dla Organów Unii Europejskiej) został utworzony w celu koordynowania sieci DPO. Inspektor ściśle współpracował z tym kwartetem, w szczególności nad przygotowywaniem porządków posiedzeń.

Inspektor brał udział w części każdego posiedzenia DPO, które odbyło się w roku 2008: w lutym w Luksemburgu (w Parlamencie Europejskim), w czerwcu (w Komitecie Regionów i Europejskim Komitecie Ekonomiczno-Społecznym w Brukseli) i w październiku (w Komisji Europejskiej w Strasburgu). Posiedzenia te stanowiły dla Inspektora dobrą sposobność do przekazania DPO aktualnych informacji na temat działań, które prowadzi, oraz do omówienia zagadnień będących przedmiotem zainteresowania obu stron. Inspektor wykorzystał to forum do wyjaśnienia i omówienia procedury kontroli wstępnych oraz niektórych z najważniejszych kwestii poruszonych podczas przeprowadzania kontroli wstępnych. Na każdym posiedzeniu przekazywano DPO informacje na temat postępów w powiadamianiu o kontrolach wstępnych.

Spotkania Inspektora z DPO stworzyły także dla Inspektora okazję do przedstawienia DPO aktualnych informacji na temat działania z wiosny 2007 roku i jego następstw, zwłaszcza w dziedzinie

kontroli (zob. sekcja 2.5.1. „Wiosna 2007 roku i okres późniejszy”). Spotkania te stanowiły również okazję dla Inspektora i części DPO do wymiany inicjatyw podjętych na rzecz Europejskiego Dnia Ochrony Danych (28 stycznia). Inspektor dokonał także prezentacji stanu projektów pilotażowych w ramach kontroli wstępnych, wraz z prezentacją na temat przekazywania danych medycznych do sądów krajowych oraz prezentacją na temat klauzul umownych, które należy wprowadzić do umów przetargowych zawieranych między instytucjami UE a podwykonawcami, dotyczących danych osobowych.

W czerwcu w siedzibie Inspektora odbyło się także spotkanie z DPO z agencji UE mające na celu omówienie konkretnych kwestii merytorycznych i proceduralnych dotyczących tych agencji. Była to także okazja do omówienia nowej procedury kontroli wstępnych *ex post* dla agencji (zob. sekcja 2.3.2 „Procedura”). Personel biura Inspektora dokonał wtedy także prezentacji głównych procedur, które, jak uznał Inspektor, znajdują się poza zakresem zastosowania art. 27 rozporządzenia i wobec tego nie podlegają kontrolom wstępным.

W 2008 roku grupa robocza ds. terminów przechowywania danych, ds. blokowania i ds. usuwania danych odbyła trzy posiedzenia robocze. Brali w nich udział zastępca Inspektora oraz dwóch członków personelu. Eksperti z dziedziny informatyki z instytucji biorących udział w posiedzeniach

zostali poproszeni o włączenie się do rozmów i przedstawienie uwag. Przedstawiono im także do omówienia wstępne wersje scenariuszy ilustrujących główne kwestie. W wyniku rozmów na forum grupy roboczej sporządzono dokument roboczy, który przekazano DPO do dalszych konsultacji z działami informatyki.

2.3. Kontrole wstępne

2.3.1. Podstawa prawna

Zasada ogólna: Art. 27 ust. 1

Art. 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 przez Inspektora. Art. 27 ust. 2 rozporządzenia zawiera wykaz operacji przetwarzania danych, które mogą stworzyć takie zagrożenia.

Wykaz ten nie jest wyczerpujący. Inne niewymienione przypadki mogą stanowić konkretne zagrożenie dla praw i wolności osób, których dane dotyczą, uzasadniają zatem przeprowadzenie kontroli wstępnej przez Inspektora. Na przykład każda operacja przetwarzania danych osobowych, która ma związek z zasadą poufności, określona w art. 36, wiąże się ze konkretnymi zagrożeniami, które uzasadniają przeprowadzenie kontroli wstępnej przez Inspektora.

Przypadki wymienione w art. 27 ust. 2

Art. 27 ust. 2 rozporządzenia zawiera wykaz kilku operacji przetwarzania danych, które mogą stworzyć konkretne zagrożenia dla praw i wolności osób, których dane dotyczą:

- a) przetwarzanie danych odnoszących się do zdrowia i dotyczących podejrzeń o popełnienie przestępstwa, przestępstw, wyroków karnych lub środków bezpieczeństwa (*sûreté* w języku francuskim, tj. środki przyjęte w ramach postępowania prawnego);
- b) operacje przetwarzania zmierzające do oceny aspektów osobistych odnoszących się do osoby, której dane dotyczą, włącznie z jej możliwościami, wydajnością lub postępowaniem;
- c) operacje przetwarzania zezwalające na tworzenie powiązań, nieuwzględnionych w odpowiednim ustawodawstwie krajowym lub legislacji wspólnotowej, między danymi przetwarzanymi do różnych celów;

- d) operacje przetwarzania w celu pozbawienia jednostki prawa, świadczenia lub wyłączenia jej z umowy.

Kryteria opracowane w latach poprzednich ⁽⁴⁾ nadal były stosowane podczas interpretacji tego przepisu zarówno podczas podejmowania decyzji, zgodnie z którą dane powiadomienie od DPO nie podlega kontroli wstępnej, jak i podczas doradzania w sprawie konsultacji dotyczącej potrzeby przeprowadzenia kontroli wstępnej (zob. także sekcja 2.3.6).

2.3.2. Procedura

Powiadomienie/konsultacja

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

Termin, zawieszenie i przedłużenie

Inspektor musi wydać opinię w terminie dwóch miesięcy od otrzymania stosownego powiadomienia. W przypadku gdy Inspektor zwraca się z wnioskiem o dostarczenie dalszych informacji, bieg tego dwumiesięcznego okresu ulega zwykle zawieszeniu do momentu uzyskania takich informacji przez Inspektora. Okres zawieszenia obejmuje czas – zazwyczaj 7–10 dni kalendarzowych, a w przypadku gdy przypadają one na dni wolne od pracy, dni roboczych – przysługujący DPO danej instytucji lub danego organu na przekazanie uwag lub, w razie potrzeby, dalszych informacji na temat wersji ostatecznej.

Jeśli wymaga tego złożony charakter sprawy, początkowy dwumiesięczny okres może również zostać przedłużony o kolejne dwa miesiące w drodze decyzji Inspektora, o której należy poinformować administratora danych przed upływem początkowego dwumiesięcznego okresu. Jeżeli do końca dwumiesięcznego okresu lub jego przedłużenia nie zostanie wydana żadna decyzja, przyjmuje się, że opinia Inspektora jest pozytywna. Do tej pory nie było przypadku takiej domyślnej opinii

Dane dotyczące spraw *ex post* otrzymanych przed dniem 1 września 2008 r. nie uwzględniają sierpnia ani dla instytucji i organów, ani dla Inspektora.

Procedura kontroli wstępnej *ex post* w agencjach

Inspektor uruchomił nową procedurę przeprowadzania kontroli wstępnych *ex post* w agencjach UE. Ponieważ w wielu sprawach standardowe procedury są takie same w większości agencji UE i są oparte

⁽⁴⁾ Zob. sprawozdanie za rok 2005, sekcja 2.3.1.



Zebranie zespołu ds. nadzoru

na decyzjach Komisji, idea polega na zgromadzeniu powiadomień na podobne tematy i przyjęcia albo opinii zbiorczej (dla różnych agencji), albo przeprowadzenia „minikontroli wstępnej” obejmującej wyłącznie konkretne aspekty danej agencji. Aby pomóc agencjom w wypełnieniu powiadomień, Inspektor przedłoży podsumowanie głównych punktów i wniosków na dany temat na podstawie poprzednich opinii z kontroli wstępnej (zwłaszcza z Komisji). DPO następnie przedłoży powiadomienie na mocy art. 27 wraz z pismem przewodnim uwydatniającym konkretne aspekty *w odniesieniu do* stanowiska Inspektora w tej dziedzinie (konkretne aspekty przetwarzania w danej agencji, kwestie problematyczne itd.). Procedurę tę uruchomiono w październiku 2008 roku, a jej pierwszym tematem była rekrutacja.

Rejestr

Art. 27 ust. 5 rozporządzenia przewiduje, że Inspektor 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.

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

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

Po wydaniu opinii przez Inspektora, jest ona podawana do wiadomości publicznej. Wszystkie opinie są dostępne na stronie internetowej Inspektora wraz ze streszczeniem danej sprawy. Obecnie rejestr jest publikowany na stronie Inspektora, tak że dostępne są także powiadomienia.

Opinie

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

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

Analiza prawna rozpoczyna się od zbadania, czy dana sprawa faktycznie kwalifikuje się do przeprowadzenia kontroli wstępnej. Jak wspomniano powyżej, jeżeli dana sprawa nie mieści się w zakresie spraw wymienionych w art. 27 ust. 2, Inspektor oceni konkretne zagrożenie dla praw i wolności osoby, której dane dotyczą. Kiedy dana sprawa zostanie zakwalifikowana do przeprowadzenia kontroli wstępnej, zasadniczym punktem analizy prawnej jest zbadanie, czy dana operacja przetwarzania jest zgodna ze stosownymi przepisami rozporządzenia. W razie potrzeby wydawane są zalecenia służące zapewnieniu przestrzegania przepisów rozporządzenia. We wnioskach Inspektor zwykle stwierdzał do tej pory, że przetwarzanie nie wydaje się powodować naruszenia żadnego przepisu rozporządzenia, pod warunkiem uwzględnienia wydanych zaleceń.

Opracowano podręcznik rozpatrywania spraw, aby zagwarantować, podobnie jak w innych obszarach,

pracę całego zespołu na takich samych podstawach oraz przyjmowanie opinii Inspektora po kompletnej analizie wszystkich istotnych informacji. Na podstawie zgromadzonych doświadczeń praktycznych podreżnik nadaje opiniom strukturę i jest stale aktualizowany. Zawiera on również listę kontrolną.

Istnieje także system przepływu pracy, który ma zapewnić wykonywanie wszystkich zaleceń w danej sprawie a, w stosownych przypadkach, przestrzeganie wszystkich decyzji wykonawczych (zob. sekcja 2.3.8).

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

Rozporządzenie weszło w życie w dniu 1 lutego 2001 r. Jego art. 50 nałożył na instytucje i organy wspólnotowe obowiązek dopilnowania, aby operacje przetwarzania będące wówczas w toku, zostały doprowadzone do zgodności z rozporządzeniem w terminie roku od tej daty (tzn. do 1 lutego 2002 r.). Mianowanie Inspektora i jego zastępcy nabrało mocy 17 stycznia 2004 r.

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

W latach 2004 i 2005 w większości instytucji i organów określono pewne kategorie, które uznano za wymagające bardziej systematycznego nadzoru (kartoteki medyczne i inne zawierające dane dotyczące stanu zdrowia, oceny personelu, również zatrudnianie personelu w przyszłości, procedury dyscyplinarne, usługi społeczne i e-nadzorowanie). Od wiosny 2007 roku kategorie te nie służą ustalaniu priorytetów i są wykorzystywane wyłącznie do kontroli systematycznej. Właściwe sprawy dotyczące kontroli wstępnej nigdy nie podlegały powyższej kategoryzacji, ponieważ muszą być rozpatrywane przed rozpoczęciem danej operacji przetwarzania. Sprawy dotyczące kontroli wstępnej w coraz mniejszym stopniu odnoszą się do tych obszarów, a także np. do operacji umożliwiających powiązania między różnymi bazami danych nie przewidziane w aktach prawnych (art. 27 ust. 2 lit. c) rozporządzenia).

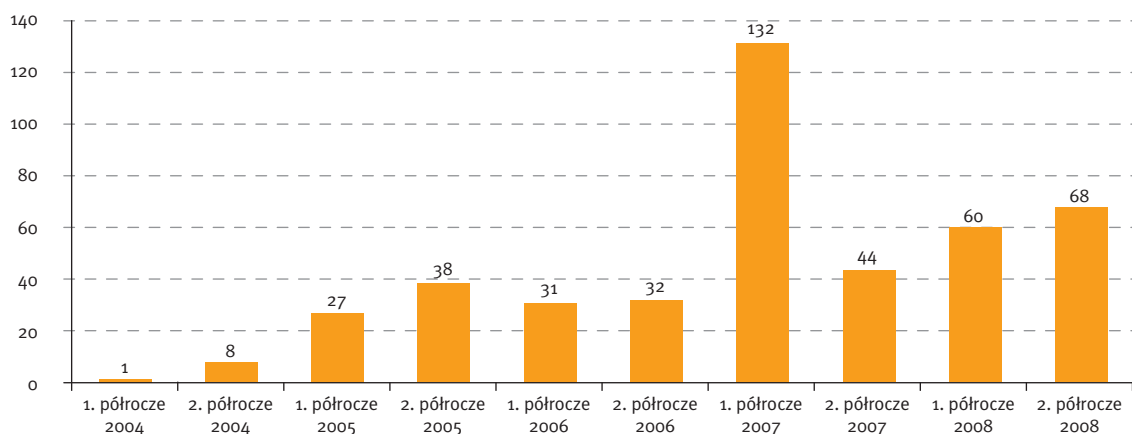
2.3.3. Analiza ilościowa

Powiadomienia dotyczące przeprowadzenia kontroli wstępnej

Jak wspomniano w poprzednich sprawozdaniach rocznych, Inspektor nieustannie zachęca inspektorów ochrony danych do zwiększania liczby kierowanych do niego powiadomień o potrzebie przeprowadzenia kontroli wstępnej.

Ostateczny termin przypadający wiosną 2007 roku (zob. sprawozdanie za rok 2007) spowodował, że instytucje i organy wzmogły starania na rzecz całkowitego spełnienia zobowiązań dotyczących powiadomień i zaowocował znaczącym zwiększeniem liczby powiadomień. W roku 2008 odnotowano wyraźne obniżenie liczby powiadomień, ale jak wskazują liczby

Powiadomienia przekazane Inspektorowi



(zob. diagram poniżej), liczba wydanych opinii jest wyższa niż w roku 2007, co jest bezpośrednim wynikiem ustanowienia terminu na wiosnę 2007 roku.

Opinie na temat spraw dotyczących kontroli wstępnej wydane w 2008 roku

W 2008 roku wydano 105 opinii⁽⁵⁾ dotyczących powiadomień o przeprowadzeniu kontroli wstępnej.

Rada Unii Europejskiej	16 spraw
Komisja Europejska	34 spraw
Europejski Bank Centralny (EBC)	1 sprawa
Trybunał Sprawiedliwości Wspólnot Europejskich	1 sprawa
Europejski Bank Inwestycyjny (EBI)	2 sprawy
Parlament Europejski	9 spraw
Centrum Tłumaczeń dla Organów Unii Europejskiej (CdT)	1 sprawa
Europejski Urząd Doboru Kadr (EPSO) ⁽¹⁾	1 sprawa
Europejski Trybunał Obrachunkowy (ETO)	4 sprawy
Komitet Regionów (KR)	1 sprawa
Europejski Komitet Ekonomiczno-Społeczny (EKES)	3 sprawy
EKES/KR	2 sprawy
Europejski Rzecznik Praw Obywatelskich	1 sprawa
Urząd Harmonizacji Rynku Wewnętrzny (UHRW)	4 sprawy
Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF)	4 sprawy
Wspólnotowy Urząd Ochrony Odmian Roślin (CPVO)	2 sprawy
Europejskie Centrum Rozwoju Kształcenia Zawodowego (CEDEFOP)	3 sprawy
Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA)	2 sprawy
Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA)	5 spraw
Europejska Agencja Leków (EMA)	5 spraw
Europejska Agencja ds. Bezpieczeństwa na Morzu (EMSA)	3 sprawy
Agencja Praw Podstawowych Unii Europejskiej (FRA)	1 sprawa

(1) EPSO korzysta z usług DPO Komisji.

Tych 109 spraw stanowi wzrost o 8% w porównaniu z liczbą przeprowadzanych kontroli wstępnych w 2007 roku.

(5) Inspektor otrzymał 109 powiadomień, lecz z przyczyn praktycznych niektóre sprawy powiązано. Dlatego na 109 powiadomień wydano 105 opinii.

Ze 109 spraw dotyczących kontroli wstępnej (105 opinii), tylko 18 to właściwe sprawy dotyczące kontroli wstępnej, tzn. zainteresowane instytucje lub organy (ETO, CEDEFOP, EKES/KR, FRA i UHRW po jednej sprawie, Parlament Europejski – dwie sprawy, OLAF – trzy sprawy i po cztery sprawy dla Rady i dla Komisji Europejskiej) zastosowały procedurę obowiązującą w przypadku przeprowadzania kontroli wstępnych przed rozpoczęciem operacji przetwarzania.

Wynikiem tych 18 kontroli wstępnych było 16 opinii, ponieważ dwie sprawy dotyczące Parlamentu Europejskiego miały powiązania, odpowiednio, z FRA i z Radą (wybór członków komitetu naukowego FRA i wybór Inspektora i jego zastępcy).

Pozostałe opinie z kontroli wstępnej dotyczyły następujących przedmiotów:

- elastycznego czasu pracy (flexitime);
- zaproszenia do składania ofert (dwie sprawy);
- systemu ochrony obejmującego telewizję przemysłową (zob. także sekcja 2.7);
- doboru kandydatów na stanowisko Inspektora i jego zastępcy (Komisja);
- powiązań między danymi przetwarzanymi dla różnych celów, nie przewidzianych w prawodawstwie (art. 27 ust. 2 lit. c) rozporządzenia) (interfejs flexitime/PersonaGrata);
- kontroli dostępu i tożsamości (dwie sprawy);
- nadzorowania Internetu;
- projektu pilotażowego dotyczącego nadzorowania indywidualnej wydajności;
- systemu zarządzania jakością;
- zapytań administracyjnych i postępowań dyscyplinarnych; oraz
- koordynacji wsparcia medycznego, psychospołecznego i administracyjnego (COMPAS) (zob. także sekcja 2.3.5).

Pozostałe opinie odnosiły się do kontroli wstępnych *ex post*.

Poza powiadomieniami, w związku z którymi została wydana opinia, Inspektor zajmował się również 13 sprawami, które uznano za niepodlegające kontroli wstępnej. Inspektor z zadowoleniem zauważa obniżenie się liczby tzw. „kontroli nie będących wstępnymi”. Jest to z pewnością częściowo spowodowane ostatecznym terminem przypadającym wiosną 2007 roku, który zwiększył świadomość wśród DPO i sprawił, że dokonywano dokładniejszych ocen przed wysyłaniem powiadomień. Analizę tych 13 spraw przedstawiono w sekcji 2.3.7.

Wycofano dziewięć powiadomień, w tym specjalną sprawę z Europejskiego Banku Inwestycyjnego dotyczącą operacji przetwarzania odnoszących się do „osób narażonych na ryzyko pod względem politycznym” (analiza tej sprawy jest rozwinięta wraz z pojęciem „kontroli nie będących wstępnymi” w sekcji 2.3.7). Po raz pierwszy Inspektor zdecydował się zasugerować, by wycofano niektóre powiadomienia. Decyzja ta była spowodowana faktem, że powiadomienia te dotyczyły starych operacji przetwarzania danych, które miały właśnie zostać zastąpione nowymi, lub też informacje w nich zawarte były niewystarczające, by możliwe było prawidłowe zrozumieniu stanu faktycznego lub procedury.

Inspektor zachęca DPO i administratorów danych do formułowania powiadomień w sposób możliwie jasny, co ma bezpośredni skutek w postaci skrócenia okresu zawieszenia, w którym dana instytucja lub organ odpowiada na wnioski Inspektora o informacje. Inspektor zamierza sporządzić udokumentowany formularz powiadomienia przeznaczony dla wszystkich DPO i podający im oraz kontrolerom szczegółowy wykaz potrzebnych informacji.

Analiza według instytucji i organu

W następstwie działania z wiosny 2007 roku instytucje i organy wspólnotowe poczyniły postępy w przestrzeganiu rozporządzenia. Większość instytucji i organów powiadamiała o operacjach przetwarzania mogących stwarzać szczególne zagrożenie.

Komisja Europejska poczyniła znaczne postępy w tej dziedzinie, przy czym znacząca liczba powiadomień została przekazana przez Wspólne Centrum Badawcze Komisji. Rada i obydwie Komitety również poczyniły znaczące postępy. Europejski Bank Inwestycyjny i Europejski Bank Centralny przekazały mniej powiadomień, ale będą miały ku temu więcej okazji z racji nowych kwestii, którymi należy się zająć.

Jeżeli chodzi o agencje, CEDEFOP, EMCCD, EMEA i EMSA wykazywały dużą aktywność w powiadamianiu o operacjach przetwarzania. Niektóre inne agencje powoli zaczynają powiadamiać o operacjach przetwarzania danych. W roku 2009 nastąpi niewątpliwie znaczące zwiększenie liczby powiadomień pochodzących od agencji. Inspektor rozpoczął przekazywanie porad na temat tego, jak dokonywać powiadomienia zgodnie z nową procedurą dotyczącą kontroli wstępnych *ex post* w agencjach, w oparciu o wytyczne wydane przez Inspektora, zwłaszcza w dziedzinach danych dotyczących rekrutacji i danych medycznych.

Analiza według kategorii

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

Kategoria pierwsza (dokumentacja medyczna)	28 spraw
Kategoria druga (ocena personelu)	53 sprawy
Kategoria trzecia (podejrzenie popełnienia przestępstwa)	6 spraw
Kategoria czwarta (usługi socjalne)	0 spraw
Kategoria piąta (e-monitoring)	4 sprawy
Inne obszary	14 spraw

Kategoria pierwsza obejmuje zwłaszcza samą kartotekę medyczną i jej zawartość, wypadki w pracy, zwolnienia chorobowe, procedurę stwierdzenia inwalidztwa, żłobki, ubezpieczenia zdrowotne, procedury przyznawania zasiłków, dozymetrię i trzy różne sprawy związane z danymi dotyczącymi stanu zdrowia. Spośród 28 spraw 17 pochodziło z różnych części Wspólnego Centrum Badawczego. Ta rosnąca liczba dała Inspektorowi okazję do doradzenia na temat głównych procedur związanych z danymi dotyczącymi stanu zdrowia w głównych instytucjach.

Głównym tematem pozostaje **kategoria druga** dotycząca oceny pracowników (53 opinie spośród 105). 23 sprawy dotyczyły rekrutacji (rekrutacji urzędników, pracowników tymczasowych i kontraktowych, stażystów, ekspertów, członków komitetów naukowych, Inspektora oraz jego zastępcy). Inne sprawy dotyczyły zwłaszcza oceny, awansów, procedur certyfikacji i zatwierdzenia, szkoleń, elastycznego czasu pracy i wcześniejszych emerytur.

Jeżeli chodzi o **kategorię trzecią** dotyczącą przestępstw i podejrzeń o popełnienie przestępstwa, to liczba spraw znacznie się zmniejszyła (sześć opinii wobec 18 w roku 2007). Tylko jedną opinię wydano w odniesieniu do procedury dyscyplinarnej, ponieważ większość instytucji powiadomiła o tych sprawach w latach ubiegłych. Inną opinię wydano w związku z dochodzeniami dotyczącymi bezpieczeństwa (zob. sekcja 2.3.4), dwie opinie – w związku z nękaniami, a dwie inne w innych sprawach.

Jeżeli chodzi o **kategorię czwartą** (usługi socjalne), Inspektor nie otrzymał żadnych powiadomień, co jest zrozumiałe, ponieważ kategoria ta została uprzednio poddana kontroli wstępnej w

odniesieniu do dużych instytucji, a większość agencji ogólnie nie ma możliwości oferowania takich usług swoim pracownikom.

Jeżeli chodzi o **kategorię piątą** (e-nadzorowanie), wydano tylko cztery opinie, ponieważ większość otrzymanych powiadomień odnosiła się do przetwarzania danych dotyczących billingów i zarządzania ruchem, zatem Inspektor uznał te sprawy za niepodlegające kontroli wstępnej z racji tego, że nie stanowią one konkretnego zagrożenia na mocy art. 27. Należy jednak podkreślić opinię przeznaczoną dla Europejskiego Trybunału Obrachunkowego, ponieważ faktycznie dotyczyła ona monitorowania łączności (sprawa 2008-284, zob. analiza w sekcji 2.3.4).

Jeżeli chodzi o powiadomienia nienależące do żadnej z tych kategorii, Inspektor nadal przekazywał opinie w następujących dziedzinach:

- przetargi;
- systemy kontroli dostępu, w których wykorzystuje się systemy porównywania danych biometrycznych;
- telewizja przemysłowa (jedna z opinii była właściwym przypadkiem kontroli wstępnej – zob. sekcja 2.7);
- powiązanie baz danych (sprawa 2008-324 – PersonaGrata – Rada – zob. sekcja 2.3.5);
- różne inne sprawy, takie jak akredytacja lub zeznania w sądzie.

Dotrzymywanie terminów

Cztery wykresy w załączniku E do niniejszego sprawozdania ukazują czas potrzebny na przetworzenie opinii na temat kontroli wstępnych przez Inspektora, instytucje i organy wspólnotowe. Szczegółowo przedstawiają one liczbę dni, których Inspektor potrzebował, aby sporządzić opinię, liczbę dni dodatkowych wymaganych przez Inspektora oraz liczbę dni zawieszenia biegu terminu (czas niezbędny do otrzymania informacji od instytucji i organów).

Liczba dni, których Inspektor potrzebował, aby sporządzić opinię: w porównaniu do roku 2007 liczba dni zmniejszyła się o ponad dwa, osiągając przeciętnie 55 dni na opinię w roku 2008. Jest to bardzo zadowalająca wielkość, również w odniesieniu do zwiększenia się liczby i złożoności powiadomień przesyłanych do Inspektora.

Liczba dni dodatkowych dla Inspektora ⁽⁶⁾: w dziewięciu przypadkach Inspektor zwrócił się o dni dodatkowe. Ogólnie, chociaż możliwe jest przedłużenie o dwa miesiące (art. 27 ust. 4 rozporządzenia), zazwyczaj wnioskowany jest jeden miesiąc. Jednak w praktyce wszystkie opinie przyjęto w ciągu tego miesiąca, a większość w znacznie krótszym czasie.

Liczba dni zawieszenia biegu terminu ⁽⁷⁾: zwiększyła się liczba dni zawieszenia biegu terminu między rokiem 2007 (przy przeciętnej wynoszącej 75 dni na sprawę) a rokiem 2008 (przy przeciętnej wynoszącej 122 dni na sprawę).

Biorąc pod uwagę fakt, że przeciętna wynosiła 30 dni na sprawę w roku 2005 i 73 dni w roku 2006, Inspektor jest zaniepokojony długimi okresami potrzebnymi instytucjom i organom do przekazania dalszych informacji. W istocie niektóre sprawy zawieszono na okres do 524 dni, by otrzymać dalsze informacje. Inspektor uważa tę sytuację za nie do przyjęcia i przypomina instytucjom i organom o ich zobowiązaniu do współpracy z Inspektorem polegającej na dostarczaniu mu wymaganych informacji zgodnie z art. 30 rozporządzenia.

Przeciętna według instytucji i organu: wykresy za rok 2008 wskazują alarmujące wydłużenie okresów zawieszenia dla prawie wszystkich instytucji i organów. Z wyjątkiem Parlamentu Europejskiego i EFSA – którym udało się obniżyć własną średnią – wszystkie pozostałe instytucje i organy bardzo znacznie zwiększyły liczbę dni zawieszenia. Odnosi się to zwłaszcza do EBI, Rady, Komisji, Trybunału Obrachunkowego, Trybunału Sprawiedliwości oraz do agencji.

Inspektor uznaje fakt, że za większą część czasu zawieszenia odpowiadają administratorzy danych. Niemniej jednak DPO powinni zwracać większą uwagę na terminy, ponieważ to oni ponoszą ostateczną odpowiedzialność za powiadomienie i dostarczanie dalszych informacji, bez względu na to, że z ewentualnych przyczyn praktycznych wnioski mogą być kierowane bezpośrednio do kontrolerów, z kopią do DPO.

⁽⁶⁾ Zgodnie z art. 27 ust. 4 Inspektor może, gdy wymaga tego złożony charakter sprawy, postanowić o przedłużeniu dwumiesięcznego terminu, w którym powinien przyjąć opinię.

⁽⁷⁾ Od połowy roku 2006 okres ten obejmuje zawieszenie na 7 lub 10 dni przewidziane na uwagi i dalsze informacje od DPO na temat wersji ostatecznej. W sprawach ex post otrzymanych przed dniem 1 września 2008 r. nie uwzględniono sierpnia.

Powiadomienia dotyczące przeprowadzenia kontroli wstępnej otrzymane przed 1 stycznia 2009 r. i powiadomienia będące w toku

Do końca 2008 roku w trakcie analizy znajdowało się 69 spraw dotyczących kontroli wstępnej. Spośród nich jedno powiadomienie przesłano w roku 2006, 11 w roku 2007 i 55 powiadomień w roku 2008.

Analiza według instytucji i organu

Parlament	7 spraw
Rada	6 spraw
Komisja Europejska	33 sprawy
EKES i KR	1 sprawa
EKES	4 sprawy
KR	3 sprawy
EBI	2 sprawy
ETO	2 sprawy
Trybunał Sprawiedliwości	1 sprawa
CEDEFOP	1 sprawa
CPVO	1 sprawa
EFSA	1 sprawa
EMEA	3 sprawy
EFK	1 sprawa
FRA	2 sprawy
UHRW	1 sprawa

Analiza według kategorii

Liczba spraw w toku dotyczących kontroli wstępnej będących przedmiotem powiadomienia na dzień 1 stycznia 2009 r. przedstawia się w rozbiu na kategorie następująco:

Kategoria pierwsza (dokumentacja medyczna)	20 spraw
Kategoria druga (ocena personelu)	26 spraw
Kategoria trzecia (podejrzenie popełnienia przestępstwa)	4 sprawy
Kategoria czwarta (usługi socjalne)	0 spraw
Kategoria piąta (e-monitoring)	3 sprawy
Inne obszary	16 spraw

2.3.4. Główne zagadnienia w sprawach dotyczących kontroli ex-post

Dane dotyczące stanu zdrowia

Inspektor wydał różne opinie na temat przetwarzania danych osobowych z dziedziny nieobecności z powodów medycznych (choroby lub

wypadku). Inspektor zalecił zwłaszcza, by dane gromadzone przez służby medyczne Parlamentu Europejskiego w celu uzasadnienia nieobecności z przyczyn medycznych mogły być wykorzystywane do innych celów (zwłaszcza do celów profilaktyki) wyłącznie za dobrowolnie wyrażoną zgodą odpowiednio poinformowanej osoby, której dane dotyczą (sprawa 2007-688). Inspektor uznał także w tym przypadku, że danych nie można przechowywać dłużej niż przez 12 lat w odniesieniu do osób, które tymczasem odeszły z instytucji.

Inspektor przeprowadził także kontrolę wstępną przetwarzania danych osobowych odnoszących się do nieobecności z przyczyn medycznych w Radzie we wspólnych sprawach 2008-271 i 2008-283. Zalecenia także dotyczyły głównie przechowywania danych przez służby medyczne kontrolujące nieobecności (*médécin contrôleur* w języku francuskim) przez 30 lat; w zaleceniach zwrócono się do tych służb o ponowne rozważenie okresu przechowywania danych w odniesieniu do celów operacji przetwarzania.

Inspektor wydał też opinię z kontroli wstępnej na temat oprogramowania PowerLab wykorzystywanego przez Wspólne Centrum Badawcze Komisji Europejskiej (sprawa 2007-649).

PowerLab jest oprogramowaniem wykorzystywanym do zarządzania cyklem pracy laboratoriów klinicznych i radio-toksykologicznych w Centrum. Stosuje się je do badań laboratoryjnych potrzebnych podczas oględzin medycznych przeprowadzanych przed zatrudnieniem oraz badań okresowych i badania innych zagrożeń chorobą zawodową. Oprogramowanie to obejmuje również wytwarzanie lub przechowywanie odpowiednich sprawozdań z badań.



Instytucje i agencje wspólnotowe przetwarzają dane dotyczące zdrowia

Główne zalecenia przedstawione w opinii z kontroli oprogramowania PowerLab dotyczyły:

- konieczności przestrzegania przez cały personel laboratorium obowiązku zachowania tajemnicy zawodowej;
- zobowiązania do niewykorzystywania otrzymanych danych do jakichkolwiek dalszych celów poza tym, do którego zostały przekazane; oraz
- potrzeby przekazywania kompletnych informacji.

Akredytacje dziennikarzy

Inspektor wydał opinię z kontroli wstępnej dotyczącą akredytowania dziennikarzy obsługujących posiedzenia Rady Europejskiej (sprawa 2004-259). Celem przetwarzania jest umożliwienie Biuru Bezpieczeństwa Rady przeprowadzenie oceny bezpieczeństwa pracowników prasy obsługujących szczyty. Osoby zarejestrowane mogą w razie potrzeby otrzymać identyfikator umożliwiający im przejście przez kordon bezpieczeństwa utworzony wokół budynku, w którym odbywa się szczyt.

Dotyczące dziennikarzy informacje służące przeprowadzeniu kontroli bezpieczeństwa są zarządzane przez ściąganie ich z formularza dostępnego na zabezpieczonej stronie (HTTPS) w sieci wewnętrznej (intranet) Rady.

Następnie administrator systemu automatycznie tworzy wykazy wniosków o sprawdzenie, które są przesyłane do różnych służb bezpieczeństwa (belgijskiego Krajowego Urzędu Bezpieczeństwa – NSA,

lub NSA należącego do prezydencji). Utworzone w tym celu wykazy zawierają imiona, nazwiska, daty urodzenia i narodowość osób. Urzędy bezpieczeństwa przekazują wyniki do osób odpowiedzialnych w biurze bezpieczeństwa – najpierw telefonicznie (by dokonać tego szybko), a następnie oficjalną pocztą. Wyniki pokazują wyłącznie „pozytywny” lub „negatywny” rezultat sprawdzania. Jednak zgodnie z decyzją Sekretarza Generalnego Rady nr 198/03 dyrektor biura bezpieczeństwa Rady może w wyjątkowych przypadkach podjąć inną decyzję podczas szczytu (np. w przypadku nieodpowiedniego zachowania).

Początkowy okres przechowywania wynosi pięć lat, ale Rada poruszyła kwestię możliwości przechowywania danych do 30 lat. W związku z tym Inspektor zalecił utrzymanie proporcjonalnego okresu przechowywania z uwzględnieniem celu przetwarzania. Inspektor poprosił także o niewprowadzanie do informacji uwagi „Należy zwrócić uwagę, że ubiegający się przekazują dane dobrowolnie i nikt nie jest zobowiązany do przekazywania tych danych” ponieważ w wielu przypadkach dziennikarze zwracają się o akredytację w ramach swojej pracy, zatem wartość ich zgody w rozumieniu art. 2 lit. h) można kwestionować.

Przyjęto także opinię z kontroli wstępnej dotyczącej akredytacji firm zewnętrznych (sprawa 2007-046). Inspektor doszedł do podobnych wniosków.

Inspektor wydał opinię (sprawa 2007-0349) na temat powiadomienia o kontroli wstępnej związanej z przetwarzaniem danych osobowych przeprowadzonym przez dyrekcję generalną ds. informatyki w Komisji Europejskiej w ramach oferowanej usługi zarządzania tożsamością (IMS).

IMS jest usługą głównie używaną do zarządzania grupami użytkowników i ich prawami w kontekście usług informatycznych. IMS w szczególności ułatwia uwierzytelnianie i kontrolę dostępu użytkowników do różnych serwisów informatycznych Komisji Europejskiej, którymi zarządzają różne dyrekcje generalne. Przez tę czynność IMS nadaje interfejsom użytkowników indywidualne cechy zgodnie z cechami charakterystycznymi danego użytkownika.



Akredytacja dziennikarzy i firm zewnętrznych w zakresie dostępu do szczytów Rady podlega kontroli wstępnej dokonywanej przez Inspektora

Usługa IMS jest wykorzystywana wobec personelu Komisji oraz personelu innych organizacji i ogółu społeczeństwa.

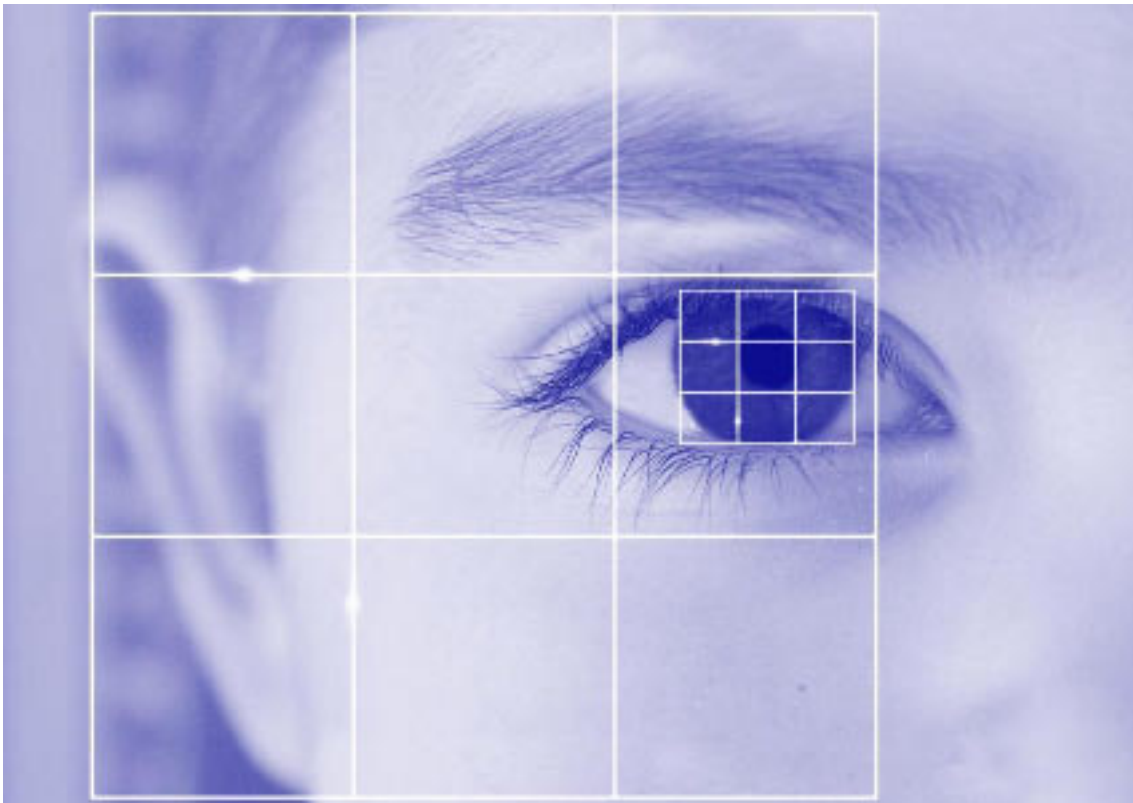
W swojej opinii Inspektor stwierdził, w Komisja w dużej mierze przestrzega rozporządzenia (WE) nr 45/2001. Niemniej jednak Inspektor wystosował zalecenia dotyczące zgodności przetwarzania z prawem i zasugerował potrzebę uzyskania zgody użytkowników na przetwarzanie danych przez IMS do celów nadania im indywidualnych cech (w sposób interaktywny i na ekranie, np. z wykorzystaniem dodatkowego okienka „pop-up”). Inspektor zasugerował także skrócenie terminów zatrzymywania plików logowania zgodnie z art. 37 ust. 2 rozporządzenia. Inspektor przyjmuje do wiadomości fakt, że IMS jest tak skonstruowany, by regularnie i automatycznie aktualizować dotyczące personelu informacje uzyskiwane za pośrednictwem kadrowych baz danych, a zatem zapewnia dokładność danych dotyczących członków personelu. Jednak nie wydaje się, by podobny system istniał w odniesieniu do informacji o użytkownikach zewnętrznych. Użytkowników

tych mogły zarejestrować strony trzecie takie jak ich pracodawcy, przy podwyższonym niebezpieczeństwie, że informacje te będą niedokładne. Inspektor podkreślił zatem, że ważne, jest, by do IMS wprowadzono system zapewniający dokładność informacji osobowych dotyczących członków personelu spoza Komisji, którzy zostali zarejestrowani w IMS przez strony trzecie, takie jak ich pracodawcy.

Kontrola dostępu

Inspektor wydał opinię z kontroli wstępnej na temat stworzenia systemu kontroli dostępu skanującego tęczówki członków personelu Europejskiego Banku Centralnego (EBC) oraz osób z zewnątrz wchodzących do ściśle zabezpieczonych miejsc w tej instytucji (sprawa 2007-501). System ten działa wraz z uprzednio istniejącym systemem kontroli dostępu, którego częścią jest bezkontaktowy identyfikator.

Wprawdzie opinia Inspektora ma bezpośrednie zastosowanie wyłącznie do EBC, jednak posłużyła ona jako bardziej ogólna wskazówka dotycząca właściwych cech systemu biometrycznego zgodnego z



Aby stwierdzić, czy stosowanie skanowania tęczówki jest uzasadnione, konieczna jest ukierunkowana ocena skutków i zbadanie możliwości użycia innych rozwiązań, mniej ingerujących w prywatność

zasadami prywatności. W szczególności Inspektor zalecił, by EBC przeprowadził ocenę oddziaływania i ponownie rozważył decyzję podjętą w odniesieniu do wyboru technologii. W istocie, mając na uwadze wysoce wrażliwy charakter danych biometrycznych, przeprowadzenie ukierunkowanej oceny oddziaływania, w której analizowano by przyczyny uzasadniające wykorzystanie systemu biometrycznego, jest niezbędne przed wprowadzeniem takiej technologii.

Inspektor wezwał EBC także do rozważenia wprowadzenia w odpowiednim czasie systemu przeszukiwania „one to one”, w którym dane biometryczne byłyby przechowywane w chipach, nie zaś w centralnej bazie danych, tak jak to ma miejsce w obecnym systemie. Ponadto, ponieważ systemy biometryczne nie są dostępne dla wszystkich ani całkowicie dokładne, należy wprowadzić łatwo dostępne procedury awaryjne. Procedury te zapewniałyby poszanowanie godności osób, których nie można było wprowadzić do systemu lub które mogły być niewłaściwie zidentyfikowane, i pozwoliłyby uniknąć przenoszenia na te osoby ciężaru niedoskonałości systemu.

Oprócz powyższego Inspektor zalecił, by EBC uchwalił akt prawny dający podstawę prawną do operacji przetwarzania, by stworzyć system kontroli dostępu oparty na wykorzystywaniu danych biometrycznych.

Rekrutacja

Nabór to – z oczywistych powodów – często wykonywana we wszystkich instytucjach i organach operacja przetwarzania. Inspektor otrzymał wiele powiadomień z tej dziedziny w roku 2008.

Inspektor przeprowadził szeroko zakrojone kontrole wstępne dotyczące procedur naboru we Wspólnym Centrum Badawczym przy Komisji Europejskiej. Procedury te dotyczyły:

- posiadaczy grantów (sprawa 2008-138);
- personelu tymczasowego (sprawa 2008-139);
- urzędników (sprawa 2008-140);
- pracowników kontraktowych (sprawa 2008-142);
- stażystów (sprawa 2008-136);

W tych opiniach Inspektor podkreślił kwestię gromadzenia zaświadczeń o niekaralności w trakcie naboru i poprosił, by Komisja przeprowadziła

indywidualną analizę treści kartotek policyjnych/rejestru karnego/zaświadczeń o niekaralności, tak by gromadzić wyłącznie dane mające znaczenie na podstawie wymogów regulaminu pracowniczego.

Inspektor zachęcił także administratora danych do znalezienia systemu, w którym informacje o przedawionych przestępstwach zostaną skreślone.

- naborze i transferach urzędników (sprawa 2004-207);
- pracowników kontraktowych (sprawa 2007-323);
- pracowników kontraktowych (sprawa 2007-384);

Wydano podobne zalecenia dotyczące przechowywania wypisów z kartotek policyjnych/rejestru karnego. Inspektor zalecił także, by usunąć z formularzy wniosków wzmiankę o tym, czy kandydat był uprzednio karany.

Europejski rzecznik praw obywatelskich również powiadomił o procedurach rekrutacji urzędników, personelu tymczasowego i pracowników kontraktowych (sprawa 2007-405).

Podobnie Rada powiadomiła o procedurze rekrutacji urzędników i innych pracowników (sprawa 2007-194). Przedstawiono także zalecenie dotyczące przechowywania informacji z rejestru karnego po zakończeniu procedury naboru.

Jak wspomniano w sekcji 2.3.2., Inspektor uruchomił nową procedurę powiadomień *ex post* związaną z przetwarzaniem w związku z rekrutacją w agencjach. W rezultacie sporządzono wytyczne na temat przetwarzania danych osobowych w trakcie rekrutacji, czego wynikiem będą liczne powiadomienia z tej dziedziny. Niemniej jednak kilka agencji przedłożyło już powiadomienia z dziedziny rekrutacji, zwłaszcza EMEA (sprawa 2007-422), UHRW (nabór kierowników – sprawa 2008-435), EMSA (rekrutacja personelu stałego, pracowników tymczasowych i kontraktowych – sprawa 2007-566 i rekrutacja stażystów – sprawa 2008-384) i EMCDDA (sprawa 2008-157).

Baza danych z nazwiskami ekspertów

Inspektor otrzymał powiadomienie dotyczące bazy danych EFSA z nazwiskami ekspertów (sprawa 2008-455). Baza danych zawiera dane zawodowe

zewnątrznych ekspertów naukowych, do których można się zwrócić o porady na rzecz EFSA (oraz na rzecz organów krajowych w państwach członkowskich mających mandat podobny do mandatu EFSA). Kandydaci składają on-line wnioski o wprowadzenie ich do bazy danych. Następnie EFSA sprawdza wnioski, by upewnić się, że bazy danych znajdują się wyłącznie eksperci spełniający kryteria kwalifikacyjne.

Zalecenia Inspektora obejmowały przede wszystkim fakt, że uwagę użytkowników końcowych należy zwrócić szczególnie na ograniczony charakter kontroli ważności przeprowadzanej przez EFSA, co sugeruje, że baza danych wykorzystywana jest jako pula wniosków, nie zaś jako pula ekspertów, których umiejętności i rzetelność zostały uprzednio starannie sprawdzone przez EFSA w każdym przypadku. Inspektor zalecił także, by do ekspertów, którzy nie zaktualizowali swoich profili (lub nie potwierdzili dotychczasowych) były wysyłane automatyczne przypomnienia z ostrzeżeniem, że brak odpowiedzi (po pewnej liczbie przypomnień) spowoduje automatyczne skreślenie danego profilu.

Ocena personelu

W dziedzinie oceny pracowników Inspektor przyjął opinię dotyczącą powiadomienia do celów kontroli wstępnej otrzymanego od inspektora ochrony danych w Parlamencie Europejskim i odnoszącego się do bazy danych „Skills” (sprawa 2008-192).

Ta baza danych zawiera dane o przebiegu kariery zawodowej pracowników obejmujące doświadczenie zawodowe zdobyte przed zatrudnieniem w Parlamencie Europejskim i w jego trakcie. Baza danych „Skills” jest metodą operacyjną, która ułatwia zarządzanie personelem w zakresie mobilności, doradztwa zawodowego, specjalistycznego pozyskiwania pracowników, obsadzania wakatów i planowania konkursów. Podstawą prawną tej działalności jest reguła 197 ust. 2 regulaminu wewnętrznego Parlamentu Europejskiego, która przewiduje możliwość organizowania różnych służb w tej instytucji. Biorąc pod uwagę ogólny charakter tej podstawy prawnej, Inspektor zalecił, by odpowiedni organ w Parlamencie Europejskim przyjął decyzję określającą charakterystykę, definicję i gwarancje tej bazy danych, by zapewnić przejrzystość i pewność prawną.

Inna opinia z kontroli wstępnej dotycząca oceny pracowników odnosiła się do systemu wewnętrznej

kontroli jakości, w trakcie której weryfikowane są wyniki prac kontrolerów znaków towarowych z ramienia UHRW, a wyniki wprowadzane do stworzonej w tym celu bazy danych (sprawa 2008-437). Głównym celem tych kontroli systematycznych jest poprawa ogólnej jakości wyników prac UHRW. Wyniki kontroli są jednak także wykorzystywane do oceny jakości pracy każdego kontrolera i do informowania kierownictwa o decyzjach dotyczących środków, które mogą mieć wpływ na poszczególnych kontrolerów, takich jak oceny wykonywania pracy, awanse, odnowienia kontraktów, środki dyscyplinarne lub szkolenia.

W swojej opinii Inspektor zalecił przyjęcie jasnej i formalnej decyzji wewnętrznej o wzmocnieniu podstawy prawnej tego działania i zapewniającej bardzo potrzebną jasność i pewność pracownikom. W decyzji tej powinien być wyczerpująco opisany system kontroli jakości *ex ante*, łącznie z ich zamierzonym celem, oraz powinny być przewidziane odpowiednie zabezpieczenia danych osobowych.

Inspektor podkreślił także, że należy dołożyć wszelkich starań, by poprawić poziom dokładności, rzetelności i spójności danych. W każdym przypadku dane zawarte w bazie powinny być wykorzystywane jedynie jako jeden z wielu czynników, które należy uwzględnić w procesie podejmowania decyzji. Gdy dane przechowywane w tej bazie są wykorzystywane do celów, które mogą mieć wpływ na poszczególnych pracowników, pracownicy ci muszą być wysłuchani i muszą mieć możliwość przedstawienia własnych stanowisk.

Dochodzenia dotyczące bezpieczeństwa

Inspektor wydał opinię na temat dochodzeń dotyczących bezpieczeństwa prowadzonych w Komisji Europejskiej (sprawa 2007-736). Dyrekcja ds. bezpieczeństwa (nakazy administracyjne) jest władna do podejmowania pewnych środków wobec sprawców czynów bezprawnych lub aktów wandalizmu wobec budynków zajmowanych przez Komisję, wobec osób pracujących w tych budynkach lub mających do nich dostęp, oraz wszelkich innych czynów, które mogą narazić tę instytucję na szwank. Obejmuje to przechowywanie wszelkich materiałów dowodowych, przeszukiwanie w celu ich pozyskania, wysłuchiwanie oświadczeń powodów, świadków lub, w razie potrzeby, osób odpowiedzialnych za te czyny.

Inspektor przeanalizował przetwarzanie danych w ramach procedur dochodzeniowych w sprawach bezpieczeństwa i poprosił, by służba ta przeanalizowała proporcjonalność prowadzonych działań. W tym sensie dochodzenia muszą być proporcjonalne nie tylko w stosunku do ogólnego celu przetwarzania, lecz także w stosunku do celu konkretnej operacji przetwarzania. Inspektor podkreślił także konieczność udzielania dostatecznych gwarancji, by zapewnić ochronę danych i zalecił przyjęcie konkretnych metod działania, których należy przestrzegać przy przeszukiwaniach w celu pozyskania materiałów dowodowych. Jeżeli chodzi o przekazywanie danych do państw trzecich i organizacji międzynarodowych, Inspektor zalecił, by – w przypadkach, w których przekazanie można uzasadnić wyłącznie na podstawie art. 9 ust. 7 – utworzyć rejestr zawierający informacje o celach przekazania, osobach, których dotyczy przekazanie, prawie dostępu, podstawie prawnej i legalności przekazania, odbiorcy danych oraz oznaczenie okresu przechowywania danych przez odbiorcę.

Inspektor podkreślił także fakt, że prawo dostępu do danych osobowych musi być ustalone jako zasada i że wszelkie wyjątki od tego prawa muszą być zatem stosowane w ograniczonym zakresie. Na tej podstawie Inspektor zaakceptował, że art. 20 ust. 1 lit. c) rozporządzenia może służyć ochronie interesów informatorów.

Procedura przeciwko napastowaniu

Inspektor wydał opinię na temat nieformalnej procedury stworzonej w Komisji Europejskiej przeciwko napastowaniu seksualnemu i psychicznemu (sprawa 2008-062).

Inspektor w szczególności podkreślił, że prawo dostępu i prawo do poprawienia danych ustalone na mocy art. 13 i 14 rozporządzenia, powinno obowiązywać także wobec osobistych notatek poufnego doradcy. Inspektor zalecił także, by prawo dostępu do kartoteki dotyczącej przypadku domniemanego napastowania było również stosowane wobec osób trzecich, jeżeli kartoteka ta zawiera dane osobowe dotyczące danej osoby. Może tak być w przypadku osób uważanych za domniemanych „napastujących” lub w przypadku świadków. Zawarte w tych kartotekach informacje mogą być konsultowane bezpośrednio przez zainteresowaną osobę lub pośrednio (zwłaszcza

poprzez Inspektora). Ograniczenia tego prawa dostępu można nałożyć na mocy art. 20 rozporządzenia, zwłaszcza w celu ochrony praw innych osób lub gdyby dostęp okazał się szkodliwy dla toczącego się dochodzenia.

Koordinacja spraw prowadzonych przez OLAF

Inspektor przyjął opinię w sprawie przetwarzania danych osobowych przez OLAF w chwili, gdy otwiera on sprawę dotyczącą koordynacji (sprawa 2007-699). Są to sprawy, które mogą być przedmiotem dochodzeń zewnętrznych OLAF, ale w których rola OLAF polega na udziale w dochodzeniach prowadzonych przez inne służby krajowe lub wspólnotowe; udział ten może obejmować m.in. ułatwianie gromadzenia i wymiany informacji oraz zapewnianie współdziałania operacyjnego między odnośnymi służbami krajowymi i wspólnotowymi. Główny wkład w dochodzenie wnoszą inne organy. Rola OLAF obejmuje ułatwianie kontaktów i zachęcanie właściwych organów do współpracy. Rodzaje informacji osobowych przetwarzanych przez OLAF w tych sprawach obejmują identyfikację, dane zawodowe i informacje dotyczące działalności związanej ze sprawami będącymi przedmiotem koordynacji.

Inspektor w swojej opinii zwrócił się do OLAF o dopilnowanie, by osoby, których dane są przetwarzane przez to biuro, były informowane o przetwarzaniu danych odbywającym się w sprawach dotyczących koordynacji. Informacje te mogłyby być przekazywane przez właściwe organy krajowe, także w oświadczeniach o ochronie prywatności kierowanych do osób, których dane dotyczą, które to oświadczenia mogłyby zawierać akapit informujący o możliwości przekazania danych osobowych do OLAF do celów koordynacji. Ponieważ osoby fizyczne byłyby poinformowane o przekazywaniu przez właściwe organy krajowe ich danych osobowych do OLAF, biuro to nie musiałoby ponownie przekazywać tych informacji. W opinii zaproponowano także pewne poprawki do oświadczenia o ochronie prywatności i zwrócono się do OLAF o przeprowadzenie wstępnej oceny konieczności 20-letniego okresu *przechowywania* danych w odniesieniu do celu takiego przechowywania.

Upoważnienie do składania zeznań

Inspektor przeprowadził kontrolę wstępną procedury ustalonej przez Komisję Europejską w celu

przestrzegania przepisów regulaminu pracowniczego dotyczących upoważnienia do składania zeznań. Zgodnie z art. 19 regulaminu pracowniczego „Urzędnik nie może bez pozwolenia organu powołującego ujawnić w ramach postępowania sądowego informacji uzyskanych przy wykonywaniu swoich obowiązków. Udzielenia pozwolenia odmawia się jedynie w przypadku, gdy wymagają tego interesy Wspólnot, a odmowa nie może pociągać za sobą odpowiedzialności karnej urzędnika. Zobowiązanie to istnieje także po zakończeniu służby.”

W swojej opinii Inspektor przedstawił zalecenia co do prawa do obrony w tym sensie, że urzędnikowi należy umożliwić wypowiedzenie się przed podjęciem decyzji przez organ powołujący, o ile nie ma ograniczeń wobec tego prawa na mocy art. 20 ust. 1 rozporządzenia (WE) nr 45/2001.

2.3.5. Główne zagadnienia we właściwych kontrolach wstępnych

Inspektor powinien zwykle wydawać swoją opinię przed rozpoczęciem operacji przetwarzania, tak aby od początku zagwarantować prawa i wolności osób, których dane dotyczą. Jest to rozumowanie przedstawione w art. 27 rozporządzenia (WE) nr 45/2001. Wraz z kontrolami wstępnymi *ex post*, w roku 2008 do Inspektora przesłano 18 spraw dotyczących „właściwej” ⁽⁸⁾ kontroli wstępnej. W rezultacie Inspektor wydał 16 opinii (zob. sekcja 2.3.3.).

Procedury wyboru

Inspektor otrzymał powiadomienie dotyczące kontroli wstępnej od Europejskiej Agencji Praw Podstawowych (FRA), którego przedmiotem było przetwarzanie danych osobowych w trakcie doboru członków komitetu naukowego w agencji. Następne powiadomienie przesłał Parlament Europejski w związku z przetwarzaniem danych osobowych w ramach kolejnego etapu procedury doboru kadr do komisji LIBE Parlamentu (ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych).

Ponieważ oba powiadomienia dotyczyły tej samej procedury doboru, Inspektor wydał jedną opinię

obejmującą całą procedurę doboru (sprawy 2008-179 i 2008-202).

Wynikiem przeprowadzonej przez Inspektora analizy były przede wszystkim zalecenia dotyczące informowania osób, których dane dotyczą. W rzeczywistości, chociaż procedura została już uruchomiona, kandydatów nie poinformowano, że dane przedłożone przez nich w trakcie procedury doboru (życiorysy, listy motywacyjne itd.) zostaną podane do wiadomości publicznej w wyniku procedury publicznej stosowanej na sesjach komisji LIBE. Zgodnie z art. 12 rozporządzenia, informacje te należy przekazać w chwili pozyskania danych lub najpóźniej w chwili pierwszego ujawnienia danych stronie trzeciej. Ponieważ informacji tych nie przekazano w zaproszeniu do składania ofert, Inspektor zalecił, by:

- FRA informowała wszystkie osoby znajdujące się w końcowym wykazie kandydatów przed przekazaniem ich danych komisji LIBE, że dane przez nich przekazane będą podane do wiadomości publicznej w wyniku publicznego charakteru sesji Parlamentu Europejskiego i że mają oni prawo do sprzeciwu wobec publikowania ich danych;
- FRA informowała osoby znajdujące się w końcowym wykazie kandydatów o procedurach wykonywania ich prawa dostępu i o prawie do odwołania się do Inspektora;

Inspektor zalecił także, by informacje te zamieścić na stronie internetowej FRA, by były one dostępne dla osób nieznajdujących się w końcowym wykazie kandydatów. Ponadto Inspektor uznał, że informacje o przetwarzaniu danych osobowych powinny pozostawać dostępne na stronie internetowej FRA przynajmniej do zakończenia procedury doboru.

Inspektor dokonał także wstępnej kontroli ⁽⁹⁾ przetwarzania danych osobowych stanowiącego część procedury doboru Inspektora i jego zastępcy. W związku z tym wydano dwie opinie – jedna dotyczyła obowiązującej w Komisji Europejskiej procedury dotyczącej tworzenia końcowego wykazu kandydatów, który ma być przekazany Radzie i Parlamentowi Europejskiemu (sprawa

⁽⁸⁾ Tzn. spraw dotyczących jeszcze nierozpoczętej operacji przetwarzania.

⁽⁹⁾ Miało to miejsce w trakcie pełnienia obowiązków przez zastępcę Inspektora niemającego udziału w procedurze doboru.

2008-222), zaś druga opinia dotyczyła procedury odbywającej się w Radzie i Parlamencie (sprawy 2008-280 i 2008-292).

Jeżeli chodzi o pierwszą część procedury, Inspektor podkreślił fakt, że na wszystkich etapach procedury odbiorcom danych przypomina się, że mogą oni przetwarzać te dane wyłącznie do celów doboru kandydatów mających znaleźć się w końcowym wykazie kandydatów na stanowisko Inspektora i jego zastępcy. Ponadto Inspektor stwierdził, że wykorzystywano aplikację CV-online, w której należy podać informacje o numerze pracowniczym osób pracujących w instytucjach UE. Uwzględniając fakt, że CV-online jest standardowym narzędziem informatycznym wykorzystywanym w Komisji we wszystkich procedurach doboru na wyższe stanowiska kierownicze – zarówno wewnętrzne, jak i zewnętrzne – oraz że w niektórych przypadkach numer ten może okazać się konieczny w fazie selekcji w pozostałych procedurach, Inspektor zalecił, by Komisja wyraźnie zaznaczała w instrukcjach dla kandydatów, że wprowadzenie numeru pracowniczego do formularza w CV-online jest nieobowiązkowe i że kandydaci nie muszą go wprowadzać. Położono także szczególny nacisk na znaczenie informowania kandydatów, że ich dane zostaną podane do publicznej wiadomości z racji publicznego charakteru sesji komisji parlamentarnej LIBE.

Jeżeli chodzi o następną część procedury odbywającej się w Parlamencie Europejskim i Radzie, Inspektor wydał osobną opinię. W opinii tej podkreślono znaczenie przekazywania osobom z obydwu instytucji znajdującym się w wykazie końcowym kandydatów dostatecznych informacji na temat przetwarzania danych osobowych.

Monitorowanie indywidualne/ projekt pilotażowy

Inspektorowi przedłożono powiadomienie o kontroli wstępnej projektu pilotażowego w Radzie dotyczącego monitorowania indywidualnej wydajności (sprawa 2008-436). Ponieważ metoda ta służy przekazywaniu kierownikom działów językowych oraz poszczególnym pracownikom wskaźników indywidualnej wydajności, powinna ona umożliwiać poszczególnym pracownikom monitorowanie własnej pracy, zaś kierownikom działów – monitorowanie wydajno-

ści każdego pracownika z osobna oraz wszystkich pracowników w dziale za pomocą jednej prostej operacji.

Operację przetwarzania poddano kontroli wstępnej, po pierwsze, ponieważ wyniki projektu pilotażowego byłyby wykorzystywane przez kierownika działu jako jeden z elementów oceny wyników pracy każdego pracownika, zwłaszcza podczas ocen okresowych, oraz ponieważ przetwarzanie danych ma na celu ocenę wydajności pracowników (art. 27 ust. 2 lit. b)). Po drugie, przetwarzanie oznacza połączenia między dwoma bazami danych, którego nie przewiduje ani prawodawstwo krajowe, ani wspólnotowe (art. 27 ust. 2 lit. c)).

Inspektor skorzystał z okazji kontroli wstępnej, by przypomnieć Radzie o polityce dotyczącej projektów pilotażowych. Zasadniczo projekt nie może rozpoczynać się przed realizacją zaleceń przedstawionych w opinii przez Inspektora. Ponadto zakończenie projektu pilotażowego nie powoduje automatycznie pełnego uruchomienia systemu, tak by można go było natychmiast wprowadzić do stosowania. W rzeczywistości należy przeanalizować wyniki uzyskane w fazie pilotażowej przed rozpoczęciem uruchamiania systemu. Wyniki projektu pilotażowego należy przekazać Inspektorowi przed uruchomieniem projektu ogólnego; Inspektora należy też poinformować o wszelkich zmianach dokonanych w systemie ogólnym, które mogą mieć wpływ na przetwarzanie danych osobowych. Następnie Inspektor przeanalizuje przed uruchomieniem systemu ogólnego wyniki projektu pilotażowego i wszelkie implikacje dla ochrony danych. W swoim zaleceniu Inspektor podkreślił, że jeżeli dany projekt pilotażowy stanie się z chwilą zakończenia pełnoprawnym przedsięwzięciem, należy przyjąć decyzję prawną lub akt prawny stwarzający konkretną podstawę prawną do przetwarzania danych osobowych.

Elastyczny czas pracy (flexitime)

Kolejna opinia oparta na art. 27 ust. 2 lit. c) rozporządzenia (WE) nr 45/2001 została przyjęta w odniesieniu do interfejsu między stosowanymi w Radzie systemami Flexitime i PersonaGrata (sprawa 2008-324). System PersonaGrata jest narzędziem zarządczym przeznaczonym do organizowania pracy w służbach tłumaczeniowych Rady. Celem interfejsu jest pobieranie danych z systemu flexitime

przez system PersonaGrata, by tym samym uniknąć dublowania danych uważanych za równorzędne w obydwu bazach danych.

Inspektor uznał, że zapisywanie danych nie jest równorzędne, ponieważ ta kategoria danych jest przypisana do systemu flexitime. Ponadto liczba wpisów dotyczących nieobecności w systemie Flexitime jest wyższa niż liczba w systemie PersonaGrata. Zatem w systemie PersonaGrata różne przyczyny nieobecności są przedstawiane użytkownikom jako ten sam, jedyny powód nieobecności. Inspektor podkreślił, że równorzędność danych w obydwu systemach mogłaby pomóc zagwarantować przestrzeganie zasady jakości danych.

Inspektor wydał także opinię na temat operacji przetwarzania związanych z systemem elastycznego czasu pracy odnoszących się konkretnie do Dyrekcji Generalnej ds. Przedsiębiorstw i Przemysłu w Komisji Europejskiej ⁽¹⁰⁾ (sprawa 2008-111). W ramach tej operacji dyrekcja ta zamierzała wprowadzić w komputerach pracowników przycisk służący gromadzeniu danych o obecnościach.

W swojej analizie Inspektor uznał, że cel przekazanej mu przez Dyrekcję Generalną ds. Przedsiębiorstw i Przemysłu operacji przetwarzania nie spełnia do końca założeń systemu flexitime wynikających z analizy systemu zarządzania czasem (TIM) stosowanego w Komisji Europejskiej. W istocie, gdyby w przekazanym przypadku dane miały być chwilowo przechowywane przez kierownika działu, mogłoby to prowadzić do oceny nieprzewidzianej w systemie TIM. Zatem Inspektor sprzeciwił się przesyłaniu listów elektronicznych do oficjalnych skrzynek pocztowych kierowników działów. Niezależnie od tego stwierdzenia Inspektor uznał, że można przychylnie odnieść się do koncepcji przyjaznego dla użytkownika interfejsu służącego przechowywaniu danych o rejestracjach w systemie zarządzania czasem, bez potrzeby stosowania graficznego interfejsu użytkownika Sysper2-TIM.

E-monitoring

Bieżące monitorowanie korzystania z Internetu przez pracowników danej instytucji lub danego organu UE stworzyło dla Inspektora okazję do podkreślenia jego preferencji dla prewencyjnego,

⁽¹⁰⁾ System zarządzania czasem (TIM) wprowadzający flexitime do narzędzia zarządzania personelem (Sysper 2) w Komisji Europejskiej był przedmiotem poprzedniej kontroli wstępnej (2007-063).



Niedopuszczalne jest monitorowanie z ukrycia, gdy użytkownicy Internetu nie są świadomi, że obserwowane jest ich korzystanie z sieci

nie zaś represyjnego, podejścia do kwestii niewłaściwego wykorzystywania Internetu oraz do położenia nacisku na potrzebę proporcjonalności stosowanych środków (sprawa 2008-284).

W tym względzie Inspektor stwierdził w szczególności, że przy braku dostatecznego podejrzenia monitorowanie wszystkich stron internetowych odwiedzanych przez wszystkich użytkowników jest niepotrzebne i nadmierne. By wykrywać niewłaściwe wykorzystywanie, Inspektor poradził, by zamiast monitorowania stron wykorzystywać wskaźniki (ilość pobieranych danych, ilość czasu spędzona na przeglądaniu sieci, duża liczba nieudanych prób wejścia na zablokowane strony itd.). Niemniej jednak Inspektor stwierdził, że w niektórych szczególnych okolicznościach może zaistnieć konieczność monitorowania przez daną instytucję stron internetowych odwiedzanych przez konkretne osoby. Może tak być, gdy istnieje dostateczne podejrzenie, że dany użytkownik wykazuje zachowania godzące w instytucję (np. pobierając materiały pedofilskie) lub gdy długość adresu danej strony wskazuje na ewentualną próbę ataku sieciowego.

System telewizji przemysłowej

Inspektor przyjął opinię na temat systemu telewizji przemysłowej obsługiwanego przez Europejski Urząd ds. Zwalczenia Nadużyć Finansowych (OLAF) do celów bezpieczeństwa w jego siedzibie w Brukseli (sprawa 2007-634). Jest to pierwszy przypadek wśród opinii Inspektora dotyczący nadzoru wideo. Więcej informacji na ten temat zawiera sekcja 2.7.2.

Kontrola tożsamości i dostępu

Inspektor przyjął opinię na temat kontroli tożsamości i dostępu stosowanej przez OLAF (sprawa 2007-635). System ten jest częścią infrastruktury bezpieczeństwa chroniącej siedzibę, systemy informacji i technologii OLAF. System ten ma za zadanie kontrolę tożsamości oraz udzielanie lub odmowę dostępu osobom wchodzącym do siedziby OLAF i opuszczającym tę siedzibę poza godzinami pracy, a także a także dostępu do specjalnych stref zabezpieczonych. W tym celu OLAF stosuje karty typu „smart card” oraz weryfikację odcisków palców. Dane biometryczne użytkowników są przechowywane jedynie na karcie, której nie można używać w jakimkolwiek innym celu.

W ramach stosowanej przez OLAF kontroli dostępu Inspektor zinterpretował zasadę ograniczonego dostępu jako żądanie, by wyłącznie osoby potrzebujące specjalnego dostępu były wprowadzane do systemu i miały pobierane odciski palców. Inspektor zatem zalecił, by OLAF ponownie ocenił i rozważył możliwość ograniczenia wykazu osób, które muszą wprowadzić do systemu swoje odciski palców, na podstawie faktycznej potrzeby wejścia do urzędu poza godzinami pracy lub by wejść do specjalnie zabezpieczonych stref w urzędzie, lub korzystać z niestrzeżonych punktów dostępu (klatek schodowych) w celu wejścia do zabezpieczonych pomieszczeń OLAF.

OLAF zamierzał przechowywać zapisane dane (lub informacje z kontroli dostępu) przez okres nie dłuższy niż jeden rok do celów badania incydentów naruszenia bezpieczeństwa. Inspektor uznał, że może zaistnieć konieczność przechowywania danych rejestracyjnych przez pewien okres czasu umożliwiający zrekonstruowanie wydarzeń podczas incydentów naruszenia bezpieczeństwa oraz że w przypadku OLAF bardzo krótki okres może nie być praktyczny. Jednak Inspektor podkreślił, że OLAF powinien opracować proces wykrywania incydentów i reagowania na nie, tak by można je było ujawnić i zgłosić jak najszybciej po ich wystąpieniu. Zwrócił się także do OLAF o ponowne rozważenie okresu przechowywania poprzez przeanalizowanie potrzeby skrócenia go dzięki wykorzystaniu danych statystycznych dotyczących incydentów.

Inspektor wydał także opinię dotyczącą prowadzonego przez OLAF przetwarzania informacji osobowych, by zagwarantować, że do podstawowych technologii informatycznych OLAF mają dostęp wyłącznie uprawnione osoby i by umożliwić badanie incydentów naruszenia

bezpieczeństwa (podstawowy system informatyczny (CBIS)) (sprawa 2008-223). Weryfikacja w tym systemie jest oparta na certyfikatach cyfrowych i odciskach palców. Certyfikaty są przechowywane w osobistych identyfikatorach OLAF („smart cards”) użytkowników i chronione przez biometryczny system identyfikacji na karcie. Każdy użytkownik posiada trzy wzory odcisków palców przechowywane na identyfikatorze OLAF, który to identyfikator jest płaszczyzną kontaktową wykorzystywaną przez system weryfikacji CBIS.

W swojej opinii Inspektor przeanalizował w szczególności przestrzeganie zasady jakości danych. W tym celu przeprowadził dokładną analizę realizacji procedur awaryjnych w przypadku niewprowadzenia do systemu. Chociaż Inspektor uznał, że proponowane przez OLAF rozwiązanie minimalizuje ryzyko niewprowadzenia do systemu, taka możliwość nadal istnieje i jeżeli wystąpiłaby taka sytuacja, zaistniałaby także dyskryminacja. Inspektor zaproponował zatem, by OLAF opracował praktyczne rozwiązanie alternatywne na wypadek, gdyby wystąpił przypadek stałej niemożności wprowadzenia do systemu. Ponadto Inspektor przeanalizował sposób, w jaki określa się odsetek fałszywych odrzuceń i zalecił, by OLAF ustalił dokładny odsetek fałszywych odrzuceń, co odzwierciedlałoby przyjętą przezeń politykę bezpieczeństwa.

2.3.6. Konsultacje dotyczące potrzeby przeprowadzenia kontroli wstępnej

W 2008 roku liczba konsultacji dotyczących potrzeby przeprowadzenia kontroli wstępnej przez Inspektora pozostawała na stałym poziomie: 20 konsultacji w roku 2008 i 20 w roku 2007.

Kilka spraw określono jako podlegające kontroli wstępnej; są to:

- rekrutacja pracowników tymczasowych;
- publikacja punktów do awansu;
- naruszenia przepisów o ruchu drogowym
- dane biometryczne i kontrola dostępu.

Powiadomienia o niektórych operacjach przetwarzania nie zostały dotychczas oficjalnie przekazane Inspektorowi po jego informacjach zwrotnych o potrzebie kontroli wstępnej.

Uznano, że operacja przetwarzania w Radzie danych dotyczących naruszenia przepisów o ruchu drogowym podlega kontroli wstępnej, ponieważ obejmuje dane związane z wyrokami skazującymi

za przestępstwa lub podejrzeniami o popełnienie przestępstwa.

Operacje przetwarzania danych dotyczące danych biometrycznych i kontroli dostępu zostały uznane za podlegające kontroli wstępnej, gdy stosowane są systemy porównania biometrycznego. Faktycznie systemy te stanowią konkretne zagrożenie dla praw i wolności osoby, której dane dotyczą. Poglądy Inspektora są oparte głównie na charakterze danych biometrycznych, które to dane są niezwykle wrażliwe z racji pewnych nieodłącznych cech tego rodzaju danych. Na przykład, dane biometryczne nieodwracalnie zmieniają związek między ciałem a tożsamością, ponieważ czynią cechy charakterystyczne ciała ludzkiego czytelnymi dla urzędników i sprawiają, że cechy te można dalej wykorzystywać. Oprócz wysoce wrażliwego charakteru tych danych, Inspektor zauważa także, że możliwości powiązań oraz stan rozwoju narzędzi technicznych mogą stworzyć dla osób, których dane dotyczą, niespodziewane lub niepożądane skutki.

Stwierdzono, że operacja przetwarzania związana z dochodzeniem prowadzonym przez inspektora ochrony danych w Trybunale Sprawiedliwości nie podlega kontroli wstępnej. Faktycznie operacja ta nie ma na celu oceny postępowania danej osoby lub ustalenia jej odpowiedzialności. Oprócz tego przeprowadzona przez DPO ocena naruszenia przepisów rozporządzenia (WE) nr 45/2001 jest szerszą koncepcją niż podejrzenie o popełnienie przestępstwa, przestępstwo lub skazania. Fakt, że dane dotyczące podejrzeń o popełnienie przestępstwa, przestępstw lub skazania mogą się sporadycznie pojawić, nie zmienia zakresu operacji przetwarzania danych.

Sprawy dotyczące dostępu do poufnych dokumentów nie uznano za podlegającą kontroli wstępnej, ponieważ charakter oraz zakres operacji przetwarzania nie wchodzi w zakres zastosowania art. 27 rozporządzenia. W istocie, choć dane dotyczące stanu zdrowia, podejrzeń o popełnienie przestępstwa, przestępstw, skazania lub środków ochrony mogą pojawić się w tych poufnych dokumentach, to celem operacji przetwarzania nie jest przetworzenie tych danych, lecz jedynie rejestrowanie osób mających dostęp do tych dokumentów.

2.3.7. Powiadomienia niepodlegające kontroli wstępnej lub wycofane

W 2008 roku Inspektor zajmował się również 12 sprawami, które uznano za niepodlegające kontroli wstępnej (9,91 % spraw przedłożonych Inspektorowi). Takie wnioski wyciągnięto po przeprowadzeniu

starannej analizy powiadomień. Niemniej jednak wynikiem tej analizy były pewne zalecenia wystosowane przez Inspektora. Dwie z tych spraw dotyczyły obszaru telekomunikacji, dwie – kontroli dostępu, siedem⁽¹¹⁾ – personelu, a jedna – innych obszarów, takich jak zaawansowany system zapisów (ARES) i *wspólnej nomenklatury* (Nomcom).

Jeżeli chodzi o siedem spraw dotyczących personelu, jedna z nich dotyczyła zarządzania czasem⁽¹²⁾. Uznano ją za niepodlegającą kontroli wstępnej, ponieważ powiadomienie to było połączone z powiadomieniem głównym na temat systemu flexitime⁽¹³⁾ i nie było znaczących zmian odnoszących się do samego przetwarzania. Inspektor przekazał jednak zalecenia dotyczące okresu zatrzymywania danych.

Jeżeli chodzi o kontrolę dostępu, jedno z powiadomień⁽¹⁴⁾ przedłożono na mocy art. 27 ust. 2 lit. a) rozporządzenia (konkretne zagrożenie istnieje przy operacji przetwarzania danych dotyczących środków ochrony). Inspektor zinterpretował przedstawione w art. 27 ust. 2 lit. a) pojęcie „środków ochrony” jako nieodnoszące się do fizycznej ochrony budynków i personelu, lecz raczej jako środki podejmowane w stosunku do osób fizycznych w związku z procedurami karnymi (lub administracyjnymi) („*mesures de sûreté*” w języku francuskim).

Inspektor rozważył także to, czy inne aspekty przetwarzania powodują powstanie potrzeby kontroli wstępnej. W tym względzie znaczącym aspektem jest wykorzystywanie technologii identyfikacji radiowej (RFID). Inspektor uważa, że wykorzystywanie RFID bez żadnych elementów dodatkowych nie stanowi konkretnego ryzyka w rozumieniu art. 27 ust. 1. Nie oznacza to jednak, że nie należy zalecać wzorcowych rozwiązań w celu zagwarantowania prywatności i ochrony danych. Niemniej jednak przedstawiono zalecenia na temat dokładnego celu przetwarzania, opisu wewnętrznej kontroli dostępu,

⁽¹¹⁾ Identyfikacja banków i osób prawnych w EMCDDA (2008-168), operacje przetwarzania we FRA w związku z wypłatą wynagrodzeń (2008-396), procedura oceny w UHRW (2008-415 aktualizacja powiadomienia), zarządzanie personelem Komisji w JRD ITU w Karlsruhe (2008-151; wykorzystywanie bazy danych jest powiązane z odrębnymi operacjami przetwarzania, które nie zostały opisane dostatecznie szczegółowo w powiadomieniu), Komisja (Wspólne Centrum Badawcze w Karlsruhe) – system flexitime ZEUS (2008-486), kartoteki osobowe w CEDEFOP (2008-197) i system Superviseo wykorzystywany w biurze europejskiego rzecznika praw obywatelskich (2008-052; narzędzie to nie służy do przeprowadzania ocen).

⁽¹²⁾ Komisja – Wspólne Centrum Badawcze w Karlsruhe – system flexitime ZEUS (2008-486).

⁽¹³⁾ Komisja – system zarządzania czasem Sysper 2 (2007-063)/

⁽¹⁴⁾ CEDEFOP (2008-195)

informowania osób, których dane dotyczą, okresu zatrzymywania danych oraz technicznych środków ochrony.

Wśród 10 wycofanych spraw znajdowała się szczególnie sprawa pochodząca z Europejskiego Banku Inwestycyjnego (EBI) i związana z „osobami narażonymi na ryzyko pod względem politycznym” (sprawa 2007-543), którą należy wyeksponować. Pierwotnie Inspektor został powiadomiony w celu przeprowadzenia kontroli wstępnej obowiązującej w EBI procedury dotyczącej osób narażonych na ryzyko pod względem politycznym, którą to procedurę stworzono w celu przestrzegania dyrektywy 2005/60/WE w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu. Powiadomienie to następnie wycofano, ponieważ pierwotnie przewidziana ręcznie obsługiwana baza danych osób narażonych na ryzyko pod względem politycznym prawdopodobnie nie zostanie utworzona w przyszłości. Przewiduje się alternatywne metody monitorowania i zostaną one przekazane Inspektorowi do kontroli wstępnej w odpowiednim czasie.

Do czasu przyjęcia alternatywnych metod monitorowania przeprowadzane są kontrole z ramienia głównego urzędnika ds. przestrzegania w celu zapewnienia przestrzegania dyrektywy 2005/60/WE. Inspektor przedstawił zatem pewne zalecenia, zwłaszcza dotyczące okresów przechowywania i informacji, które należy przekazywać osobom, których dane dotyczą.

Jeżeli chodzi o okres przechowywania, EBI ustalił okres 15 lat, by oprócz ogólnych ograniczeń czasowych dotyczących pozwów cywilnych uwzględnić wnioski o dostęp od organów na całym świecie w związku z terroryzmem i innymi poważnymi przestępstwami wymienionymi w dyrektywie. Inspektor zwrócił się do EBI, by ten ponownie rozważył 15-letni okres przechowywania w związku z faktycznymi wnioskami o informacje wystosowanymi przez organy poszczególnych krajów.

Jeżeli chodzi o obowiązek informowania osób, których dane dotyczą, zgodnie z art. 11 i 12 rozporządzenia, Inspektor przyjął do wiadomości, że przekazywanie informacji każdej osobie narażonej na ryzyko pod względem politycznym mogłoby w niektórych przypadkach poważnie zakłócić i zniweczyć skuteczność działań EBI na mocy dyrektywy służących zapobieganiu praniu pieniędzy. W tym celu można stosować zwolnienia z obowiązku informowania przewidziane

w art. 20 ust. 1 lit. a), b) i c) rozporządzenia. Ponadto biorąc pod uwagę fakt, że w wielu przypadkach EBI nie posiada bezpośrednich ani umownych związków z danymi osobami, można także zastosować wyjątek przewidziany w art. 12 ust. 2. Inspektor był gotów zaakceptować – jako alternatywę dla informacji indywidualnych – zawiadomienie ogólne dotyczące procedur przetwarzania danych w stosunku do osób narażonych na ryzyko pod względem politycznym, które byłoby umieszczone na stronie internetowej EBI i publikowane w jego dokumentacji.

2.3.8. Dalsze działania po wydaniu opinii dotyczących kontroli wstępnej

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

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

Wszystkie sprawy dotyczące kontroli wstępnej skutkowały wydaniem zaleceń. Jak wyjaśniono powyżej (zob. sekcje 2.3.4 i 2.3.5), większość zaleceń dotyczy informacji przekazywanych osobom, których dane dotyczą, okresów przechowywania danych, ograniczenia celu oraz prawa dostępu i prawa do poprawy danych. Instytucje i organy chętnie stosują się do tych zaleceń i do tej pory

decyzje wykonawcze nie były potrzebne. Czas realizacji tych środków jest różny w poszczególnych przypadkach. W oficjalnym piśmie przesyłanym wraz z opinią Inspektor zwraca się do danej instytucji o informowanie go w terminie trzech miesięcy o środkach przedsięwziętych w celu realizacji zaleceń. W roku 2008 Inspektor zamknął 36 spraw, co stanowi prawie tę samą liczbę spraw co w roku 2007. Liczba ta powinna zwiększyć się w roku 2009, ponieważ uruchomiono lub ponownie przeprowadzono wiele działań następczych.

2.3.9. Wnioski i przyszłość

Tak jak w latach poprzednich kontrole wstępne, szczególnie kontrole wstępne *ex post*, stanowią bardzo ważne narzędzie nadzoru instytucji i organów wspólnotowych.

Wnioski dotyczące 2008 roku można podsumować w sposób następujący:

- rok 2008 był rokiem wyjątkowej pracy – wydano 105 opinii, więcej niż w roku 2007 (90 opinii);
- dokonano tego przy mniejszej liczbie dni na sporządzenie opinii oraz znacznie mniejszą liczbą potrzebnych dni dodatkowych;
- z drugiej strony, nastąpił niepokojący wzrost liczby dni zawieszenia potrzebnych do otrzymania informacji od administratorów danych lub inspektorów ochrony danych;
- uruchomiono nową procedurę kontroli wstępnej *ex post* operacji przetwarzania prowadzonych w agencjach, by ułatwić zarówno powiadamianie, jak i sporządzanie opinii, z zastosowaniem systematycznej metody podejścia według tematów;
- niektóre ważne kwestie zostały poruszone po raz pierwszy, np. usługa zarządzania tożsamością, kontrola dostępu przez skanowanie tęczówki lub potwierdzenie autentyczności przy użyciu odcisków palców, postępowania sprawdzające, monitorowanie korzystania z Internetu przez personel, system telewizji przemysłowej (CCTV) itd.

Przyszłe działania będą się koncentrować na następujących punktach:

- główne instytucje powinny zakończyć powiadomienia we wszystkich dziedzinach wchodzących w zakres zastosowania art. 27 rozporządzenia, a agencje powinny poczynić znaczące postępy w przestrzeganiu tego zobowiązania;
- należy znacznie zmniejszyć ilość czasu potrzebną do odpowiedzi na wystosowywane przez Inspektora dalsze zapytania o informacje, głównie przez sporządzanie powiadomień i załączników we właściwy sposób;
- w niektórych obszarach, takich jak nadzór wideo, nastąpi istotny postęp w wyniku stosowania nowej polityki ograniczającej kontrole wstępne do systemów odbiegających od „standardowych” praktyk przewidzianych w wytycznych (zob. sekcja 2.7);
- działania następcze w wyniku zaleceń będą kontynuowane, zarówno przez otrzymywanie informacji od administratorów danych (zob. sekcja 2.3.8), jak i przez kontrole (zob. sekcja 2.5).

2.4. Skargi

2.4.1. Wprowadzenie

Art. 41 ust. 2 rozporządzenia (WE) nr 45/2001 przewiduje, że Inspektor „jest odpowiedzialny za monitorowanie i zapewnienie zastosowania przepisów niniejszego rozporządzenia i każdego innego aktu wspólnotowego, odnoszącego się do podstawowych praw i wolności osób fizycznych, w odniesieniu do przetwarzania danych osobowych przez instytucje i organy wspólnotowe”. Elementem takiego monitorowania jest rozpatrywanie skarg zgodnie z art. 46 lit. a) ⁽¹⁵⁾.

Każda osoba fizyczna może wnieść skargę do Inspektora na podstawie art. 32 i 33 rozporządze-

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

nia, ⁽¹⁶⁾, niezależnie od narodowości czy miejsca zamieszkania. Skargi mogą także wnosić członkowie personelu instytucji i agencji europejskich, do których stosuje się regulamin pracowniczy, na podstawie art. 90 lit. b) regulaminu pracowniczego ⁽¹⁷⁾.

Skargi są dopuszczalne wyłącznie wtedy, gdy pochodzą od osoby fizycznej i dotyczą naruszenia zasad ochrony danych przez instytucję lub organ Wspólnoty w trakcie przetwarzania danych osobowych w ramach wykonywania działań, których całość lub część wchodzi w zakres prawa wspólnotowego. Jak zobaczymy poniżej, wiele skarg złożonych do Inspektora uznano za niedopuszczalne, ponieważ nie wchodziły one w obszar kompetencji Inspektora.

Każdorazowo gdy Inspektor otrzymuje skargę, przesyła on stronie skarżącej potwierdzenie odbioru bez przesądzania o dopuszczalności sprawy, chyba że bez potrzeby dalszej analizy widać, że skarga jest wyraźnie niedopuszczalna. Inspektor zwraca się też do skarżącego, by poinformował go o innych ewentualnych postępowaniach przed sądem krajowym, Trybunałem Sprawiedliwości Wspólnot Europejskich lub Europejskim Rzecznikiem Praw Obywatelskich (bez względu na to, czy postępowania te są w toku).

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

W przypadku domniemanego naruszenia przepisów dotyczących ochrony danych Inspektor może przekazać sprawę zainteresowanemu administratorowi danych i zaproponować środki mające na celu usunięcie tego naruszenia lub poprawę ochrony

⁽¹⁶⁾ Zgodnie z art. 32 ust. 2 „każdy podmiot danych może wnieść skargę do europejskiego inspektora ochrony danych, jeżeli uważa, że jego prawa wynikające z art. 286 Traktatu zostały naruszone w wyniku przetwarzania jego danych osobowych przez instytucję lub organ Wspólnoty”. Art. 33: „Każda osoba zatrudniona w instytucji lub organie Wspólnoty może złożyć skargę do europejskiego inspektora ochrony danych, dotyczącą domniemanego naruszenia przepisów [rozporządzenia (WE) nr 45/2001 ...], bez użycia oficjalnych dróg”.

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

osób, których dane dotyczą. W tym przypadku Inspektor może:

- nakazać administratorowi danych zastosowanie się do wniosków o wykonanie pewnych praw osoby, której dane dotyczą;
- ostrzec lub upomnieć administratora danych;
- nakazać sprostowanie, zablokowanie, usunięcie lub zniszczenie wszystkich danych;
- nałożyć zakaz przetwarzania;
- przekazać sprawę zainteresowanej instytucji wspólnotowej lub Parlamentowi, Radzie i Komisji.
- przekazać sprawę do Trybunału Sprawiedliwości ⁽¹⁸⁾.

Gdyby decyzja miała obejmować przyjęcie środków przez instytucję lub organ, Inspektor sprawdza wykonanie tego przez tę instytucję lub ten organ.

W 2008 roku Inspektor otrzymał 91 skarg. Jedynie 23 z nich zostały uznane za dopuszczalne i zostały poddane przez Inspektora dalszej analizie. Większość pozostałych skarg nie dotyczyła przetwarzania danych osobowych przez instytucję lub organ Wspólnoty, lecz odnosiła się wyłącznie do przetwarzania na szczeblu krajowym.

W roku 2008 rozwiązano 21 dopuszczalnych skarg. Poniżej przedstawiono krótką analizę niektórych z nich.

2.4.2. Sprawy uznane za dopuszczalne

Gromadzenie lub transfer nadmiernej ilości danych

Inspektor otrzymał skargę od członka personelu Komisji Europejskiej dotyczącą wymogu Komisji dotyczącego przedłożenia kompletnej belgijskiej deklaracji podatkowej małżonka członka personelu, by skontrolować jego uprawnienie do dodatkowego ubezpieczenia zdrowotnego (sprawa 2008-370). Po zbadaniu sprawy Inspektor stwierdził, że zakres tego wymogu jest nadmierny i niezgodny z zasadą dostateczności danych przedstawioną w art. 4 ust. 1 lit. b) i c) rozporządzenia. W następstwie przeprowadzonego przez Inspektora dochodzenia praktyki tej zaprzestano i Komisja gromadzi dane zawarte w belgijskiej deklaracji podatkowej wyłącznie w odniesieniu do dochodów z tytułu działalności zawodowej, a pozostałe źródła dochodów mogą pozostać nieujawnione.

Kolejną skargę otrzymano od komitetu pracowniczego i różnych pracowników UHRW w sprawie

⁽¹⁸⁾ Zob. art. 47 ust. 1 rozporządzenia (WE) nr 45/2001.

przetwarzania danych osobowych w ramach systemu kontroli jakości (sprawa 2008-0119). Skarżący zwrócili się do Inspektora, by zbadał tę sprawę i potwierdził, że:

- łączenie dwóch ewentualnych baz danych do celów innych niż historyczne, statystyczne lub naukowe nie ma wpływu na poszczególnych członków personelu;
- gromadzone dane są dostateczne i rzetelne;
- gromadzone dane rzeczywiście nie mają nadmiernego charakteru, uwzględniając liczne statystyki dotyczące wydajności oceniających dotychczas dostępne do celów oceny;
- gromadzone dane są dokładne;
- dane nie są przechowywane dłużej niż jest to konieczne.

Inspektor uznał, że skarga jest dopuszczalna zarówno w odniesieniu do przedstawicieli komitetu pracowniczego, jak i pracowników na podstawie art. 33 i 90 regulaminu pracowniczego oraz że Inspektor jest władny ją rozpatrzyć. Stwierdził on, że *a priori* nie wystąpiło naruszenie zasady jakości danych ani zasad dotyczących przechowywania danych.

Jednak badana procedura miała na celu ocenę jakości pracy wykonywanej przez oceniających i stanowi ona część procesu oceny. Inspektor zatem uznał, że procedura ta kwalifikuje się do kontroli wstępnej. Kontrola ta powinna normalnie odbyć się przed rozpoczęciem stosowania danej procedury, nawet jeśli procedura ta znajduje się dopiero w fazie testowej i działa przez okres kilku miesięcy. Stworzenie nowego systemu kontroli jakości bez powiadomienia Inspektora w celu przeprowadzenia przez niego kontroli wstępnej byłoby zatem naruszeniem przepisów rozporządzenia (WE) nr 45/2001. Zgodnie ze swoimi uprawnieniami przedstawionymi w art. 47 ust. 1 lit. b) tego rozporządzenia Inspektor zwrócił się do organu o powiadomienie o przetwarzaniu danych osobowych wynikającym z systemu kontroli jakości, by można było przeprowadzić kontrolę wstępną na mocy art. 27 ust. 1.

W innym przypadku osoba skarżąca twierdziła, że imiona i nazwiska wszystkich pracowników instytucji europejskich w Luksemburgu zostały przekazane przez Komisję Europejską do przedsiębiorstwa komunikacji autobusowej w mieście Luksemburg (sprawa 2008-421). Celem tej czynności było wydanie karty uprawniającej do darmowego korzystania z komunikacji autobusowej; na karcie nie widniałoby imię ani nazwisko, lecz tylko numer. Skarżący

twierdził, że rozwiązanie takie nie jest konieczne ani proporcjonalne oraz że narusza ono zasady ochrony danych.

Inspektor zbadał tę sprawę i stwierdził, że Komisja przesłała swoim pracownikom komunikat, w którym poinformowała ich o wszystkich niezbędnych elementach zgodnie z art. 11 i 12 rozporządzenia (WE) Nr 45/2001, zanim operacja przetwarzania miała miejsce. Osobom, których dane dotyczą, umożliwiono zaakceptowanie lub odrzucenie przekazania ich imion i nazwisk przedsiębiorstwu komunikacji autobusowej miasta Luksemburg. W rezultacie, w tym wypadku element zgody uzasadniał legalność przedmiotowego przekazania zgodnie z art. 5 lit. d) rozporządzenia. Ponadto Inspektor uznał, że inicjatywa Komisji polegająca na wydaniu nieodpłatnych biletów komunikacji autobusowej jest czynnością wykonywaną w interesie publicznym na podstawie regulaminu pracowniczego, w którym przewidziana jest możliwość świadczenia przez instytucje pewnych usług socjalnych służących pracownikom tych instytucji. Ten dodatkowy element uzasadniałby zatem legalność przekazania na mocy art. 5 lit. a) rozporządzenia.

Dostęp do danych

Pracownica Parlamentu Europejskiego złożyła skargę u Inspektora twierdząc, że dział zarządzania zwolnieniami chorobowymi w Parlamencie odmówił jej możliwości wykonywania prawa do dostępu i do poprawy danych w jej kartotece medycznej (sprawa 2007-681).

W swojej analizie prawnej Inspektor przedstawił m.in. nierestrykcyjną wykładnię art. 13 rozporządzenia (WE) nr 45/2001 i stwierdził, że skarżąca ma prawo nie tylko do uzyskania dostępu do swojej kartoteki medycznej, lecz także prawo do uzyskania odpisu lub fotokopii swoich danych medycznych bez ograniczeń w odniesieniu do liczby egzemplarzy. Jeżeli chodzi o jej prawo do poprawienia danych Inspektor podkreślił, że chociaż niemożliwe jest skorygowanie opinii medycznych, skarżąca powinna mieć prawo do aktualizowania swojej kartoteki medycznej, przez wprowadzanie do niej innych opinii medycznych. Jeżeli chodzi o wniosek skarżącej o przekazanie jej kartoteki medycznej wskazanemu przez nią lekarzowi, Inspektor stwierdził, że konieczność przekazania została wykazana przez jej wyraźną zgodę, co dowodziło także, że nie mogło tu dojść do naruszenia uzasadnionych interesów podmiotu danych.

Decyzja Inspektora w sprawie tej skargi była szczególnie interesująca dla działającego w Parlamencie Europejskim związku zawodowego SFIE, który wysłał pracownikom Parlamentu Europejskiego e-mail cytujący zalecenia Inspektora.

Kolejną skargę otrzymano w sprawie domniemanego naruszenia art. 13 rozporządzenia (WE) nr 45/2001 przez Komisję Europejską i Europejski Urząd Doboru Kadr (EPSO) przez odmowę dostępu do wyników uzyskanych w otwartym konkursie organizowanym przez EPSO (sprawa 2007-0250). Inspektor był zdania, że zgodnie z art. 13 rozporządzenia skarżący ma prawo dostępu do swoich wyników lub ocen uzyskanych w ramach otwartego konkursu EPSO podczas preselekcji, testów pisemnych i ustnych. Prawo to może podlegać pewnym ograniczeniom na mocy art. 20 ust. 1 lit. c) rozporządzenia. W szczególności może zająć potrzeba usunięcia lub ukrycia nazwisk pozostałych uczestników konkursu znajdujących się w zestawieniu porównawczym wyników testu oraz, w razie potrzeby, należałoby uniemożliwić identyfikację poszczególnych członków komisji selekcyjnej. Po interwencji Inspektora EPSO zgodziło się przekazać osobie, której dane dotyczą, żądane wyniki testów i sprawę zamknięto.

Interesującą skargę dotyczącą dostępu do „nieistniejących” danych odebrano od byłego pracownika Komisji Europejskiej (sprawa 2008-0438). Osoba ta skarżyła się na to, że w skierowanym do niej piśmie Komisja wspomniała badanie porównawcze zawierające dane osobowe tej osoby. Poproszona o przekazanie tego badania Komisja odmówiła twierdząc, że „badanie” to nigdy nie zostało zapisane i było oparte jedynie na ustnej konsultacji z ekspertem. Po zbadaniu faktów Inspektor stwierdził, że nie ma dowodów na istnienie tego badania, zatem nie istnieją żadne dane osobowe i nie ma możliwości uzyskania dostępu do nich.

Przetwarzanie danych szczególnie chronionych

Do Inspektora wpłynęła skarga byłego pracownika Komisji dotycząca niewłaściwej operacji przetwarzania danych dotyczących zdrowia w ramach administrowania ubezpieczeniem od wypadkowym (sprawa 2007-0521). Skarżący był zdania, że przekazano stronie trzeciej – bez dostatecznego

uzasadnienia konieczności takiego działania zgodnie z art. 10 ust. 2 lit. b) – szczególne kategorie danych osobowych, o których mowa w art. 10 ust. 1. Faktycznie Komisja przekazała informacje o osobie, której dane dotyczą dotyczące jej „wiedzy fachowej z zakresu psychiatrii”. Po przeanalizowaniu faktów Inspektor stwierdził, że Komisja nie miała powodów do ujawniania tej informacji.

Kolejna skarga wpłynęła od pracownika Komisji w związku z przetwarzaniem danych osobowych dotyczących jego życia seksualnego (sprawa 2007-459). Pracownik ten skarżył się także na przeciek tych danych do osób trzecich. Po zbadaniu sprawy Inspektor stwierdził, że:

- dane osobowe skarżącego zostały przetworzone bez podstawy prawnej;
- skarżącemu nie przekazano niezbędnych informacji dotyczących przetwarzania (ani przyczyn odroczenia ich przekazania);
- obowiązujące środki bezpieczeństwa nie są adekwatne do poziomu ryzyka przetwarzania i charakteru danych osobowych.

Ponadto Inspektor zwrócił się do właściwych służb Komisji o wprowadzenie środków służących zapobieganiu naruszeniom przepisów rozporządzenia (WE) nr 45/2001 w przyszłości. Po decyzji Inspektora Komisja zobowiązała się do podjęcia odpowiednich działań w celu przestrzegania przepisów tego rozporządzenia.

Złożono skargę na Komisję Europejską w związku z procedurą przyznawania miejsc parkingowych pracownikom niepełnosprawnym (sprawa 2007-611). Pracownik Komisji skarżył się, że szczególnie chronione dane dotyczące jego stanu zdrowia były przesyłane pocztą elektroniczną do różnych osób trzecich bez widocznego powodu. Po ocenie faktów Inspektor stwierdził, że istniała podstawa prawna do przekazania poczty elektronicznej innym osobom, by można było podjąć decyzję o przedłużeniu prawa do korzystania z miejsca parkingowego, ale dane medyczne powinny być zostać usunięte z e-maili wysłanych do niektórych odbiorców. Inspektor przekazał sprawę administratorowi danych i zwrócił się o usunięcie danych medycznych przez tych odbiorców, którzy otrzymali je omyłkowo.

W innej skardze domniemane naruszenie praw do ochrony danych wiąże się z działaniami podjętymi na podstawie wniosku o urlop specjalny z powodu poważnej choroby małżonka (sprawa 2007-602). Skarżący twierdził, że kierownik kadr przekazał lub przynajmniej pokazał dwa zaświadczenia lekarskie organowi powołującemu, naruszając tym samym art. 10 ust. 3 rozporządzenia.

Po uznaniu skargi za dopuszczalną Inspektor w swojej decyzji skupił się na fakcie, że dane dotyczące stanu zdrowia zostały przekazane organowi powołującemu bez zgody osoby, której dane dotyczą, i bez podstawy prawnej w Traktacie WE ani w akcie prawnym przyjętym na podstawie traktatów, co narusza art. 10 ust. 3 rozporządzenia.

Istotnie, przepisy wykonawcze dotyczące urlopów i zwolnień stanowią, że przy składaniu wniosku o urlop specjalny trwający do trzech dni osobie zarządzającej urlopami i zwolnieniami należy przekazać zaświadczenie lekarskie. Przepisy nie stanowią, że zaświadczenie to można przekazać organowi powołującemu. Interwencją tego organu przewiduje się wyraźnie wyłącznie w przypadkach chronicznych, poważnych schorzeń, kiedy to organ powołujący może udzielić przedłużenia na okres do trzech dni. Ponadto przepisy wykonawcze stanowią, że gdy dana osoba uważa, że informacje zawarte w zaświadczeniu lekarskim są poufne, zaświadczenie to można przekazać wyłącznie do służby medycznej, a osoba zarządzająca zwolnieniami otrzyma jedynie podstawowe informacje dotyczące zwolnienia. W rezultacie przepis ten wyraźnie wyklucza przekazywanie poufnych danych osobie zarządzającej zwolnieniami i wobec tego, *a fortiori* organowi powołującemu. W związku z brakiem służby medycznej w tym organie skarżący przekazał zaświadczenie lekarskie kierownikowi kadr, wyraźnie prosząc o zachowanie poufności. Późniejsze przekazanie takich danych organowi powołującemu nie miało zatem uzasadnienia w przepisach wykonawczych.

Inspektor poruszył także kwestię, że ponieważ procedura wnioskowania o urlop specjalny pociąga za sobą przetwarzanie danych dotyczących stanu zdrowia, procedurę tę należy przekazać Inspektorowi do kontroli wstępnej.

W innym przypadku skarżący twierdził, że przetwarzanie niektórych jego danych w ramach procedury

oceny przeprowadzanej w agencji, stanowi naruszenie art. 10 rozporządzenia (sprawa 2008-124). Dane przetwarzane przez urzędnika zajmującego się oceną tego pracownika były związane z jego zdrowiem (liczba dni zwolnień lekarskich), z działalnością zawodową jego małżonki oraz do faktu, że był on czynnym członkiem komitetu pracowniczego.

Jeżeli chodzi o dane dotyczące stanu zdrowia tego pracownika, Inspektor stwierdził, że dane te były stosowne w zakresie, w jakim były niezbędne do uwzględnienia faktycznego okresu spędzonego przez pracownika w pracy, co było potrzebne do oceny. Jeżeli chodzi o dane dotyczące działalności zawodowej małżonki skarżącego, Inspektor zwrócił uwagę, że informacje te nie są istotne z punktu widzenia ochrony danych. Jeżeli chodzi o członkostwo skarżącego w Komitecie Pracowniczym, Inspektor uznał, że takich danych nie obejmuje art. 10 ust. 1 rozporządzenia, który wyraźnie odnosi się do zakazu przetwarzania danych osobowych ujawniających członkostwo w związkach zawodowych, nie zaś członkostwo w Komitecie Pracowniczym. Zwrócono także uwagę, że dane te są ważne i nienadmierne do celów oceny, ponieważ czas poświęcony na tę działalność stanowi część godzin pracy, zatem jest to zgodne z art. 4 ust. 1 lit. c) rozporządzenia.

Prawo do poprawy danych

Inspektor otrzymał skargę urzędnika Komisji dotyczącą prawa do poprawy danych (sprawa 2008-0353). Skarżący przesłał kilka wniosków do różnych służb Komisji w celu skorygowania danych osobowych związanych z elastycznym czasem pracy w ramach systemu Sysper2. Komisja nie zareagowała na te wnioski. Po złożeniu przez pracownika skargi u Inspektora, dyrekcja ds. personelu i administracji skorygowała nieprawidłowe dane w odpowiedniej kartotece.

Obowiązek udzielania informacji

Osoba, której dane dotyczą, złożyła skargę na Komisję Europejską w związku z przetwarzaniem danych dotyczących ubezpieczenia wypadkowego (sprawa 2007-0520). Skarżący oświadczył, że dane go dotyczące uzyskane od niego i od stron trzecich zostały zgromadzone, przechowane i przekazane stronom trzecim bez informowania go o tym (art. 11 i 12 rozporządzenia). Podmiot danych skarżył się

także, że nie umożliwiono mu dostępu do wszystkich jego danych przetwarzanych przez Komisję. Ponadto skarżący twierdził, że Komisja przedstawiła jego zdaniem jego sprawę w sposób wybiórczy i tendencyjny, zatem pragnął on wykonać swoje prawo do korekty (art. 14 rozporządzenia).

Po oceniu sprawy Inspektor stwierdził, że administrator danych nie przestrzegał zobowiązań nałożonych na mocy art. 11 i 12 rozporządzenia, i odrzucił skargę z innych przyczyn.

Inspektor otrzymał kolejną skargę od byłego pracownika Europejskiej Agencji ds. Środowiska (EEA), w której pracownik przywoływał domniemane naruszenie przez agencję rozporządzenia (WE) nr 45/2001 – chodziło o nielegalne i nadmierne przekazywanie szczegółowych danych finansowych skarżącego między dwoma odbiorcami wewnętrznymi w agencji (sprawa 2007-0718).

Inspektor, po przeprowadzeniu niezbędnych dochodzeń, stwierdził, że chociaż przekazywanie danych finansowych skarżącego było niezbędne do celów planowania budżetu przedsięwzięcia, to agencja nie poinformowała skarżącego o jego prawach dotyczących przekazania zanim ono nastąpiło, zgodnie z art. 12 rozporządzenia. W swojej decyzji Inspektor zalecił zatem, by agencja wprowadziła specjalne przepisy dotyczące przekazywania danych wewnątrz agencji, przechowywania przekazywanych danych oraz informacji, jakie należy przekazać osobom, których dane dotyczą.

Publikacja w sprawozdaniu rocznym za rok 2005 – dalsza aktualizacja

W lipcu 2005 r. do Inspektora wpłynęła skarga przeciwko OLAF – odnosząca się do 2002 roku oraz początku 2004 roku – która dotyczyła różnych kwestii objętych rozporządzeniem (WE) nr 45/2001, zwłaszcza nierzetelnego przetwarzania danych osobowych oraz przekazywania przez OLAF nieprawidłowych danych dotyczących skarżącego w kontekście dochodzenia prowadzonego w sprawie jego domniemanego udziału w aferze łapówkarskiej (sprawa 2005-0190).

W grudniu 2005 r. zastępca Inspektora przyjął decyzję dotyczącą tej skargi. Zgodził się on wprawdzie, że zajęcie się tą skargą leżało w kompetencjach Inspektora w zakresie, w jakim dotyczyła ona kwestii objętych zakresem zastosowania rozporządzenia; uznał jednak, że Inspektor nie jest w stanie podjąć żadnych dalszych działań, które mogłyby

doprowadzić do pożądanej zmiany sytuacji. Sprawę tę skrótowo wspomniano w sprawozdaniu rocznym za rok 2005.

W 2006 roku skarżący złożył skargę do Europejskiego Rzecznika Praw Obywatelskich dotyczącą sposobu postępowania z jego pierwotną skargą. Strona skarżąca sprzeciwiła się również krótkiemu przedstawieniu tej sprawy w sprawozdaniu rocznym za rok 2005, stwierdzając, że było ono nieprawidłowe i przedwcześnie. Jeżeli chodzi o drugą skargę, Inspektor zgodził się przedstawić odpowiednią aktualizację sprawy wraz z prawidłowym i kompletnym opisem sprawy przedłożonej przez skarżącego. Aktualizację tę opublikowano w sprawozdaniu rocznym za rok 2007. Ponadto na podstawie decyzji Europejskiego Rzecznika Praw Obywatelskich dotyczącej drugiej skargi, do sprawozdania za rok 2005 w wersji dostępnej na stronie internetowej Inspektora dołączono odpowiednią notatkę.

Jeżeli chodzi o pierwszą skargę, w kwietniu 2008 roku Europejski Rzecznik Praw Obywatelskich stwierdził, że dalsza analiza zarzutów i twierdzeń skarżącego nie jest uzasadniona, i zamknął sprawę. W kolejnej uwadze przyjął do wiadomości fakt, że na podstawie art. 46 lit. a) i b) rozporządzenia (WE) nr 45/2001 Inspektorowi przysługuje pewien margines swobody w decydowaniu, w sprawie których skarg powinien przeprowadzić analizę i dochodzenie. Europejski Rzecznik Praw Obywatelskich stwierdził także, że właściwe i bardzo pomocne dla przyszłych skarżących byłoby przedstawienie przez Inspektora – w dokumencie dotyczącym polityki ogólnej – kryteriów lub wytycznych, które zamierza on stosować przy wykonywaniu swojego prawa do swobodnej decyzji przy rozpoczynaniu analiz i prowadzeniu dochodzeń w sprawie przedstawianych mu skarg. Sprawa ta zostanie podjęta w kontekście opracowywania wewnętrznego podręcznika rozpatrywania skarg oraz planowanej następnie publikacji informacji na temat głównych elementów tej procedury, wraz z informacją o dopuszczalności skarg, na stronie internetowej Inspektora (zob. sekcja 2.4.5).

2.4.3. Sprawy niedopuszczalne: główne przyczyny niedopuszczalności

Z 91 skarg otrzymanych w roku 2008 68 uznano za niedopuszczalne. Znakomita większość tych skarg nie dotyczyła przetwarzania danych osobowych przez instytucję lub organ WE, a odnosiła

się wyłącznie do przetwarzania danych na szczeblu krajowym. W niektórych z tych skarg zwracano się do Inspektora o ponowne przeanalizowanie stanowiska przyjętego przez krajowy organ ds. ochrony danych; takie działanie nie jest objęte mandatem Inspektora. Strony skarżące poinformowano, że Komisja Europejska będzie właściwa w przypadku, gdy dane państwo członkowskie nie wykonuje prawidłowo dyrektywy 95/46/WE.

Instytucje wspólnotowe i organy nie zaangażowane bezpośrednio

Jako przykład, Inspektor otrzymał dwie skargi dotyczące przetwarzania danych osobowych pracowników KE, chociaż przetwarzania nie dokonywała instytucja ani organ Wspólnoty, lecz związki zawodowe działające w tych instytucjach. Jeden z przykładów to pracownik skarżący się, że otrzymał informacje polityczne od związku zawodowego na swój biurowy adres poczty elektronicznej. W tym przypadku związek zawodowy korzystał z listy adresów poczty elektronicznej przekazanych przez instytucję. Skarga dotyczyła jednak tego, że związek zawodowy działał na mocy prawa krajowego i wykorzystał te informacje (sprawa 2008-724). Kolejny przykład dotyczy ujawnienia danych osobowych stronom trzecim przez związek zawodowy działający w KE. Również w tym przypadku Inspektor stwierdził, że rozporządzenie (WE) nr 45/2001 nie ma zastosowania, ponieważ związek zawodowy ten jest osobą prawną na mocy prawa krajowego (sprawa 2008-071). W związku z tym przekazano dane kontaktowe krajowych organów ds. ochrony danych, wraz z wyjaśnieniem powodów, dla których Inspektor nie jest organem właściwym do zajęcia się tą sprawą.

Naruszenia niezwiązane z przetwarzaniem danych osobowych

Wysoka liczba niedopuszczalnych skarg obejmowała także domniemane naruszenia dokonane przez instytucje i organy wspólnotowe, ale ich przedmiot okazał się być poza zakresem zastosowania rozporządzenia (WE) nr 45/2001. W rzeczywistości niektórzy skarżący usiłowali zweryfikować lub anulować indywidualne decyzje podjęte przez administrację KE dowodząc, że decyzje te zawierają pewne dane osobowe i że należy szanować ich prawo do poprawienia danych osobowych.

Inspektor uznał takie skargi za niedopuszczalne dlatego, że nawet jeśli decyzja administracji KE zawiera

dane osobowe, to nie oznacza to, że Inspektor jest władny prowadzić dochodzenie w sprawie skargi na taką decyzję. Skarga, by była dopuszczalna, musi wiązać się z przetwarzaniem danych osobowych jako takich, nie zaś z interpretacją danych osobowych, gdy dana instytucja wykonuje władzę dyskrecyjną.

Te same fakty są już badane przez inne organy

Inspektor zazwyczaj uznaje daną skargę za niedopuszczalną, gdy tę samą sprawę (te same okoliczności faktyczne) zbadał już sąd, Europejski Rzecznik Praw Obywatelskich lub podobne organy administracyjne. Jednym z przykładów był przypadek pracownika skarżącego się na niezastosowanie rozporządzenia (WE) nr 45/2001 do dochodzenia administracyjnego prowadzonego przez organ wspólnotowy. Dochodzenie to przeprowadzono w celu ustalenia faktów dotyczących kontrowersji na temat domniemanego nieuprawnionego dostępu do komputerowej skrzynki pocztowej skarżącego. Po dochodzeniu administracyjnym nastąpiło postępowanie dyscyplinarne, które nadal toczyło się w chwili przesłania skargi. Ponadto, skarżący złożył podobną skargę na ręce Europejskiego Rzecznika Praw Obywatelskich.

Według Inspektora przedwczesne byłoby zajmowanie jakiegokolwiek stanowiska w kwestii niezastosowania rozporządzenia przed przekazaniem przez administrację wniosków końcowych z postępowania dyscyplinarnego. Badanie sprawy przez Inspektora spowodowałoby także dublowanie procedur z Europejskim Rzecznikiem Praw Obywatelskich.

2.4.4. Współpraca z Europejskim Rzecznikiem Praw Obywatelskich

Zgodnie z art. 195 Traktatu WE Europejski Rzecznik Praw Obywatelskich jest uprawniony do przyjmowania skarg, które dotyczą przypadków niewłaściwego administrowania w działaniach instytucji lub organów wspólnotowych. Kompetencje Europejskiego Rzecznika Praw Obywatelskich i Inspektora są zbieżne w dziedzinie rozpatrywania skarg w tym sensie, że przypadki niewłaściwego administrowania mogą dotyczyć przetwarzania danych osobowych. W związku z tym skargi wnoszone do Rzecznika Praw Obywatelskich mogą obejmować kwestie ochrony danych. Podobnie, skargi wnoszone do Inspektora

mogą dotyczyć skarg, które były już, w części lub w całości, przedmiotem decyzji Rzecznika Praw Obywatelskich.

Aby uniknąć zbędnego powielania pracy i zapewnić spójne podejście zarówno do ogólnych, jak i szczególnych kwestii ochrony danych zgłaszanych przez strony skarżące, w listopadzie 2006 roku podpisano protokół ustaleń między Europejskim Rzecznikiem Praw Obywatelskich a Inspektorem. W praktyce powyższy protokół w każdym stosownym przypadku skutkuje użyteczną wymianą informacji między Inspektorem a Europejskim Rzecznikiem Praw Obywatelskich.

Europejski Rzecznik Praw Obywatelskich konsultował się z Inspektorem w sprawach dotyczących ochrony danych i informował go o swoich decyzjach związanych ze sprawami, które również wpłynęły do Inspektora lub miały wpływ na kwestie ochrony danych. W przypadku jednej ze skarg, kiedy to skarżący postanowił także złożyć skargę do Europejskiego Rzecznika Praw Obywatelskich, wyniki dochodzenia przeprowadzonego przez Inspektora zostały przesłane Europejskiemu Rzecznikowi Praw Obywatelskich, aby uniknąć powielania działań.

2.4.5. Dalsze prace w dziedzinie skarg

Inspektor kontynuował prace nad przygotowaniem wewnętrznego podręcznika rozpatrywania skarg przez jego personel. Główne elementy procedury i wzór formularza do składania skarg, wraz z informacjami na temat dopuszczalności skarg, zostaną udostępnione na stronie internetowej Inspektora w 2009 roku. Oczekuje się, że publikacja ta pomoże potencjalnym skarżącym w składaniu skarg, jednocześnie ograniczając liczbę wyraźnie niedopuszczalnych skarg i dostarczając Inspektorowi bardziej kompletnych i aktualnych informacji, które powinny ułatwiać rozpatrywanie skarg.

2.5. Polityka w zakresie kontroli

2.5.1. Wiosna 2007 roku i okres późniejszy

Zgodnie z art. 41 ust. 2 rozporządzenia (WE) 45/2001 Inspektor jest odpowiedzialny za monitorowanie i zapewnienie stosowania tego rozporządzenia. W marcu 2007 roku Inspektor zainicjował procedurę pod nazwą „wiosna 2007”, której celem była ocena przestrzegania rozporządzenia w różnych instytucjach i agencjach oraz podsumowanie osiągniętych do tego czasu postępów.

Na pierwszym etapie tego działania rozpoczętego w 2007 roku do dyrektorów instytucji i agencji wystosowano pisma, których celem było sprawdzenie poziomu przestrzegania wspomnianego rozporządzenia. Dotyczyły one czterech zagadnień, mianowicie: statusu inspektora ochrony danych (DPO); spisu operacji przetwarzania danych, w ramach których przetwarzano dane osobowe; spisu operacji przetwarzania danych objętych zakresem art. 27 rozporządzenia, a także dalszego wdrażania rozporządzenia jako takiego. W ramach omawianego działania zobowiązano agencje, które jeszcze nie powołały swojego DPO, by obsadziły to stanowisko oraz do zajęły się kwestią zasobów i personelu niezbędnych do pełnienia przez DPO swoich obowiązków. Zachęcono również agencje i instytucje do wskazania operacji przetwarzania danych obejmujących dane osobowe oraz do ustalenia, które z tych operacji podlegają przeprowadzeniu kontroli wstępnej przez Inspektora. Wspomniane działanie skłoniło instytucje i agencje do nadrobienia zaległości w zakresie kontroli wstępnej *ex post*, co spowodowało ogromny wzrost liczby spraw przedłożonych Inspektorowi do kontroli wstępnej w 2007 roku.

Na podstawie informacji zwrotnych otrzymanych od instytucji i agencji Inspektor sporządził ogólne sprawozdanie dotyczące poziomu przestrzegania rozporządzenia. Sprawozdanie to upubliczniono w maju 2008 roku i przesłano je do wszystkich instytucji i agencji.

Jak zapowiedziano, wspomniana operacja zapoczątkowała prowadzone obecnie przez Inspektora działania mające zapewnić przestrzeganie rozporządzenia; działanie to wiąże się z ewentualnymi kontrolami na miejscu oraz regularnym wysyłaniem przez Inspektora wniosków o informacje do dyrektorów instytucji i agencji z myślą o ocenie dalszych postępów osiągniętych w tej dziedzinie. Jeśli chodzi o wymianę informacji, w październiku 2008 roku wysłano pisma z prośbą o kolejne uaktualnienie informacji na temat sytuacji w agencjach i instytucjach. Poruszono w nich dodatkowe zagadnienia dotyczące dalszego wdrażania rozporządzenia; odnosiły się one w szczególności do korzystania z własnych praw przez osoby, których dane dotyczą, a także liczby skarg wnoszonych do DPO. Odpowiedzi na te wnioski oczekiwano w grudniu 2008 roku; posłużą one do sporządzenia kolejnego sprawozdania wiosną 2009 roku.

2.5.2. Kontrole

Inspektor rozpoczął ostatnio dopracowywanie swojej polityki w zakresie kontroli. Wcześniejsze doświadczenia wynikające z dochodzeń przeprowadzonych w odpowiedzi na skargi oraz z działania „wiosna 2007” sprawiły, że konieczne stało się usystematyzowanie działalności kontrolnej Inspektora wynikającej z uprawnień nadanych mu na mocy różnych artykułów rozporządzenia (WE) nr 45/2001.

Kontrole są zasadniczym narzędziem stosowanym przez Inspektora jako organ nadzoru; pozwalają mu one monitorować i zapewniać stosowanie przepisów zawartych w rozporządzeniu (art. 41 ust. 2 i art. 46 lit. c)). Szerokie uprawnienia umożliwiające Inspektorowi dostęp do wszelkich informacji i danych osobowych niezbędnych do jego dochodzeń oraz do wszelkich pomieszczeń, w których administrator, instytucja lub organ Wspólnoty prowadzą swoją działalność, mają na celu zapewnienie mu skutecznych środków wykonywania jego funkcji publicznej (art. 47 ust. 2 rozporządzenia). Inspektor może przeprowadzać kontrolę w wyniku otrzymania skargi lub z własnej inicjatywy (art. 46 lit. a) i b) rozporządzenia).

Od instytucji i organów europejskich wymaga się, by współpracowały z Inspektorem, gdy ten będzie wykonywał swoje obowiązki, oraz by dostarczały mu żądane informacje i zapewniały niezbędny dostęp (art. 30 rozporządzenia).

Podczas kontroli Inspektor weryfikuje fakty i rzeczywistą sytuację na miejscu z myślą o tym, by zapewnić przestrzeganie rozporządzenia w instytucjach i organach Wspólnoty. Kontrole mogą ponadto w dużej mierze przyczynić się do poszerzenia wiedzy na temat dotyczące ochrony danych w kontrolowanych instytucjach, a także stanowić wsparcie dla pracy inspektorów ochrony danych.

W 2008 roku Inspektor określił pierwszą kompleksową procedurę mającą zastosowanie w jego działaniach kontrolnych prowadzonych w ramach nadzoru. Procedura ta miała trzy etapy:

- na pierwszym etapie przeprowadzono dwie wizyty próbne, po to by przetestować metodologię Inspektora *in situ*;
- w drugim etapie Inspektor dopracował swoją praktyczną metodologię;
- w trzecim etapie przeprowadzono dwie kontrole w instytucjach europejskich wybranych w ramach działania „wiosna 2007”.

„Wizyty próbne”

Wspomniane kontrole na miejscu miały zasadniczo podwójny cel: oprócz przetestowania metodologii Inspektora w zakresie kontroli zamierzano sprawdzić rzeczywiste przestrzeganie rozporządzenia w niektórych wybranych dziedzinach. W kilku przypadkach wiązało się to z wydaniem przez Inspektora zaleceń służących poprawie poziomu ochrony danych w wizytowanych służbach. W przypadkach tych w określonym terminie administratorzy mieli przekazać informacje zwrotne.

Rada Unii Europejskiej

W lipcu 2008 roku przeprowadzono trzy kontrole w siedzibie Rady Unii Europejskiej (sprawa 2008-359). Oprócz planowanego dopracowania praktycznej metodologii kontroli Inspektor sprawdził dwie operacje przetwarzania danych i przeprowadził rozmowy z w dyrekcji.

Podczas pierwszej wizyty Inspektor zweryfikował niektóre elementy zawarte w powiadomieniu skierowanym do DPO (stanowiące wyciąg z rejestru DPO) odnoszące się do przetwarzania danych osobowych przy określaniu uprawnień pracowników w momencie obejmowania przez nich obowiązków (w języku francuskim: *fixation du droits*). Administratorzy poinformowali już Inspektora o krokach, które podjęto w odpowiedzi na zalecenia wydane przez niego w następstwie wizyty.

Kolejna wizyta – w dyrekcji zajmującej się systemem informacji i komunikacji – miała na celu ustalenie, jakie środki zostały przedsięwzięte przez administratora, po to by zapewnić powiadamianie inspektora ochrony danych o operacjach przetwarzania danych (art. 25 rozporządzenia). Inspektor będzie śledził postępy w tej dziedzinie; zwrócił się także o przesłanie informacji na temat wyznaczenia osoby, która będzie odpowiadać we wspomnianej dyrekcji za kontakty w kwestiach dotyczących ochrony danych, oraz informacji związanych ze stanem powiadomień.

Trzecie działanie obejmowało operację przetwarzania danych, która została już wstępnie skontrolowana przez Inspektora. Personel Inspektora sprawdził operacje przetwarzania danych w ramach procedury naboru stażystów (sprawa 2007-217), a także wykonanie zaleceń Inspektora. Administrator poinformował już Inspektora o wykonaniu niektórych jego zaleceń wydanych po przeprowadzonej wizycie. Nadal nie rozstrzygnięto jednak kilku kwestii.

OLAF

W październiku 2008 roku personel Inspektora przeprowadził wizytę na miejscu w siedzibie OLAF; miała ona na celu dalsze dopracowanie praktycznej metodologii Inspektora w zakresie kontroli. Jej celem było również stwierdzenie stanu faktycznego, jeżeli chodzi o środki przedsięwzięte przez OLAF, po to by zapewnić wykonanie niektórych zaleceń przedstawionych w opinii Inspektora na temat wewnętrznych dochodzeń OLAF-u, którą wydał on na podstawie kontroli wstępnej (sprawa 2005-418).

Wizyta Inspektora (sprawa 2008-488) koncentrowała się na kilku elementach, które są istotne z punktu widzenia ochrony danych, w szczególności na praktyce polegającej na identyfikowaniu pewnych kategorii osób, których dane dotyczą, w karcie „osoby” w systemie zarządzania sprawami (CMS) OLAF-u. Personel Inspektora uzyskał również dostęp do wybranych spraw OLAF-u w jego systemie zarządzania sprawami, po to by sprawdzić powiadomienia wysłane osobom, których dane dotyczą, praktykę odraczania obowiązku informowania oraz transfery danych osobowych w związku ze sprawami wybranymi do celów wizyty. Ponadto Inspektor prosił o informacje na temat przewidzianego powiadamiania inspektora ochrony danych z OLAF – w przypadkach gdy chodzi o pocztę elektroniczną lub dokumenty natury osobistej – w kontekście stosowanego przez OLAF protokołu standardowych procedur operacyjnych dotyczących prowadzenia sądowego badania komputerów.

W informacji zwrotnej przekazanej OLAF-owi po wizycie Inspektor pozostał przy swojej wcześniejszej opinii na temat zbadanych dziedzin. Należy wypełniać obowiązek informowania, a jeżeli przekazanie informacji zostało odroczone, należy to odnotować w aktach. W przypadku transferu danych osobowych należy przekazywać powiadomienia. Inspektor zachęcił OLAF do zajęcia się praktyką ustnych przekazów danych. Zalecił OLAF-owi wykorzystywanie karty „osoby” do identyfikowania w systemie CMS osób, których dane dotyczą, gdyż jest to pożyteczne narzędzie umożliwiające właściwe wypełnianie innych obowiązków.

Jako że protokół OLAF-u dotyczący sądowego badania komputerów jest nadal w fazie projektu, Inspektor zachęcił ten urząd do tego, by podjął niezbędne kroki w celu przyjęcia protokołu jako dokumentu OLAF-u i rozpoczął wprowadzanie go w życie.

Ogólnie Inspektor zachęcił OLAF do sporządzenia projektu standardowych oświadczeń lub powiadomień o ochronie danych, z których mogłyby korzystać osoby zajmujące się poszczególnymi sprawami i które mogłyby umieszczać w sporządzanych *na bieżąco* dokumentach. Ponadto pokreślił, że konieczne jest podjęcie niezbędnych kroków, by uruchomić cały moduł ochrony danych, po to by wypełnić obowiązki przewidziane w rozporządzeniu (WE) nr 45/2001.

Dopracowanie praktycznej metodologii

Dzięki wspomnianym dwóm wizytom próbnym Inspektor miał możliwość dopracowania wewnętrznego podręcznika kontroli oraz sporządzenia aktualnej wersji wytycznych polityki w zakresie kontroli.

Podręcznik kontroli stanowi praktyczny przewodnik dla członków personelu Inspektora, którzy zajmują się nadzorem i którzy wchodzi w skład zespołu prowadzącego kontrole. Zawiera on opis procedur administracyjnych, zadań inspektorów, standardowe formularze umożliwiające sporządzanie dokumentów z kontroli, a także mówi o polityce bezpieczeństwa do celów kontroli. W podręczniku wyjaśniono cele wspomnianych dokumentów i przedstawiono porady przydatne przy przygotowywaniu kontroli. W miarę wypracowywania praktyk stosowanych przez Inspektora i w miarę zdobywania przez niego doświadczeń w aktualnej wersji podręcznika wprowadza się zmiany. Podręcznik zostanie oficjalnie przyjęty w 2009 roku; następnie co roku będzie poddawany przeglądowi, a w razie konieczności – aktualizowany.

Przed przeprowadzeniem kontroli do instytucji i organów wysyłana jest aktualna wersja wytycznych polityki w zakresie kontroli. Wytyczne, po ich doprecyzowaniu, zostaną opublikowane na stronie internetowej Inspektora. Opisano w nich między innymi główne kroki podejmowane w ramach procedury kontroli, podstawę prawną kontroli, uprawnienia Inspektora oraz rolę, jaką podczas kontroli odgrywają inspektorowie ochrony danych.

Kontrole dotyczące działania „wiosna 2007”

W maju 2008 roku Inspektor wybrał do skontrolowania trzy instytucje i jedną agencję; wybór ten opierał się przede wszystkim na wnioskach zebranych w toku działania „wiosna 2007”. Przeprowadzono dwie kontrole – w listopadzie i grudniu 2008 roku – a dwie kolejne zaplanowano na początek 2009 roku.

Europejski Komitet Ekonomiczno-Społeczny

W listopadzie 2008 roku Inspektor przeprowadził kontrolę w Europejskim Komitecie Ekonomiczno-Społecznym (EKES) (sprawa 2008-574). Celem kontroli było sprawdzenie stanu faktycznego, jeśli chodzi o środki podejmowane przez Komitet w celu przestrzegania rozporządzenia w dwóch zasadniczych dziedzinach:

- status spisu prowadzonego przez DPO oraz spoczywający na administratorach obowiązek powiadamiania DPO o operacjach przetwarzania danych osobowych (art. 25 rozporządzenia);
- operacje przetwarzania danych dotyczących zarządzania wnioskami o płatny staż (sprawa 2005-297) oraz przetwarzanie danych osobowych przez służbę medyczną (sprawa 2007-0004). Obie operacje przetwarzania danych zostały wcześniej poddane wstępnej kontroli Inspektora, który zalecił administratorom poprawę poziomu ochrony danych osobowych.

Spis i powiadomienia: kontrolerzy z biura Inspektora przeprowadzili rozmowy z administratorami, którzy nie przedłożyli jeszcze inspektorowi ochrony danych ostatecznego powiadomienia dotyczącego przetwarzania danych, aby poznać przyczyny takiej sytuacji, środki zastosowane w celu zapewnienia dalszych postępów w tej dziedzinie, a także przewidziany termin powiadomienia DPO.

Zarządzanie wnioskami o płatny staż: kontrolerzy z biura Inspektora weryfikowali i analizowali pewne elementy wniosku elektronicznego oraz akt papierowych, między innymi: dokumenty (informacje) zebrane od osób, które złożyły wniosek, na różnych etapach procesu składania wniosków, informacje przetworzone we wniosku elektronicznym, praktyki zatrzymywania danych, środki bezpieczeństwa w odniesieniu do akt papierowych, wymagane informacje na temat roli doradcy ds. stażu i jego dostępu do informacji, a także wymagane informacje na temat oświadczenia o ochronie danych osobowych.

Przetwarzanie danych przez służbę medyczną EKES: kontrolerzy zbadali między innymi praktyki stosowane przez służbę medyczną EKES od czasu rozdzielenia służb medycznych EKES i KR, skontrolowali środki bezpieczeństwa dotyczące akt papierowych, zwrócili się o informacje na temat obowiązku zachowania tajemnicy służbowej przez personel nielekarski, sprawdzili ewentualne informacje dotyczące stanu zdrowia, jakie lekarz EKES może otrzymać, w przypadku gdy pracownik

decyduje się na wizytę lekarską u wybranego przez siebie lekarza, pytali o praktyki dotyczące: przedkładania *note d'honoraires* i prawa dostępu do własnych danych przez osoby, których dane dotyczą, a także sposobów informowania tych osób.

Po przeprowadzonej kontroli Inspektor przekazał szczegółowe informacje zwrotne i oczekuje, że w niektórych skontrolowanych dziedzinach poczynione zostaną dalsze postępy.

Europejski Urząd ds. Bezpieczeństwa Żywności

W grudniu 2008 roku kontrolerzy z biura Inspektora przeprowadzili kontrole w siedzibie Europejskiego Urzędu ds. Bezpieczeństwa Żywności (2008-575). Celem tej kontroli było sprawdzenie środków przedsięwziętych przez EFSA w celu przestrzegania rozporządzenia w następujących głównych dziedzinach:

- spoczywający na administratorach obowiązek powiadamiania inspektora ochrony danych (DPO) o operacjach przetwarzania danych osobowych (art. 25 rozporządzenia);
- sprawdzenie operacji przetwarzania danych osobowych dotyczących polityki szkolenia personelu, które zawarte są w spisie, lecz o których jeszcze nie powiadomiono;
- sprawdzenie stosowania się do zaleceń Inspektora sformułowanych w opinii z kontroli wstępnej pt. „Rozwój kariery i cykl ocen”(2007-585) (art. 27 rozporządzenia).

W odniesieniu do działania „wiosna 2007” Inspektor pytał również o procentowe wydłużenie czasu pracy DPO oraz zwiększenie wsparcia administracyjnego i sekretarskiego, jakim dysponuje DPO.

Wnioski z kontroli zostaną przekazane EFSA na początku 2009 roku.

Podsumowanie

Podczas wspomnianych kontroli Inspektor skoncentrował się na różnych aspektach, takich jak sprawdzenie stanu spisu prowadzonego przez DPO oraz powiadomień kierowanych do DPO (był to jeden z elementów, o które pytano w działaniu „wiosna 2007”), sprawdzenie konkretnych operacji przetwarzania danych pochodzących z prowadzonego przez DPO spisu lub rejestru, a także weryfikacja konkretnych reakcji na zalecenia wydane przez Inspektora w opiniach z kontroli wstępnych.

Pierwsze doświadczenia z kontroli pokazują, że są one nie tylko użytecznym sposobem badania

faktycznej sytuacji w instytucjach i organach Wspólnoty, lecz także narzędziem służącym poszerzaniu wiedzy. Przy okazji tych kontroli Inspektor spotkał się z wieloma administratorami, którym wyjaśnił ich obowiązki na mocy z rozporządzenia (WE) 45/2001. Dzięki rozmowom z różnymi zainteresowanymi stronami oraz ocenie poczynionych postępów Inspektora uzyskał jasny obraz współpracy między administratorami a DPO. Pod tym względem kontrole można dodatkowo postrzegać jako środek wspierający pracę DPO.

2.6. Środki administracyjne

W art. 28 ust. 1 rozporządzenia (WE) nr 45/2001 przewidziano, że Inspektor ma prawo do uzyskiwania informacji o środkach administracyjnych, które dotyczą przetwarzania danych osobowych. Na wniosek instytucji lub organu albo z własnej inicjatywy Inspektor może wydać opinię. Termin „środki administracyjne” oznacza wydaną przez administrację decyzję ogólnego zastosowania dotyczącą przetwarzania danych osobowych przez daną instytucję lub dany organ. Mogą to być przyjęte przez administrację środki wykonawcze do rozporządzenia, przepisy wewnętrzne lub polityki ogólnego zastosowania dotyczące przetwarzania 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 Inspektor doradza instytucjom i organom Wspólnoty w konkretnych przypadkach związanych z przetwarzaniem danych lub w kwestiach ogólnych dotyczących interpretacji rozporządzenia.

W ramach konsultacji w sprawie środków administracyjnych⁽¹⁹⁾ planowanych przez instytucje i organy wspólnotowe poruszono rozmaite trudne zagadnienia; były wśród nich na przykład:

- nowy wzór zaświadczenia lekarskiego,
- dostęp do dokumentów zawierających dane osobowe,
- przepisy mające zastosowanie do niektórych działań związanych z przetwarzaniem danych,

⁽¹⁹⁾ Nawet jeżeli konsultacje przeprowadzane na podstawie art. 28 ust. 1 i art. 46 lit. d) częściowo pokrywają się lub częściowo różnią się od siebie, w kontekście niniejszego sprawozdania jedne i drugie nazywa się „konsultacjami w sprawie środków administracyjnych”.

- przekazywanie akt medycznych do sądów krajowych,
- zatrzymywanie danych o karach dyscyplinarnych związanych z danymi,
- przepisy wykonawcze do rozporządzenia (WE) nr 45/2001 przyjęte przez Trybunał Sprawiedliwości,
- skargi rozpatrywane przez Europejskiego Rzecznika Praw Obywatelskich.

2.6.1. Nowy wzór zaświadczenia lekarskiego

Międzyinstytucjonalne Kolegium Medyczne (IMB) przedłożyło Inspektorowi projekt nowego wzoru zaświadczenia stwierdzającego niezdolność do pracy w związku z chorobą lub wypadkiem. Nowy wzór zaświadczenia ma na celu uproszczenie i zmodernizowanie służby medycznej Komisji oraz zapewnienie korzyści personelowi (tj. będzie on dostępny w intranecie i będzie można z niego korzystać w razie potrzeby przy okazji wizyt lekarskich).

Inspektor zalecił między innymi, by ponownie przeanalizowano w świetle zasady adekwatności i istotności treść danych medycznych zawartych we wzorze zaświadczenia. Zalecił ponadto sporządzenie noty informacyjnej zawierającej określone informacje dotyczące przetwarzania danych oraz wyczerpujące informacje na temat praw dostępu do danych i ich poprawiania, a także ich przechowywania zgodnie z art. 11 i 12 rozporządzenia. Informacje te powinny się również znaleźć na odwrocie zaświadczenia lekarskiego, tak by zarówno pacjenci, jak i lekarze znali swoje prawa (sprawa 2008-312).

2.6.2. Dostęp do dokumentów

Inspektor ochrony danych (DPO) Komisji Europejskiej skonsultował się z Inspektorem w sprawie wniosku o dostęp do dokumentów zawierających dane osobowe, które wydawały się istotne w kontekście jednej ze spraw zawisłych przed sądem krajowym.

Komisja początkowo odmówiła udzielenia wnioskodawcy informacji na temat zatrudnienia pewnej osoby w Komisji, mianowicie, czy osoba ta jest

zatrudniona w odnośnej Dyrekcji Generalnej w pełnym wymiarze godzin i czy pracowała w Komisji w określonych przedziałach czasu.

Komisja powołała się na art. 8 rozporządzenia (WE) nr 45/2001 i stwierdziła, że:

- wnioskodawca, nie był w stanie uzasadnić konieczności przekazania takich danych;
- istnieje ryzyko naruszenia dóbr osoby, której dane dotyczą, gdyż nie wyraziła ona zgody na ujawnienie danych i wnikanie się w spór.

Osoba, która zwróciła się z wnioskiem o dostęp do dokumentów, złożyła jednak skargę do Europejskiego Rzecznika Praw Obywatelskich. Europejski Rzecznik Praw Obywatelskich przyjął propozycję polubownego rozwiązania sprawy, sugerując „by Komisja ponownie rozważyła zakwestionowaną odmowę i dostarczyła powodowi dokumenty/informacje [...], o które bez powodzenia prosił, chyba że poda uzasadnione i należyte powody, by tego nie czynić”.

Jako że informacje, których dotyczył wniosek, zawierały dane osobowe, sprawdzono, czy zastosowanie ma wyjątek przewidziany w art. 4 ust. 1 lit. b) rozporządzenia (WE) nr 1049/2001. Aby ocenić, czy w omawianym przypadku zostanie naruszona prywatność danej osoby, Inspektor zastosował metodologię opisaną w jego opracowaniu na temat „Publicznego dostępu do dokumentów i ochrony danych”⁽²⁰⁾. Uznał, że nie podano mu ani sam nie dostrzega żadnych stosownych dowodów na to, by prywatność i integralność osoby, której dane dotyczą, miałyby być zagrożona, i w każdym przypadku, by interes polegający na ochronie danych tej osoby w omawianej sprawie nie miał być podporządkowany interesowi publicznego dostępu do dokumentów. W związku z tym Inspektor uznał, że nie ma powodów, by odmówić takiego dostępu w świetle art. 4 ust. 1 lit. b) rozporządzenia (WE) nr 1049/2001 (Sprawa 2008-427).

2.6.3. Szczególne kategorie danych: prawo właściwe

DPO Agencji Praw Podstawowych Unii Europejskiej (FRA) skonsultował się z Inspektorem w sprawie operacji przetwarzania danych obejmujących pulę zainteresowanych osób z państw

członkowskich Unii Europejskiej, które wyraziły wolę udziału w badaniach sondażowych dotyczących praw podstawowych, takich jak badanie dotyczące dyskryminacji oraz ofiar przestępstw kryminalnych wśród wybranych grup imigrantów oraz innych mniejszości. Agencja Praw Podstawowych UE zawarła umowę z wykonawcą zewnętrznym. Jednym z celów tej umowy było zebranie szczególnych kategorii danych, przede wszystkim danych ujawniających pochodzenie rasowe lub etniczne. Pojawiła się wątpliwość, czy można zastosować jakiegokolwiek odstępstwo od art. 10 ust. 1 rozporządzenia (WE) nr 45/2001, tak by uniknąć konieczności uzyskania pozwolenia organów państw członkowskich na przeprowadzenie wspomnianej operacji przetwarzania danych.

DPO Agencji Praw Podstawowych Unii Europejskiej (FRA) skonsultował się z Inspektorem w sprawie operacji przetwarzania danych obejmujących pulę zainteresowanych osób z państw członkowskich Unii Europejskiej, które wyraziły wolę udziału w badaniach sondażowych dotyczących praw podstawowych, takich jak badanie dotyczące dyskryminacji oraz ofiar przestępstw kryminalnych wśród wybranych grup imigrantów oraz innych mniejszości. Agencja Praw Podstawowych UE zawarła umowę z wykonawcą zewnętrznym. Jednym z celów tej umowy było zebranie szczególnych kategorii danych, przede wszystkim danych ujawniających pochodzenie rasowe lub etniczne. Pojawiła się wątpliwość, czy można zastosować jakiegokolwiek odstępstwo od art. 10 ust. 1 rozporządzenia (WE) nr 45/2001, tak by uniknąć konieczności uzyskania pozwolenia organów państw członkowskich na przeprowadzenie wspomnianej operacji przetwarzania danych.

2.6.4. Wniosek o kopię pełnej dokumentacji medycznej urzędnika wydany przez sąd

DPO jednej z agencji skonsultował się z Inspektorem w związku z otrzymanym przez jej służbę medyczną sądowym wnioskiem o kopię pełnej dokumentacji medycznej pewnego urzędnika do celów sprawy rozwodowej.

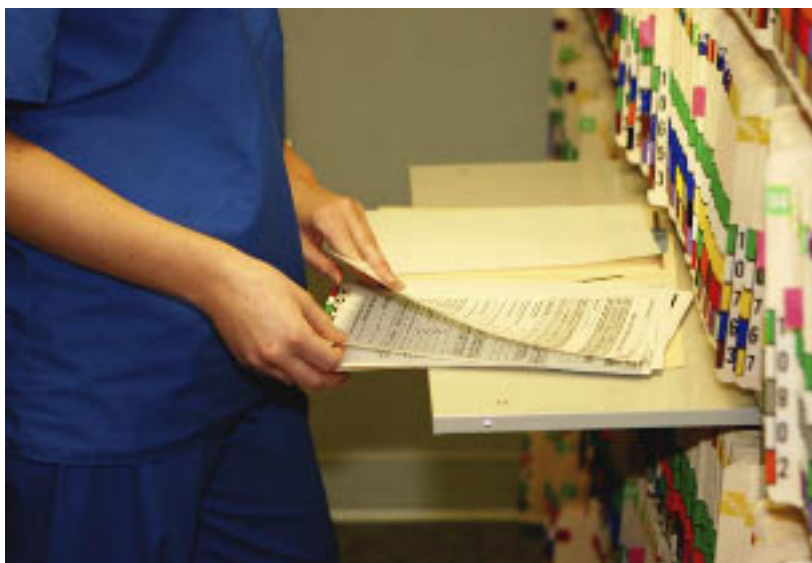
Inspektor uznał, że w analizowanej sprawie administrator danych podlega obowiązkowi współpracy z krajowym wymiarem sprawiedliwości i, co za tym idzie, z tego punktu widzenia przetwarzanie danych byłoby uzasadnione (w świetle art. 5 lit. b) rozporządzenia, w którym przewidziano,

⁽²⁰⁾ Dostępne na stronie www.edps.europa.eu od lipca 2005 roku. Zob. w szczególności sekcja 4.3.

że dane osobowe mogą być przetwarzane, tylko gdy „przetwarzanie jest konieczne dla zgodności ze zobowiązaniem prawnym, któremu podlega administrator danych”). Służba medyczna podlega jednak obowiązkowi wynikającemu z tajemnicy lekarskiej. W konsekwencji w sprawach, w których sąd zwraca się o informacje w ramach postępowania sądowego, współpraca z krajowym wymiarem sprawiedliwości musi przebiegać zgodnie z wymogami i mechanizmami wynikającymi z krajowych przepisów dotyczących tajemnicy lekarskiej.

Inspektor zauważył, że ze względu na szczególny charakter omawianej kategorii danych, zgoda osoby, której dane dotyczą, byłaby zalecana jako dodatkowa podstawa legalności (art. 5 lit. d) rozporządzenia). Odmowa zgody ze strony osoby, której dane dotyczą, nie spowodowałaby jednak nieważności podstawy, o której mowa w art. 5 lit. b), wyjaśnionej powyżej. Odmowa zgody musi być w każdym razie rozpatrywana z perspektywy ogólnej proporcjonalności i jakości danych.

Inspektor podkreślił również, że przed przekazaniem dokumentacji medycznej administrator musi upewnić się, czy przekazywane są tylko dane prawidłowe, stosowne i nienadmierne w stosunku do celów. W związku z tym, że wniosek sądu nie precyzował, w jakim celu dane mają być przetwarzane, w świetle art. 4 ust. 1 lit. b) uzasadnione jest zwrócenie się o wyjaśnienie tej kwestii (sprawa 2008-145).



Przed przekazaniem dokumentacji medycznej do sądu administrator danych musi zadbać o to, by respektowano zasadę jakości danych

2.6.5. Zatrzymywanie danych o karach dyscyplinarnych związanych z danymi

Inspektor przedstawił kolegium szefów administracji swoje stanowisko na temat okresu przechowywania danych o karach w aktach postępowań dyscyplinarnych po wykonaniu tych kar. Zauważono brak zgodności między stosowaną obecnie interpretacją regulaminu pracowniczego a prawami podstawowymi, takimi jak ochrona danych.

Inspektor podkreślił w szczególności, że po pierwsze art. 27 załącznik IX do regulaminu pracowniczego stoi w sprzeczności z rozporządzeniem (WE) nr 45/2001, gdyż przepisy regulaminu wskazują na dyskrecjonalny charakter decyzji o usunięciu danych podejmowanej przez organ powołujący. Rozporządzenie natomiast wymaga między innymi, by dane zachowywano „przez czas nie dłuższy, niż jest to konieczne do celów, dla których dane były gromadzone lub dla których są przetwarzane dalej”. W tej sytuacji Inspektor zalecił zatem jako słuszne, by w związku z tym w przyszłości przy dokonywaniu zmiany regulaminu pracowniczego ponownie przeanalizować stosowane limity czasowe i by wprowadzić obowiązek usunięcia wszelkich wzmianek o środkach dyscyplinarnych po upływie ustalonego okresu.

Po drugie Inspektor zalecił, by prawidłowa interpretacja art. 10 lit. h) i i) nie powodowała żadnej sprzeczności z właściwym celem art. 27. Ten pierwszy artykuł należy zatem interpretować „nie naruszając” drugiego, a nie odwrotnie, dzięki czemu uniknie się wszelkich szkód dla praw podstawowych personelu.

Po trzecie akta postępowań dyscyplinarnych nie powinny być przechowywane w nieskończoność, nawet po usunięciu z akt osobowych wzmianki o karze. Narusza to nie tylko art. 4 ust. 1 lit. e) rozporządzenia, lecz także zasadę wynikającą z orzecznictwa Sądu Pierwszej Instancji

mówiącą, że nie należy przechowywać analogicznych akt.

Po czwarte Inspektor zauważył, że w załączniku IX art. 13 terminu „akta osobowe” używa się w znaczeniu „akta osobowe postępowania dyscyplinarnego”. Żadna inna interpretacja nie wniosłaby nic nowego do art. 26 regulaminu pracowniczego, a pozbawiłaby art. 13 wszelkiego znaczenia, na przykład dotyczącego prawa pracownika wynikającego z art. 41 ust. 2 lit. b) Karty praw podstawowych UE (sprawa 2006-075).

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

Inspektor ochrony danych (DPO) Trybunału Sprawiedliwości Wspólnot Europejskich skonsultował się z Inspektorem w sprawie projektu decyzji Komitetu Administracyjnego Trybunału Sprawiedliwości dotyczącej przepisów wykonawczych do rozporządzenia (WE) nr 45/2001. W projekcie tym poruszono jedynie aspekty związane z art. 24 ust. 8 oraz z załącznikiem do rozporządzenia (zadania i obowiązki DPO i administratorów), a nie aspekty odnoszące się do osób, których dane dotyczą, obecne w innych przepisach wykonawczych. W ramach tego ograniczonego zakresu zauważono brak pewnych przepisów, np. dotyczących długości mandatu DPO oraz oceny inspektorów. Zalecono także pewne rozszerzenie zakresu zapytań kierowanych przez DPO. Mimo wszystko Inspektor z zadowoleniem przyjął wspomniany projekt, gdyż wprowadza on pewne popierane przez niego dobre praktyki, takie jak utrzymywanie kontaktów między DPO a służbami sądowymi odpowiedzialnymi za technologie informacyjne (sprawa 2008-0658).

2.6.7. Skargi rozpatrywane przez Europejskiego Rzecznika Praw Obywatelskich

Inspektor służył radą Europejskiemu Rzecznikowi Praw Obywatelskich w sprawie zagadnień ochrony danych wiążących się z przekazywaniem odnośnym instytucjom Wspólnoty decyzji Rzecznika o niewszczygnięciu dochodzenia w związku z niektórymi skargami oraz w sprawie uzasadnienia tych decyzji (sprawa 2008-608). W tym konkretnym przypadku, uwzględniając to, że domyślną zasadą w biurze Europejskiego Rzecznika Praw Obywatelskich jest publiczne rozpatrywanie skarg,

Inspektor zalecił informowanie skarżącego, o ile nie zdecydował się on jeszcze na utajnienie sprawy, o tym, że jeżeli jego skarga zostanie uznana za niedopuszczalną, może on jeszcze zdecydować się na utajnienie sprawy po otrzymaniu decyzji.

2.7. Nadzór wideo

2.7. Nadzór wideo

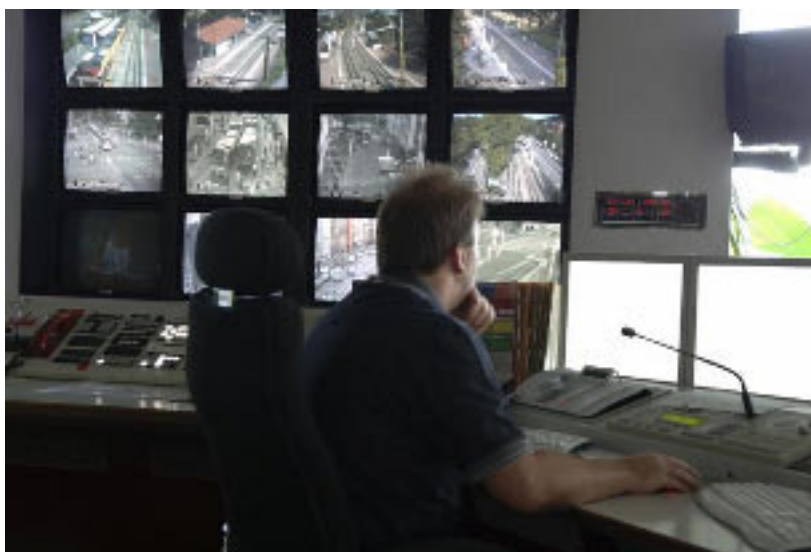
W 2008 roku Inspektor kontynuował prace nad wytycznymi w sprawie nadzoru wideo, aby zapewnić instytucjom i organom UE praktyczne wskazówki dotyczące przestrzegania przepisów o ochronie danych przy wykorzystywaniu systemów nadzoru wideo. Pierwszy wewnętrzny roboczy projekt wytycznych został przygotowany pod koniec 2008 roku. Projekt ten zostanie upubliczniony w połowie 2009 roku i poddany konsultacjom.

Wytyczne mają zawierać raczej praktyczne wskazówki niż teorię prawną. Mają być elastyczne, ale też mają oferować pewność, co do następujących kwestii: które ze sposobów wykorzystania nadzoru wideo Inspektor może uznać za niewłaściwe; jakie kroki powinny zostać podjęte przez instytucje przed zainstalowaniem systemu nadzoru wideo lub zmodernizowaniem istniejącego; oraz jakie środki powinny przedsięwziąć na bieżąco, aby zapewnić odpowiednie rozwiązywanie problemów dotyczących ochrony danych w toku działania systemu nadzoru wideo.

We wspomnianych wytycznych zalecono instytucjom, by:

- precyzyjnie ustaliły cel, jaki pragną osiągnąć dzięki systemowi;
- dokładnie przeanalizowały, czy technologia nadzoru wideo jest skutecznym i proporcjonalnym środkiem do osiągnięcia tego celu;
- szukały alternatywnych rozwiązań, zanim podejmą decyzję o zastosowaniu kamer; oraz
- współpracowały ze swoim DPO przed podjęciem decyzji, gdzie umieścić kamery, jak z nich korzystać oraz jakie wprowadzić zabezpieczenia i ograniczenia pomagające chronić prywatność osób zarejestrowanych przez kamery.

Wymaga się również, by: instytucje nie przechowywały nagrań wideo dłużej niż to konieczne; ściśle ograniczyły liczbę ich odbiorców; udokumentowały każdy przypadek wykorzystania i przekazania nagrań; oraz przedsięwzięły stosowne środki



Bezpieczne stosowanie nadzoru wideo wymaga zabezpieczeń w zakresie ochrony danych

bezpieczeństwa, aby zminimalizować niebezpieczeństwo dostępu do nich osób nieupoważnionych. Ponadto instytucje mają również obowiązek poinformować w odpowiedniej formie społeczeństwo. Jeśli chodzi o powiadamianie, Inspektor zachęca do zastosowania podejścia wielopoziomowego, które oprócz ustawiania tablic informacyjnych na miejscu, powinno obejmować zamieszczenie szczegółowych informacji na stronie internetowej danej instytucji. Każda instytucja ma również ustanowić mechanizm zapewniania dostępu osobom, które pragną wiedzieć, jakie dotyczące ich dane wideo są przetwarzane.

Omawiane wytyczne dostarczają szczegółowych wskazówek mniejszym instytucjom, w tym wielu agencjom, dysponującym stosunkowo prostymi i standardowymi systemami nadzoru wideo.

2.7.2. Kontrola wstępna

W 2008 roku Inspektor otrzymał dwa kolejne powiadomienia w sprawie kontroli wstępnej *ex post* w odniesieniu do nadzoru wideo: z JRC IE w Petten oraz z JRC ITU w Karlsruhe. Zawieszono je, podobnie jak powiadomienia w sprawie kontroli wstępnej *ex post* otrzymane w 2007 roku, w oczekiwaniu na przyjęcie wytycznych Inspektora w sprawie nadzoru wideo.

Inspektor dokonał już jednak przeglądu praktyk stosowanych przez OLAF w dziedzinie telewizji przemysłowej (CCTV), poddanych faktycznej procedurze kontroli wstępnej (sprawa 2007-634). Opinia

z tej kontroli wstępnej jest pierwszą opinią Inspektora dotyczącą nadzoru wideo. Sprawa dotyczyła telewizji przemysłowej wykorzystywanej przez OLAF do celów bezpieczeństwa w jego siedzibie w Brukseli.

Zasadniczo Inspektor uznał za satysfakcjonujące proporcjonalność systemu telewizji przemysłowej i wdrożone przez OLAF zabezpieczenia w zakresie ochrony danych. System ten ma precyzyjnie określone, stosunkowo ograniczone i słuszne cele. Ponadto umiejscowienie, zasięg i rozdzielczość, a także inne aspekty ustawień systemu telewizji przemysłowej

wydają się być prawidłowe, stosowne i nienadmierne w stosunku do określonych celów, również gdy uwzględni się szczególny charakter informacji będących w posiadaniu OLAF-u.

Inspektor wydał jednak OLAF-owi istotne zalecenia: by ponownie przeanalizował przewidywany okres zachowywania danych, tak by dane przechowywane były nie dłużej niż jest to konieczne do pierwotnie przyjętych celów. Inspektor zalecił również przyjęcie przez OLAF wewnętrznego dokumentu, w którym opisano by system telewizji przemysłowej OLAF-u i przewidziano odpowiednie zabezpieczenia służące ochronie danych. I wreszcie Inspektor zachęcił OLAF do zapewniania konkretniejszych i dokładniejszych informacji osobom, których dane dotyczą.

2.7.3. Skarga

W 2008 roku Inspektor nadal badał skargę obywatelską w sprawie wykorzystywania telewizji przemysłowej w Parlamencie Europejskim dotyczącą monitoringu poza budynkami Parlamentu (sprawa 2006-0185).

Poczyniono postępy, jeśli chodzi o pewne istotne aspekty przestrzegania ochrony danych. Parlament dokonał przeglądu miejsc, w których znajdują się kamery, i gdy stwierdził, że zasięg kamery obejmuje prywatne tereny przyległych budynków, zastosował środki techniczne, by uniknąć takich przypadków

lub je ograniczyć. Parlament zgodził się również, by przekazywać osobom, których dane dotyczą, bardziej kompleksowe informacje dotyczące wykorzystywania telewizji przemysłowej, w tym umieszczać informacje na stronie internetowej. Ponadto Parlament prowadzi obecnie rejestr wszystkich przypadków, gdy dział ochrony doraźnie przekazuje nagrania telewizji przemysłowej innym odbiorcom zarówno z instytucji, jak i spoza nich (np. wszystkie przypadki przekazywania nagrań policji są obecnie odnotowywane w rejestrze).

Mimo to Inspektor nie uznał środków zastosowanych przez Parlament za w pełni satysfakcjonujące. Na przykład wolałby, by okres zatrzymywania nagrań spoza siedziby Parlamentu był znacznie krótszy niż obecnie. Inspektor zamknął jednak omawianą sprawę, ale jednocześnie ostrzegł Parlament, że gdy tylko zostaną przyjęte wytyczne w sprawie nadzoru wideo, instytucja ta powinna podjąć kroki w celu dostosowania swoich praktyk do jego zaleceń. Inspektor zwrócił również uwagę na to, że możliwe jest dalsze badanie przestrzegania przepisów w ramach formalnej procedury kontroli wstępnej *ex post* lub w ramach kontroli.

2.7.4. Inne wnioski

Inspektor przekazywał również na życzenie nieformalne wskazówki w sprawie praktyk dotyczących nadzoru wideo inspektorom ochrony danych. Powtarzały się pytania dotyczące sposobu zapewnienia informacji osobom, których dane dotyczą, oraz miejsc, w których zainstalowanie kamer byłoby właściwe i proporcjonalne.

W jednym z przypadków agencja pytała o to, czy proporcjonalne jest wykorzystywanie ukrytej kamery, po to by wykryć sprawcę powtarzających się kradzieży produktów żywnościowych z indywidualnego biura. Inspektor uznał, że zastosowanie ukrytych kamer jest nieproporcjonalne i zalecił agencji wykorzystanie innych metod, aby wykryć sprawcę lub powstrzymać go przed takim zachowaniem.

Pod koniec 2008 roku zapytano również Inspektora o proporcjonalność wykorzystania kamer telewizji przemysłowej w poczekalni punktu medycznego. Inspektor bada obecnie tę sprawę.

2.8. Eurodac

Eurodac to obszerna baza danych zawierająca odciski palców osób ubiegających się o azyl i nielegalnych imigrantów wykrytych na terytorium UE. Ta baza danych pomaga w skutecznym stosowaniu konwencji dublińskiej w sprawie rozpatrywania wniosków o azyl. Baza Eurodac została utworzona na mocy przepisów szczegółowych, przyjętych na szczeblu europejskim i obejmujących zabezpieczenia służące ochronie danych ⁽²¹⁾.

Inspektor sprawuje nadzór nad przetwarzaniem danych osobowych w centralnej bazie danych, którą zarządza jednostka centralna w Komisji, oraz nad ich przesyłaniem do państw członkowskich. Organy ds. ochrony danych w państwach członkowskich nadzorują przetwarzanie danych przez organy krajowe oraz przesyłanie tych danych do jednostki centralnej. Aby zapewnić skoordynowane podejście, Inspektor i organy krajowe spotykają się regularnie w celu omówienia wspólnych problemów związanych z funkcjonowaniem Eurodac oraz zalecenia wspólnych rozwiązań. To podejście oparte na „skoordynowanym nadzorze” działa jak dotąd bardzo skutecznie i w 2008 roku poświęcono mu dużo uwagi (zob. sekcja 4.3)

Inne działania Inspektora odnoszące się do Eurodac miały punkty styczne z konsultacjami w zakresie powiązanych zagadnień, takich jak kwestie polityki dotyczącej granic (zob. sekcja 3.4 i 3.6) oraz przygotowania do przeglądu rozporządzenia Dublin II i rozporządzenia Eurodac, na których temat Inspektor wydał opinie w lutym 2009 roku.

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

3. Konsultacje

3.1. Wprowadzenie

Rok 2008 jest już czwartym rokiem, w którym Europejski Inspektor Ochrony Danych (Inspektor) w pełni wykonywał swoje uprawnienia konsultacyjne jako doradca instytucji wspólnotowych w kwestiach dotyczących wniosków prawodawczych (i powiązanych dokumentów). Był to kolejny ważny rok, w którym nastąpiła intensyfikacja jego działań. Dalej rozwijał i poprawiał swoją wydajność oraz przedłożył opinie dotyczące jeszcze większej liczby ważnych wniosków prawodawczych. W 2008 roku poszerzył się zakres jego działania, który objął dodatkowe dziedziny polityki Unii Europejskiej (UE). Ponadto Inspektor brał udział we wszystkich etapach procedury legislacyjnej: od początku (reagowanie na zieloną księgę o majątku dłużnika) do samego końca (aktywne śledzenie, czasami bycie uczestnikiem debat prowadzonych w Parlamencie Europejskim i w Radzie na temat istotnych kwestii, jak na przykład europejskiego systemu danych dotyczących przelotu pasażera (PNR) czy dyrektywy o prywatności i łączności elektronicznej).

Celem udziału Inspektora w procesie legislacyjnym UE jest aktywne promowanie tego, by środki prawodawcze przyjmowane były wyłącznie po należytym przeanalizowaniu ich wpływu na prywatność i ochronę danych. Inspektor wydaje oficjalną opinię, która staje się częścią procesu legislacyjnego. Kilka opinii przedstawiono na forum Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (Komisja LIBE) oraz odpowiednich grup roboczych Rady.

Tak jak w latach poprzednich Inspektor korzystał ze spisu własnych zamierzeń na nadchodzący rok.

„Spis zamierzeń na rok 2008” został opublikowany na stronie internetowej Inspektora w grudniu 2007 roku. Zawiera on krótką analizę najważniejszych wydarzeń oraz priorytety na rok 2008.

Od czasu rozpoczęcia działalności przez instytucję kierowaną przez Inspektora, liczba wydawanych przez niego opinii stale wzrasta. W 2008 roku wydano 14 opinii. Opinie te odzwierciedlają również istotne zagadnienia zawarte w programach Komisji, Parlamentu Europejskiego i Rady dotyczących kierunków polityki. Większość opinii dotyczyła kwestii związanych z przestrzenią wolności, bezpieczeństwa i sprawiedliwości, w tym zarówno tzw. „trzeciego filaru” UE (współpraca policyjna i sądowa), jak i zarządzania granicami (w ramach „pierwszego filaru”). Wnioski w tej dziedzinie mogą propagować na przykład wymianę informacji między organami w celu zwalczania terroryzmu oraz innych przestępstw, która może się wiązać z tworzeniem dużych baz danych dotyczących milionów ludzi. Ważnym wydarzeniem w tej dziedzinie było przyjęcie decyzji ramowej Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej sądowej w sprawach karnych w listopadzie 2008 roku ⁽²²⁾.

Pewne opinie dotyczyły również transgranicznej wymiany informacji niezwiązanej ze zwalczaniem terroryzmu, jak na przykład wniosku z grudnia 2008 roku dotyczącego dyrektywy w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej. Zasadniczo Inspektor uznał, że wspomniane

⁽²²⁾ Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350, 30.12.2008, s. 60).



Zespół ds. konsultacji podczas omawiania opinii prawnej

wnioski w dostateczny sposób uzasadniają ustanowienie rozpatrywanych systemów. Wydał jednak zalecenia mające na celu dopracowanie głównych elementów tych wniosków mających związek z ochroną danych.

Aby udzielać porad instytucjom UE w zakresie prowadzonych przez nie prac prawodawczych, Inspektor stosuje nie tylko opinie. Korzysta także z innych narzędzi interwencji, takich jak uwagi. Wstępne uwagi Inspektora do pakietu Komisji dotyczącego zarządzania granicami UE są jednym z przykładów.

Niniejszy rozdział poświęcono działaniom Inspektora jako organu doradczego przeprowadzonym w 2008 roku. Poszczególne opinie opublikowane w 2008 roku podsumowano w sekcji 3.3.2. Niniejszy rozdział zawiera także opis skutków, jakie mają dla Inspektora rozwój nowych technologii oraz nowe wydarzenia w dziedzinie polityki i prawodawstwa.

3.2. Ramy polityki i priorytety

3.2.1. Realizacja polityki konsultacyjnej

W dokumencie strategicznym zatytułowanym „Inspektor jako doradca instytucji wspólnotowych w zakresie wniosków prawodawczych i dokumentów pokrewnych”⁽²³⁾ nakreślono główne elementy obrazujące, w jaki sposób Inspektor zamierza wykonywać swoje zadania w dziedzinie konsultacji. Dokument ten wyjaśnia, jakie kroki podejmuje Inspektor, aby skutecznie wypełnić

⁽²³⁾ Dostępny na stronie internetowej Inspektora: (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/05-03-18_PP_EDPSadvisor_EN.pdf).

wyznaczone mu zadania w zakresie konsultacji dotyczących wniosków prawodawczych.

Ten dokument strategiczny ma zapewnić Inspektorowi status godnego zaufania i przewidywalnego uczestnika procesu prawodawczego w UE, jeśli chodzi o kwestie dotyczące przetwarzania danych osobowych. Dokument ten, przyjęty w marcu 2005 roku, okazał się solidną podstawą Inspektora.

Strategia przedstawiona we wspomnianym dokumencie obejmuje następujące trzy elementy.

- Zagadnienia, co do których wymagane są konsultacje z Inspektorem: ich zakres jest szeroki, gdyż z ochroną danych osobowych mogą wiązać się wnioski dotyczące wielu tematów.
- Treść interwencji Inspektora: interwencje te opierają się na ogólnej idei, by wkład wnoszony w proces prawodawczy miał charakter nie tylko krytyczny, lecz także konstruktywny.
- Rola Inspektora zakłada prowadzenie działań mieszczących się w ramach instytucjonalnych UE: funkcja doradcza Inspektora staje się coraz bardziej oczywista dla instytucji.

Wspomniany dokument strategiczny przewiduje, że do interwencji dochodzi na różnych etapach. Służby Komisji Europejskiej zazwyczaj zwracają się do Inspektora o jego wkład przed formalnym przyjęciem wniosku Komisji, często odbywa się to równoległe z wewnętrznymi konsultacjami wśród poszczególnych służb. Na tym etapie Inspektor przekazuje nieformalne uwagi. Po przyjęciu swojej opinii Inspektor utrzymuje również nieformalne kontakty z Radą za pośrednictwem prezydencji i Sekretariatu Generalnego Rady. W wielu przypadkach Inspektor wyjaśniał i omawiał swoją opinię na forum grup roboczych Rady zajmujących się danym wnioskiem prawodawczym. Takie same działania podejmował też w odniesieniu do LIBE i innych komisji Parlamentu zaangażowanych w daną inicjatywę. Inspektor zainicjował ponadto nieformalne kontakty z Parlamentem Europejskim – zarówno z posłami, jak i z sekretariatem – a jednocześnie był gotów brać udział w ogólniejszych debatach, takich jak wysłuchania publiczne. Nowym zjawiskiem w 2008 roku było ściśle angażowanie się w kwestie prawodawcze na późniejszych etapach procedury

legislacyjnej, zwłaszcza w związku z europejskim systemem PNR oraz dyrektywą o prywatności i łączności elektronicznej.

W 2009 roku szczególna uwaga zostanie poświęcona temu, jak doradzać Komisji, w przypadku gdy nie przyjmuje ona wniosku (skierowanego do Rady lub Parlamentu Europejskiego), lecz stanowi samodzielnie. Do sytuacji tej dochodzi w przypadkach dotyczących:

- przepisów wykonawczych Komisji (podlegających procedurze komitetowej lub nie);
- decyzji Komisji stwierdzających istnienie odpowiedniego stopnia ochrony danych w państwach trzecich zgodnie z art. 25 ust. 6 dyrektywy 95/46/WE;
- publikowania komunikatów Komisji.

W tych konkretnych przypadkach formalna opinia wydana po przyjęciu instrumentu przez Komisję nie ma wpływu na jego tekst.

W dniu 28 kwietnia 2008 r. Inspektor przedstawił kolejny dokument strategiczny zatytułowany „Europejski Inspektor Ochrony Danych a badania i rozwój technologiczny w UE”. Inspektor postanowił uważnie śledzić siódmy program ramowy w zakresie badań i rozwoju technologicznego zainicjowany przez Komisję pod koniec 2006 roku. Zdecydował, że opracuje kilka możliwych modeli wkładu w ukierunkowane projekty badawcze w ramach realizowanego obecnego siódmego programu ramowego. Te modele wkładu mają dostarczyć Komisji lub podmiotom przygotowującym projekty porad przydatnych w ich staraniach, by wykorzystywać w badaniach i w rozwoju technologicznym metody zgodne z zasadami prywatności i ochrony danych, oraz mają zachęcić do wypracowywania technologii i procesów propagujących i zwiększających skuteczność ram prawnych UE w zakresie ochrony danych. W omawianym dokumencie przedstawiono główne elementy strategii Inspektora w tej dziedzinie (zob. sekcja 3.6.5).

3.2.2. Spis zamierzeń na rok 2008

Co roku Inspektor publikuje spis swoich zamierzeń na kolejny rok. Spis zamierzeń na rok 2008 opublikowano w grudniu 2007 roku na stronie internetowej Inspektora.

Spis ten jest elementem rocznego cyklu prac Inspektora. Raz w roku Inspektor przedstawia w corocznym sprawozdaniu informacje o działaniach z minionego okresu Inspektor przedstawia ponadto

spis zamierzeń w zakresie konsultacji na kolejny rok. Przedstawia zatem informacje o działaniach w tej dziedzinie dwa razy w roku. Istotnym elementem stosowanej przez Inspektora metody pracy jest selekcja i planowanie, które są niezbędne, by mógł on skutecznie pełnić rolę doradcy.

Głównym materiałem źródłowym przy sporządzaniu spisu są program legislacyjny i program prac Komisji oraz kilka powiązanych dokumentów Komisji dotyczących planowania. Kilku zainteresowanym podmiotom z Komisji umożliwiono wniesienie wkładu w proces przygotowywania spisu.

Spis zamierzeń na rok 2008 zawiera następujące elementy:

- część wprowadzającą obejmującą krótką analizę kontekstu, a także priorytety Inspektora na rok 2008;
- załącznik zawierający odesłanie do stosownych wniosków Komisji i innych dokumentów przyjętych ostatnio lub zaplanowanych, które wymagają uwagi Inspektora.

Opublikowany w grudniu 2007 roku załącznik dotyczący roku 2008 zaktualizowano dwukrotnie w ciągu tego roku (w maju i październiku 2008 roku).

Wyniki

W załączniku do spisu zamierzeń na rok 2008 wymieniono 34 ważne dokumenty (oznaczone jako „czerwone”), w których sprawie Inspektor zamierzał wydać opinię lub podjąć podobne działanie. Osiągnięto następujące wyniki:

Wydane opinie	13 dokumentów (w tym 3 wydane przed końcem grudnia 2007 roku)
Uwagi/inne dokumenty Inspektora	4 dokumenty
Działanie za pośrednictwem grupy roboczej art. 29	1 dokument
Wnioski Komisji lub opinie Inspektora przełożone na rok 2009	14 dokumentów ¹
Bez dalszych działań Inspektora	2 dokumenty

(¹) Siedem spośród tych 14 dokumentów to dokumenty dotyczące Eurodac i SIS. Zostały one ponownie ujęte w spisie na rok 2009.

Spis zawierał ponadto 33 inne zagadnienia o mniejszym znaczeniu, w których sprawie Inspektor mógł wydać opinię lub zareagować w inny sposób. Sytuacja na koniec roku 2008 była różnicowana:

Stale śledzenie przez Inspektora (programy badawcze, kwestie/tematy ogólne, takie jak zdrowie publiczne czy systemy informacyjne na dużą skalę)	17 dokumentów
Działania podjęte przez Inspektora w 2008 roku (uwagi lub inne działania)	3 dokumenty
Usunięte ze spisu bez dalszych działań Inspektora	7 dokumentów
Działania Komisji przełożone na rok 2009	4 dokumenty
Status podwyższony do „czerwonego” (opinia wydana 2008 roku)	2 dokumenty

Priorytety na rok 2008

Priorytet 1: W 2008 roku Inspektor uważnie analizował i komentował konsekwencje traktatu lizbońskiego, chociaż wejście tego traktatu w życie zależy teraz między innymi od drugiego referendum w Irlandii. Traktat ten będzie miał duży wpływ na ochronę danych.

Priorytet 2: Inspektor nadal skupiał się na przechowywaniu i wymianie informacji w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, kładąc nacisk między innymi na zapewnienie odpowiednich ram prawnych ochrony danych w tej dziedzinie z uwzględnieniem ograniczonego zakresu zastosowania decyzji ramowej Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

Priorytet 3: Skrupulatnie analizowano i komentowano również – w następstwie komunikatu Komisji Europejskiej w sprawie identyfikacji radiowej i inteligentnego otoczenia technologicznego i związanej z tym opinii Inspektora – postępy czynione w ramach społeczeństwa informacyjnego. W tym kontekście duży nacisk położono na zmianę dyrektywy o prywatności i łączności elektronicznej.

Priorytet 4: Podejmowano działania następcze po wydaniu przez Inspektora opinii w sprawie przyszłości dyrektywy 95/46/WE. Inspektor uczestniczył w działaniach związanych z pełnym wdrożeniem tej dyrektywy. Ścisłe angażował się w różnorodne debaty na temat jej przyszłości.

Priorytet 5: Zwrócono uwagę na kilka szczególnych dziedzin działalności UE, takich jak zdrowie publiczne, relacje między ochroną danych a gromadzeniem i wykorzystywaniem danych statystycznych, a także dalsze działania związane z publicznym dostępem do dokumentów.

Priorytet 6: Wiele działań koncentrowało się na przekazywaniu danych państwom trzecim – w szczególności na przekazywaniu danych pasażerów – a także na postępowach w zakresie ustanawiania ewentualnych zasad transatlantycznych (wspólnych przede wszystkim dla UE i USA) dotyczących wymiany informacji w celu egzekwowania prawa.

3.2.3. Spis zamierzeń na rok 2009

Priorytety Inspektora na rok 2009

Strategia Inspektora nie będzie odbiegać od kierunków nakreślonych w spisie zamierzeń na rok 2008. Jak można zauważyć, w 2008 roku w ocenach skutków regulacji, o których mowa w programie legislacyjnym i programie prac Komisji na ten rok, w odpowiedni sposób uwzględniono prywatność i ochronę danych.

Priorytety na rok 2009 będą opierać się na tych wyznaczonych na rok 2008 z uwzględnieniem osiągniętych od tego czasu postępów. Oprócz nowych wniosków ze szczególną uwagą traktowany będzie komunikat Komisji w sprawie programu sztokholmskiego w dziedzinie wolności, bezpieczeństwa i sprawiedliwości⁽²⁴⁾. Inicjatywa ta ma zasadniczo służyć ustaleniu priorytetów i celów przyszłych działań UE w tej dziedzinie oraz wskazaniu najskuteczniejszych środków i przedsięwzięć umożliwiających ich osiągnięcie. Obejmowałaby ona globalny pakt o imigracji, e-sprawiedliwość oraz plan działania dotyczący narkotyków. Daje ona Inspektorowi możliwość zastanowienia się nad swoimi priorytetami na pięć

⁽²⁴⁾ Komunikat Komisji w sprawie programu sztokholmskiego w dziedzinie wolności, bezpieczeństwa i sprawiedliwości 2008/JLS/119.

najbliższych lat. Inspektor będzie reagować na etapie przygotowań, a gdy dojdzie do przyjęcia aktu – wyda opinię. Korzystny jest także fakt, że zbiegnie się to z nowym mandatem Inspektora rozpoczynającym się w 2009 roku.

3.3. Opinie prawne

3.3.1. Uwagi ogólne

W 2008 roku Inspektor przyjął 14 opinii prawnych. Podobnie jak w latach poprzednich duża część tych opinii dotyczyła przestrzeni wolności, bezpieczeństwa i sprawiedliwości, zarówno w ramach pierwszego, jaki i trzeciego filaru. Blisko połowa wydanych opinii prawnych, tzn. 6 z 14, odnosiła się do tej dziedziny. Szczególną uwagę Inspektor poświęcił także propozycji wprowadzenia zmian do rozporządzenia (WE) nr 1049/2001 w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji. Inne ważne inicjatywy, w których sprawie Inspektor wydał opinie, dotyczyły następujących zagadnień: systemu wymiany informacji na rynku wewnętrznym (IMI), komputerowego systemu rezerwacji (KSR), bezpieczeństwa ruchu drogowego, statystyk europejskich oraz transgranicznej opieki zdrowotnej.

Na podstawie przeglądu wspomnianych 14 opinii można stwierdzić, że w większości przypadków Inspektor poparł wnioski, lecz zwrócił się o zapewnienie dodatkowych zabezpieczeń służących ochronie danych.

Wymiana informacji

Obszarem o szczególnym znaczeniu dla Inspektora była kwestia wymiany informacji, w szczególności ustanowienie systemów informacyjnych oraz dostępu różnych organów do tych systemów w określonych celach. Transgraniczna wymiana informacji jest obecnie coraz szerzej wykorzystywana.

W 2008 roku Inspektor przyjął opinie w sprawie wymiany informacji w związku z: systemem wymiany informacji na rynku wewnętrznym (IMI), Eurojustem, bezpieczeństwem ruchu drogowego, ochroną dzieci korzystających z Internetu, ECRIS, grupą kontaktową wysokiego szczebla UE–USA ds. wymiany informacji oraz europejską strategią w dziedzinie e-sprawiedliwości. Inspektor przeanalizował konsekwencje prawne wynikające z rozwijania różnych systemów informacyjnych i technologicznych na dużą skalę. Z analizy tej wynika, że należy każdorazowo właściwie i starannie ocenić potrzebę takiej wymiany informacji. Ponadto w chwili ustanawiania takiej wymiany informacji należy wdrożyć konkretne zabezpieczenia służące ochronie danych.

Zobowiązania prawne, z których wynika konieczność tworzenia dużych baz danych, wiążą się ze szczególnym ryzykiem dla osób, których dane dotyczą, ze względu na niebezpieczeństwo nieuprawnionego wykorzystania tych danych. Inspektor niejednokrotnie wyrażał zaniepokojenie w związku z brakiem zabezpieczeń stosowanych w dziedzinie wymiany danych osobowych z państwami trzecimi. W kilku wnioskach przewidziano taką wymianę informacji, w związku z czym Inspektor wskazywał na konieczność zapewnienia mechanizmów, które gwarantowałyby wspólne standardy i skoordynowane decyzje dotyczące adekwatności. Wymiana informacji z państwami trzecimi powinna być dozwolona wyłącznie wtedy, gdy państwa te zapewniają odpowiedni stopień ochrony danych osobowych lub gdy dana operacja przekazania informacji odbywa się w ramach jednego z odstępstw określonych w dyrektywie 95/46/WE.

Nowe technologie

Inspektor kilkakrotnie poruszał kwestię wykorzystywania nowych technologii. Wielokrotnie wzywał do dbania o to, by kwestie dotyczące ochrony danych uwzględniano na możliwie najwcześniejszym etapie („wbudowana ochrona prywatności”). Podkreślał również, że narzędzia oparte na nowych technologiach powinny być wykorzystywane nie tylko po to, by umożliwić wymianę informacji, lecz także po to by rozszerzyć prawa osób, których dane są przetwarzane. W przypadku ECRIS i e-sprawiedliwości Inspektor z zadowoleniem przyjął zapewnienie osobie, której dane dotyczą, możliwości zwracania się do centralnego organu danego państwa członkowskiego o dotyczące jej informacje zawarte w rejestrze, pod warunkiem że osoba ta jest lub była rezydentem lub obywatelem państwa członkowskiego, do którego wniosek jest kierowany, lub państwa składającego wniosek. Jeśli chodzi o koordynację systemów ubezpieczeń społecznych, Inspektor wskazał również na możliwość wykorzystania jako „punktu kompleksowej obsługi” organu, który jest najbliższy danej osobie. Inspektor zachęca zatem Komisję do rozwijania narzędzi technologicznych, w szczególności dostępu on-line, co umożliwi obywatelom lepszą kontrolę nad własnymi danymi osobowymi, nawet w przypadku gdy przemieszczają się oni między różnymi państwami członkowskimi.

Jakość danych

Innym ważnym tematem była jakość danych. Aby uniknąć niejasności przetwarzanych informacji, niezbędny jest wysoki poziom dokładności danych. W związku z tym niezbędne jest regularne i właściwe sprawdzanie dokładności danych. Ponadto wysoka jakość danych nie stanowi wyłącznie jednej

z podstawowych gwarancji dla osoby, której dane dotyczą; pozwala ona także podmiotom przetwarzającym dane na skuteczne ich wykorzystywanie.

3.3.2. Poszczególne opinie

System wymiany informacji na rynku wewnętrznym (IMI)

W dniu 22 lutego 2008 r. Inspektor przedstawił opinię dotyczącą decyzji Komisji w sprawie wdrożenia systemu wymiany informacji rynku wewnętrznego (IMI) ⁽²⁵⁾. System wymiany informacji na rynku wewnętrznym (IMI) jest narzędziem technologii informacyjnej, które umożliwia wymianę informacji pomiędzy właściwymi organami państw członkowskich w związku z wdrażaniem prawodawstwa dotyczącego rynku wewnętrznego. IMI powstał w ramach programu IDABC („Interoperatywne świadczenie ogólnoeuropejskich usług eGovernment dla administracji publicznej, przedsiębiorstw i obywateli”).

Główne zalecenie Inspektora dotyczyło konieczności zapewnienia decyzji w sprawie IMI solidnej podstawy prawnej. Zdaniem Inspektora, istniejąca podstawa prawna (decyzja w ramach programu IDABC) nie gwarantuje niezbędnej pewności prawa, gdyż istnieją wątpliwości co do wiążącego charakteru tego dokumentu. Inspektor przedstawił ponadto kilka sugestii co do przepisów regulujących aspekty IMI wiążące się z ochroną danych. Dotyczyły one przejrzystości i proporcjonalności; wspólnego administrowania i podziału obowiązków; powiadamiania osób, których dane dotyczą; prawa dostępu do danych, wnoszenia sprzeciwu i poprawiania danych; zatrzymywania danych; środków bezpieczeństwa i wspólnego nadzoru.

Zabezpieczenia i dane biometryczne w paszportach

W dniu 26 marca 2008 r. Inspektor przedstawił opinię na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie, mimo że nie konsultowano się z nim w sprawie tego wniosku ⁽²⁶⁾.

⁽²⁵⁾ Opinia z dnia 22 lutego 2008 r. dotycząca decyzji Komisji z dnia 12 grudnia 2007 r. w sprawie wdrożenia systemu wymiany informacji rynku wewnętrznego (IMI) pod względem ochrony danych osobowych (2008/49/WE) (Dz. U. C 270 z 25.10.2008, s. 1).

⁽²⁶⁾ Opinia z dnia 26 marca 2008 r. na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie (Dz. U. C 200 z 6.8.2008, s. 1).

Dane biometryczne – wraz z zabezpieczeniami – służą wzmocnieniu związku między paszportem a posiadaczem tego dokumentu. Z myślą o ujednoczeniu wyjątków dotyczących paszportów biometrycznych we wniosku dodano następujące środki: dzieci w wieku poniżej 6 lat są zwolnione z obowiązku złożenia odcisków palców; także osoby fizycznie niezdolne do złożenia odcisków palców powinny być zwolnione z tego wymogu. Poza tym wniosek wprowadza wymóg „jedna osoba – jeden paszport”, który został opisany jako dodatkowy środek bezpieczeństwa i dodatkowa ochrona dzieci.

Inspektor zalecił zmianę proponowanego rozporządzenia w taki sposób, by:

- wyznaczyć granicę wieku dla dzieci – w wyniku spójnej, pogłębionej analizy, której celem byłoby właściwe określenie dokładności systemów uzyskanej w warunkach rzeczywistych oraz odzwierciedlenie różnorodności przetwarzanych danych; analizę tę powinna przeprowadzić instytucja europejska dysponująca konkretną wiedzą fachową oraz odpowiednim wyposażeniem w tej dziedzinie;
- jako dodatkowe zwolnienie wprowadzić granicę wieku dla osób starszych, która może opierać się na podobnych rozwiązaniach (w programie US-visit: 79 lat); takie zwolnienia nie powinny w żadnym wypadku powodować stygmatyzacji ani dyskryminacji osób, których one dotyczą;
- zasadę „jedna osoba – jeden paszport” należy stosować jedynie do dzieci powyżej odpowiedniej granicy wieku;
- dokumenty „źródłowe”: należy zaproponować dodatkowe środki, których celem byłaby harmonizacja sporządzania i wykorzystywania dokumentów wymaganych przez państwa członkowskie przy wydawaniu paszportów (dokumentów „źródłowych”);



Dane biometryczne w paszportach: jeden ze sposobów potwierdzania autentyczności wymagający rygorystycznych zabezpieczeń

- bardziej zharmonizować proces wdrażania rozporządzenia (WE) nr 2252/2004; należy wprowadzić wyłącznie zdecentralizowane przechowywanie danych biometrycznych gromadzonych do celów wydawania paszportów w państwach członkowskich, a także wspólne odsetki błędów w procesie wprowadzania i porównywania danych.

E-prywatność

W dniu 10 kwietnia 2008 r. Inspektor udzielił porady w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej, zwana także „dyrektywą o e-prywatności”) ⁽²⁷⁾.

Wniosek ma na celu poprawienie ochrony prywatności osób fizycznych i ich danych osobowych w sektorze łączności elektronicznej. Dokonuje się tego nie poprzez nadanie zupełnie nowego kształtu obowiązującej dyrektywie o prywatności i łączności elektronicznej, lecz przez zaproponowanie doraźnych zmian, które służą przede wszystkim wzmocnieniu przepisów dotyczących bezpieczeństwa i poprawieniu mechanizmów ich egzekwowania.

We wspomnianej opinii poruszono następujące zagadnienia:

- zakres zastosowania dyrektywy o e-prywatności, w szczególności usługi, których ma ona dotyczyć (proponowana zmiana w art. 3 ust. 1);
- powiadamianie o przypadkach naruszenia bezpieczeństwa (proponowana zmiana polegająca na dodaniu art. 4 ust. 3 i 4);
- przepisy dotyczące plików *cookie*, oprogramowania szpiegującego i podobnych urządzeń (proponowana zmiana w art. 5 ust. 3);
- występowanie na drogę sądową przez dostawców usług łączności elektronicznej i inne osoby prawne (proponowana zmiana polegająca na dodaniu art. 13 ust. 6); oraz
- usprawnienie egzekwowania przepisów (proponowana zmiana polegająca na dodaniu art. 15a).

Po wydaniu tej opinii Inspektor brał czynny udział w kolejnych etapach procedury legislacyjnej (zob. sekcja 3.6).

⁽²⁷⁾ Opinia z dnia 10 kwietnia 2008 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. C 181 z 18.7.2008, s.1).

Komputerowe systemy rezerwacji

W dniu 11 kwietnia 2008 r. Inspektor przedstawił opinię na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie kodeksu postępowania dla komputerowych systemów rezerwacji ⁽²⁸⁾.

Celem tego wniosku jest zaktualizowanie przepisów kodeksu postępowania dla komputerowych systemów rezerwacji, który został ustanowiony w 1989 roku na mocy rozporządzenia Rady (EWG) nr 2299/89. Kodeks zdaje się coraz mniej przystawać do nowych warunków rynkowych; aby mógł on wzmocnić konkurencję, należałoby go uprościć, a jednocześnie utrzymać podstawowe zabezpieczenia oraz zagwarantować konsumentom dostarczanie obiektywnych informacji.

Inspektor doszedł do następujących wniosków:

- Z zadowoleniem przyjął uwzględnienie w omawianym wniosku zasad ochrony danych, które doprecyzowują przepisy dyrektywy 95/46/WE. Przepisy te zwiększają pewność prawa; celowe byłoby ponadto uzupełnienie ich dodatkowymi zabezpieczeniami dotyczącymi następujących trzech punktów: zapewnienia w pełni świadomej zgody osoby, której dane dotyczą, na przetwarzanie danych szczególnie chronionych, zapewnienia środków bezpieczeństwa uwzględniających różne usługi oferowane przez komputerowe systemy rezerwacji, a także ochrony danych marketingowych.
- Jeżeli chodzi o zakres zastosowania wspomnianego wniosku, w związku z kryteriami, które sprawiają, że wniosek ten ma zastosowanie do KSR umiejscowionych w państwach trzecich, pojawiła się kwestia jego praktycznego stosowania w sposób spójny z *lex generalis*, tzn. dyrektywą 95/46/WE.
- Aby zapewnić skuteczne wykonanie wniosku należy, zdaniem Inspektora, potraktować całą problematykę komputerowych systemów rezerwacji w sposób przejrzysty i kompleksowy, z uwzględnieniem złożoności sieci KSR i warunków dostępu stron trzecich do danych osobowych przetwarzanych przez KSR.

Eurojust

W dniu 25 kwietnia 2008 r. Inspektor udzielił porady na temat inicjatywy grupy państw członkowskich mającej na celu przyjęcie decyzji Rady w

⁽²⁸⁾ Opinia z dnia 11 kwietnia 2008 r. na temat wniosku dotyczącego rozporządzenia w sprawie kodeksu postępowania dla komputerowych systemów rezerwacji (Dz.U. C 233 z 11.9.2008, s. 1).

sprawie wzmocnienia Eurojustu i zmiany decyzji 2002/187/WSiSW⁽²⁹⁾.

Inicjatywa ta ma na celu dalszą poprawę skuteczności działania Eurojustu.

Inspektor zaproponował kilka zmian do wniosku, które obejmują między innymi:

- zamieszczenie odesłania do decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Wykaz danych osobowych, które można przetwarzać na mocy wspomnianej decyzji Rady, powinien zachować charakter zamknięty.
- włączenie przepisu podobnego do przepisu zawartego w art. 38 ust. 5a wniosku dotyczącego decyzji Rady ustanawiającej Europejski Urząd Policji (Europol), dzięki czemu ustalone zostanie, że do przetwarzania danych osobowych pracowników Eurojustu mają zastosowanie przepisy rozporządzenia (WE) nr 45/2001.

Bezpieczeństwo ruchu drogowego

W dniu 8 maja 2008 r. Inspektor przedstawił opinię na temat wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady wprowadzającej ułatwienia w transgranicznym egzekwowaniu prawa dotyczącego bezpieczeństwa drogowego⁽³⁰⁾. Wspomniany wniosek jest środkiem podjętym w ramach ogólnego celu zakładającego ograniczenie liczby zabitych i rannych w wypadkach drogowych oraz zmniejszenie szkód materialnych będących rezultatem tych wypadków. Wniosek dąży zatem do stworzenia systemu, który ułatwi transgraniczne egzekwowanie kar za określone przestępstwa i wykroczenia drogowe. Aby przyczynić się do niedyskryminacyjnego i skuteczniejszego egzekwowania kar wobec sprawców przestępstw i wykroczeń drogowych, wniosek przewiduje stworzenie systemu transgranicznej wymiany informacji między państwami członkowskimi.

Wspomniana opinia zawiera następujące zalecenia:

- Jeśli chodzi o informowanie osób, których dane dotyczą: sposób, w jaki osoby, których dane dotyczą, będą informowane o przysługujących im szczegółowych prawach, będzie zależał od formatu powiadomienia o popełnieniu przestępstwa lub

wykroczenia. Ważne jest zatem, by wniosek zawierał wszystkie informacje istotne dla osoby, której dane dotyczą, w zrozumiałym dla niej języku.

- Jeśli chodzi o kwestie bezpieczeństwa: Inspektor nie ma zastrzeżeń co do wykorzystywania przy wymianie informacji istniejącej już infrastruktury, jednak podkreśla, że nie powinno to prowadzić do interoperacyjności z innymi bankami danych. Z zadowoleniem przyjął wprowadzone we wniosku ograniczenie dotyczące wykorzystywania danych przez państwa członkowskie inne niż państwo, w którym przestępstwo lub wykroczenie zostało popełnione.
- Inspektor chętnie wypowie się też, gdy Komisja będzie opracowywać wspólne przepisy dotyczące procedur technicznych elektronicznej wymiany danych między państwami członkowskimi, zwłaszcza na temat aspektów bezpieczeństwa tych przepisów.

Statystyki europejskie

W dniu 20 maja 2008 r. Inspektor wydał opinię na temat wniosku dotyczącego rozporządzenia w sprawie statystyk europejskich⁽³¹⁾. Wspomniany wniosek ma na celu dokonanie zmiany aktualnie obowiązujących podstawowych ram prawnych, które dotyczą tworzenia statystyk na szczeblu europejskim, po to by dostosować je do obecnych realiów oraz by je ulepszyć w sposób umożliwiający uwzględnianie przyszłych postępów i wyzwań.

Inspektor z zadowoleniem przyjął ten wniosek, gdyż będzie on stanowić trwałą i powszechnie obowiązującą podstawę prawną opracowywania, tworzenia i rozpowszechniania statystyk na szczeblu europejskim. Zwrócił jednak uwagę na następujące punkty:

- Inspektor oczekuje, że zostanie poproszony o opinię w sprawie przepisów sektorowych odnoszących się do statystyk, które to przepisy Komisja może przyjąć w celu wdrożenia wspomnianego rozporządzenia po jego przyjęciu;
- Należy ponownie zastanowić się nad proponowanym pojęciem „podmiotu danych statystycznych”, tak aby nie było ono mylone z pojęciami z dziedziny ochrony danych.
- Przy dokonywaniu przez Komisję oceny jakości danych należy uwzględnić zasadę zachowania odpowiedniej jakości danych.
- W kontekście rozpowszechniania danych należy uwzględnić wieloznaczność pojęcia „przetwarzanie danych w celu zachowania anonimowości”.

⁽²⁹⁾ Opinia z dnia 25 kwietnia 2008 r. na temat inicjatywy 14 państw członkowskich mającej na celu przyjęcie decyzji Rady w sprawie wzmocnienia Eurojustu i zmiany decyzji 2002/187/WSiSW (Dz.U. C 310 z 5.12.2008, s. 1).

⁽³⁰⁾ Opinia z dnia 8 maja 2008 r. na temat wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady wprowadzającej ułatwienia w transgranicznym egzekwowaniu prawa dotyczącego bezpieczeństwa drogowego (Dz.U. C 310 z 5.12.2008, s. 9).

⁽³¹⁾ Opinia z dnia 20 maja 2008 r. na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie statystyk europejskich (COM(2007) 625 wersja ostateczna) (Dz.U. C 308 z 3.12.2008, s. 1).



Dzieci są łatwym celem w Internecie.
Aby je chronić, potrzebne są odpowiednie środki ochrony danych.

Ochrona dzieci korzystających z Internetu

W dniu 23 czerwca 2008 r. Inspektor przyjął opinię na temat wniosku dotyczącego decyzji Parlamentu Europejskiego i Rady w sprawie ustanowienia wieloletniego wspólnotowego programu ochrony dzieci korzystających z Internetu i z innych technologii komunikacyjnych⁽³²⁾.

Wyraził zadowolenie z tego, że wspomniany program ma być ukierunkowany na rozwój nowych technologii oraz przygotowanie konkretnych działań zwiększających skuteczność ochrony dzieci. Zasadniczym warunkiem bezpieczeństwa dzieci korzystających z Internetu jest ochrona danych osobowych. Należy zapobiegać niewłaściwemu wykorzystywaniu danych osobowych dzieci, podejmując działania zaproponowane w programie, a zwłaszcza:

- rozwijając świadomość u dzieci i innych zaangażowanych stron, np. rodziców i wychowawców;
- propagując wypracowywanie najlepszych wzorców przez usługodawców;
- propagując opracowywanie narzędzi technicznych pozwalających respektować prywatność;

⁽³²⁾ Opinia z dnia 23 czerwca 2008 r. na temat wniosku dotyczącego decyzji w sprawie ustanowienia wieloletniego wspólnotowego programu ochrony dzieci korzystających z Internetu i z innych technologii komunikacyjnych (Dz.U. C 2 z 7.1.2009, s. 2).

— sprzyjając wymianie dobrych wzorców oraz praktycznych doświadczeń przez odpowiednie organy, w tym organy ochrony danych.

Działania te należy podejmować, nie zapominając o tym, że tam, gdzie chroni się dzieci, w grę mogą wchodzić także prawa innych osób. Inspektor przypomniał zwłaszcza, że nadzór nad sieciami telekomunikacyjnymi powinien być zadaniem organów ochrony porządku publicznego.

Odnótował również, że przedmiotowy program stanowi ogólną podstawę do dalszych konkretnych działań. Zalecił, by w opracowywanie tych praktycznych projektów ściśle włączyć organy ds. ochrony danych.

Publiczny dostęp do dokumentów

W dniu 30 czerwca 2008 r. Inspektor przedstawił opinię na temat wniosku dotyczącego rozporządzenia w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji⁽³³⁾. Wniosek został poprzedzony publicznymi konsultacjami. Po przyjęciu wniosku w czerwcu 2008 roku dożyło się wysłuchanie publiczne na forum Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (LIBE). Przy tej okazji przedstawiciele Komisji Europejskiej podkreślili, że chociaż wniosek odzwierciedla obecny stan rzecz, są oni otwarci na dyskusję nad tekstem i rozważenie propozycji ulepszenia go, nie wykluczając rozwiązań alternatywnych.

Inspektor potraktował takie otwarte jako szansę i dążył do wzbogacenia dyskusji o alternatywny tekst proponowanego art. 4 ust. 5, który dotyczy trudnej relacji między dostępem do dokumentów a prawem do prywatności i do ochrony danych osobowych. Wspomniany przepis miał wprowadzić

⁽³³⁾ Opinia z dnia 30 czerwca 2008 r. na temat wniosku dotyczącego rozporządzenia w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. C 2 z 7.1.2009, s. 7).

w życie wyrok Sądu Pierwszej Instancji w sprawie *Bavarian Lager* (sprawa T-194/04). Inspektor w pewnym stopniu poparł argumenty przemawiające za zastąpieniem art. 4 ust. 1 lit. b) nowym przepisem, lecz nie poparł samego przepisu.

Przepis ten spotkał się z jego krytyką z następujących względów:

- Inspektor nie był przekonany, czy jest to odpowiedni czas na zmiany, gdyż Europejski Trybunał Sprawiedliwości nie rozpatrzył jeszcze odwołania dotyczącego zasadniczych kwestii.
- Wniosek nie zapewnił odpowiedniego rozwiązania, gdyż zawiera on ogólną zasadę (art. 4 ust. 5 zdanie drugie), która:
 - nie odzwierciedla wyroku Sądu Pierwszej Instancji w sprawie *Bavarian Lager*;
 - nie zapewnia właściwej równowagi pomiędzy wchodzącymi tu w grę podstawowymi prawami;
 - jest nierealistyczna, ponieważ odwołuje się do prawodawstwa WE dotyczącego ochrony danych, które nie daje jasnej odpowiedzi w sytuacjach, gdy trzeba podjąć decyzję o publicznym dostępie do dokumentów.
- Ponadto zawiera on konkretną zasadę (art. 4 ust. 5 zdanie pierwsze), która jest wprawdzie dobrze zdefiniowana, ale ma zdecydowanie zbyt ograniczony zakres.

ECRIS

W dniu 16 września 2008 r. Inspektor udzielił porady na temat wniosku dotyczącego decyzji Rady w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2008/.../WSiSW⁽³⁴⁾.

Wniosek ma na celu wykonanie przepisów art. 11 decyzji ramowej Rady w sprawie organizacji wymiany informacji pochodzących z rejestru skazanych pomiędzy państwami członkowskimi oraz treści tych informacji, by stworzyć i rozwinąć skomputeryzowany system wymiany informacji między państwami członkowskimi. Ustanawia on ECRIS oraz elementy standardowego formatu elektronicznej wymiany informacji, a także inne ogólne i techniczne aspekty wdrażania systemu, tak by zorganizować i ułatwić wymianę informacji.

Inspektor poparł wniosek i zgłosił parę uwag.

- Aby zagwarantować pewność prawa, należy doprecyzować kwestię odpowiedzialności Komisji za wspólną infrastrukturę systemu, a także możliwości zastosowania rozporządzenia (WE) nr 45/2001.
- Ponadto nie państwa członkowskie, jak przewidziano we wniosku, lecz Komisja powinna odpowiadać za oprogramowanie ECRIS do łączności, tak by poprawić skuteczność wymiany informacji i umożliwić lepszy nadzór nad systemem.
- Zastosowanie automatycznego tłumaczenia powinno zostać wyraźnie objaśnione i ograniczone; ma ono ułatwiać wzajemne zrozumienie kategorii przestępstw kryminalnych bez oddziaływania na jakość przekazywanych informacji.

Dostępność informacji o majątku dłużnika

W marcu 2008 r. Komisja Europejska wydała zieloną księgę w sprawie dostępności informacji o majątku dłużnika⁽³⁵⁾. Analizowana zielona księga

⁽³⁴⁾ Opinia z dnia 16 września 2008 r. na temat wniosku dotyczącego decyzji Rady w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2008/.../WSiSW (Dz.U. C 42 z 20.2.2009, s. 1).

⁽³⁵⁾ COM (2008) 128 wersja ostateczna.



Inspektor przyczynia się do właściwej równowagi między publicznym dostępem do dokumentów UE a prywatnością

skupia się na środkach, jakie można by przyjąć na poziomie UE, by „poprawić dostępność informacji o majątku dłużnika oraz ułatwić wierzycielom korzystanie z prawa do uzyskania takich informacji, (...) z zachowaniem zasad ochrony prawa do prywatności dłużnika” zgodnie z przepisami dyrektywy 95/46/WE.

W dniu 22 września 2008 r. Inspektor przedstawił opinię na temat zielonej księgi ⁽³⁶⁾, w której to opinii zalecił, by w ramach ewentualnych działań legislacyjnych wynikających z omawianej zielonej księgi zadbano o to, by przetwarzanie danych osobowych przez różnorodne organy egzekucyjne podyktowane było co najmniej jednym spośród względów prawnych określonych w art. 7 dyrektywy 95/46/WE. Inspektor zwrócił się także o należyte uwzględnienie zasady proporcjonalności oraz o to, by wszelkie środki dotyczące dostępności informacji o majątku dłużnika były zgodne z zasadą ograniczenia celu, a wszelkie niezbędne wyjątki – z warunkami określonymi w art. 13 dyrektywy 95/46/WE.

Grupa kontaktowa wysokiego szczebla UE–USA ds. wymiany informacji

W dniu 11 listopada 2008 r. Inspektor przedstawił opinię na temat sprawozdania końcowego grupy kontaktowej wysokiego szczebla UE–USA ds. wymiany informacji oraz ochrony prywatności i danych osobowych ⁽³⁷⁾. W sprawozdaniu tym starano się wskazać wspólne zasady, którym podlegałaby ochrona prywatności i danych, a tym samym uczynić pierwszy krok ku wymianie informacji między UE a USA do celów walki z terroryzmem i poważną przestępczością międzynarodową.

W swojej opinii Inspektor zwrócił uwagę na to, że taki transatlantycki instrument dotyczący ochrony danych należy rozpatrywać, uwzględniając obowiązujące przepisy prawne oraz skutki tego instrumentu dla obywateli. Inspektor opowiedział się za umową, która byłaby prawnie wiążąca, co miałoby zagwarantować dostateczną pewność prawa.

⁽³⁶⁾ Opinia z dnia 22 września 2008 r. na temat zielonej księgi Komisji w sprawie skutecznego wykonywania orzeczeń w Unii Europejskiej: dostępność informacji o majątku dłużnika — COM(2008) 128 wersja ostateczna (Dz.U. C 20 z 27.1.2009, s. 1).

⁽³⁷⁾ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf

Ponadto zaapelował o większą precyzję i uszczegółowienie przepisów, zwłaszcza przepisów, które odnoszą się do następujących kwestii:

- dokładne badanie stopnia ochrony danych, oparte na podstawowych wymogach odnoszących się do treści, szczegółów i nadzoru systemu; Inspektor uważa, że instrument o charakterze ogólnym mógłby zostać uznany za odpowiedni tylko wtedy, gdy towarzyszyłyby mu odpowiednie, zawierane w poszczególnych przypadkach umowy szczegółowe;
- wyraźnie wskazany zakres zastosowania umowy oraz jasne wspólne definicje celów związanych z egzekwowaniem prawa, do których się dąży;
- silne mechanizmy nadzoru oraz mechanizmy odwoławcze dostępne dla osób, których dane dotyczą, w tym administracyjne i sądowe środki odwoławcze
- skuteczne środki gwarantujące osobom, których dane dotyczą, możliwość korzystania ze swoich praw niezależnie od obywatelstwa;
- zaangażowanie niezależnych organów ochrony danych zwłaszcza w nadzór i w pomoc osobom, których dane dotyczą.

Inspektor zalecił także opracowanie planu prac, który na późniejszym etapie prowadziłyby do ewentualnego sporządzenia umowy. Zaapelował również o większą przejrzystość podczas opracowywania zasad rządzących ochroną danych. Zaangażowanie wszystkich zainteresowanych stron, w tym Parlamentu Europejskiego, jest warunkiem tego, by przyszły akt odniósł korzyść z demokratycznej debaty i zdobył niezbędne poparcie i uznanie.

Transgraniczna opieka zdrowotna

W dniu 2 grudnia 2008 r. Inspektor udzielił porady na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej ⁽³⁸⁾. Celem tego wniosku jest ustanowienie wspólnotowych ram udzielania transgranicznej opieki zdrowotnej w UE, w przypadkach gdy dana forma opieki poszukiwana przez pacjentów świadczona jest w państwie członkowskim innym niż ich własne państwo.

⁽³⁸⁾ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-02_Cross-border_healthcare_EN.pdf

Inspektor popiera inicjatywy, które mają na celu poprawę warunków transgranicznej opieki zdrowotnej. Wyraził jednak zaniepokojenie faktem, że inicjatywy WE w zakresie opieki zdrowotnej nie zawsze są należycie skoordynowane pod względem wykorzystania technologii informacyjno-komunikacyjnych (TIK) oraz pod względem prywatności i bezpieczeństwa, co opóźnia przyjęcie ogólnego podejścia w zakresie ochrony danych w dziedzinie opieki zdrowotnej.

Inspektor z zadowoleniem przyjął odniesienie do prywatności zawarte we wspomnianym wniosku. Jego sugestie były następujące:

- należy zamieścić definicję danych dotyczących zdrowia, która będzie obejmowała wszelkie dane osobowe mogące mieć oczywisty i ścisły związek z opisem stanu zdrowia danej osoby; powinna ona zasadniczo objąć dane medyczne, jak również dane administracyjne i finansowe dotyczące zdrowia;
- należy wprowadzić konkretny artykuł dotyczący ochrony danych, jasno przedstawiający pełen obraz, w którym opisano by zobowiązania państw członkowskich ubezpieczenia i leczenia oraz określono główne obszary dalszych prac, tj. w zakresie harmonizacji pod względem bezpieczeństwa oraz uwzględniania prywatności zwłaszcza w aplikacjach dotyczących e-zdrowia;
- zaleca się, aby w proponowanym wspólnotowym wzorze recepty elektronicznej uwzględnić koncepcję „wbudowanej ochrony prywatności”.

Europejska strategia w dziedzinie e-sprawiedliwości

W dniu 19 grudnia 2008 r. Inspektor wydał opinię w sprawie komunikatu Komisji dotyczącego europejskiej strategii w dziedzinie e-sprawiedliwości ⁽³⁹⁾. Komunikat ten służy zaprezentowaniu e-strategii, która ma zwiększyć zaufanie obywateli do europejskiej przestrzeni sprawiedliwości. Głównym celem e-sprawiedliwości powinna być pomoc w skuteczniejszym wymierzaniu sprawiedliwości w Europie z korzyścią dla obywateli. Działania UE powinny ułatwiać obywatelom dostęp do informacji bez względu na bariery językowe, kulturowe i prawne wynikające z wielości systemów.

⁽³⁹⁾ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-19_eJustice_EN.pdf.

Inspektor poparł wspomniany wniosek z zastrzeżeniem uwag, które zawarł w swojej opinii; dotyczyły one:

- uwzględnienia decyzji ramowej Rady 2008/977/WSiSW w sprawie ochrony danych osobowych w dziedzinie współpracy policyjnej i sądowej w sprawach karnych;
- włączenia do e-sprawiedliwości procedur administracyjnych;
- dalszego preferowania systemów zdecentralizowanych z jasno określonym zakresem odpowiedzialności wszystkich podmiotów przetwarzających dane osobowe w przewidywanych systemach; za wspólną infrastrukturę powinna być odpowiedzialna Komisja;
- gwarantowania, by połączenia między systemami i interoperacyjność systemów naleźycie uwzględniały zasadę ograniczenia celu;
- dbania o to, by przetwarzanie danych osobowych do celów innych niż te, do których je zebrano, odbywało się z zachowaniem szczególnych warunków ustanowionych na mocy mających zastosowanie przepisów dotyczących ochrony danych.

3.4. Uwagi

Uwagi są prostszym niż opinie prawne narzędziem interwencji. Inspektor korzysta z tego narzędzia, w przypadkach gdy pełna analiza prawna nie wydaje się konieczna. Uwagi zawierają analizę polityki i dostarczają konstruktywnych zaleceń, które służą temu, by proponowane działania były odpowiednio zgodne z zasadami ochrony danych i by takie zasady propagowały.

Zarządzanie granicami

W dniu 3 marca 2008 r. Inspektor przedstawił wstępne uwagi odnoszące się do trzech komunikatów Komisji Europejskiej dotyczących zarządzania granicami zewnętrznymi UE ⁽⁴⁰⁾. Uwagi skupiły się na środkach, które budzą zastrzeżenia z punktu widzenia ochrony danych, zwłaszcza na utworzeniu systemu wjazdu/wyjazdu obejmującego rejestrowanie informacji o podróżnych, wykorzystywaniu danych biometrycznych oraz

⁽⁴⁰⁾ COM (2008) 69, COM (2008) 68 i COM (2008) 67.

ewentualnym utworzeniu dużej bazy danych UE do przechowywania wspomnianych danych.

Inspektor podkreślił, że proponowane środki, chociaż są zasadne, gdyż mają na celu sprawienie, by granice UE stały się bezpieczniejsze, a podróże osób przemieszczających się w uczciwych celach – łatwiejsze, wymagają dokładnej analizy; zakładają one bowiem prowadzenie operacji przetwarzania danych na dużą skalę, wiążących się z poważną ingerencją w prywatność. Inspektor zwrócił uwagę na to, że niezwykle istotne jest, by odpowiednio uwzględnić wpływ, jaki będzie to miało na prawo do prywatności osób przekraczających granice UE. Brak zabezpieczeń służących ochronie danych oznaczałby nie tylko to, że dane osoby mogłyby ponieść nadmierne szkody w związku z proponowanymi środkami, lecz także że środki te przez zmniejszenie społecznego zaufania do działań administracji, byłyby mniej skuteczne czy nawet przyniosłyby skutek przeciwny do zamierzonego.

Uwagi inspektora zawierały także ogólne spostrzeżenia dotyczące: nagromadzenia wniosków prawodawczych w omawianej dziedzinie, wagi przywiązywanej do danych biometrycznych oraz braku dowodów uzasadniających potrzebę tworzenia nowych systemów danych.

Decyzja Komisji dotycząca IMI – działania w związku z opinią Inspektora z dnia 22 lutego 2008 r.

W dniu 14 lipca 2008 r. Inspektor odpowiedział na pismo Komisji, w którym proponowała ona dalsze działania zmierzające do pełniejszego wdrożenia niezbędnych zabezpieczeń służących ochronie danych do celów systemu wymiany informacji na rynku wewnętrznym (IMI).

Inspektor zgodził się, że przyjęcie wytycznych w zakresie ochrony danych w formie zaleceń Komisji jest istotnym i właściwym krokiem w kierunku ustanowienia kompleksowych ram ochrony danych do celów IMI. Podkreślił, że zakres działania IMI, który obecnie ogranicza się do wymiany informacji na mocy dyrektywy usługowej i dyrektywy o kwalifikacjach zawodowych, będzie stopniowo rozszerzany na dodatkowe obszary prawodawstwa dotyczącego rynku wewnętrznego. Spowoduje to większą złożoność IMI oraz wzrost liczby organów uczestniczących i przeprowadzanych operacji wymiany danych. W związku z tym, konieczne będzie, zdaniem Inspektora, by w prawnie wiążącym prawodawstwie wspólnotowym przewidzieć konkretne zabezpieczenia służące ochronie danych, które to zabezpieczenia powinny wykraczać poza obecnie stosowane przepisy w zakresie ochrony danych.

Usługa powszechna i e-prywatność – działania w związku z opinią Inspektora z dnia 10 kwietnia 2008 r.

Jeśli chodzi o dyrektywę o e-prywatności i dyrektywę o usłudze powszechnej, Inspektor przedstawił uwagi co do wybranych kwestii zasygnalizowanych w sprawozdaniu Komisji Rynku Wewnętrznego i Ochrony Konsumentów (IMCO) poświęconym przeglądowi dyrektywy 2002/22/WE. W dniu 2 września 2008 r. Inspektor wysunął zastrzeżenia co do niektórych zmian wprowadzonych *ad hoc* w sprawozdaniu Komisji IMCO, które, jeżeli zostaną przyjęte, spowodują osłabienie ochrony danych osobowych i prywatności osób korzystających z Internetu (zob. także sekcja 3.6).

3.5. Interwencje przed Trybunałem

Inspektor ma prawo występować przed Europejskim Trybunałem Sprawiedliwości w sprawach istotnych dla swoich zadań. Prawo to rozciąga się na wszystkie sprawy wspólnotowe mające związek z przetwarzaniem danych osobowych.

Prawo do występowania w sądzie opiera się na art. 47 rozporządzenia (WE) 45/2001 i obejmuje także Sąd Pierwszej Instancji oraz Sąd ds. Służby Publicznej. Wystąpienia Inspektora służą wyjaśnieniu koncepcji ochrony danych.

W dniu 1 lipca 2008 r. Inspektor uczestniczył w rozprawie dotyczącej sprawy C-301/06, *Irlandia przeciwko Radzie i Parlamentowi*. Inspektor przedstawił argumenty za tym, że dyrektywa o zatrzymywaniu danych (2006/24/WE) słusznie opiera się na art. 95 Traktatu WE ⁽⁴¹⁾.

Ponadto zwrócił się o to, by dopuszczono go do udziału w następujących sprawach:

- sprawa C-518/07 (*Komisja przeciwko Niemcom*) przed Europejskim Trybunałem Sprawiedliwości dotycząca niezależności organów ds. ochrony danych,
- sprawa T-3/08 (*Coédo Suárez przeciwko Radzie*) przed Sądem Pierwszej Instancji dotycząca prawa dostępu w rozporządzeniu o ochronie danych,
- sprawa F-35/08 (*Pachtitis przeciwko Komisji*) przed Sądem ds. Służby Publicznej dotycząca prawa dostępu w rozporządzeniu o ochronie danych,

⁽⁴¹⁾ Pisma procesowe Inspektora można znaleźć na jego stronie internetowej.

- sprawa F-48/08 (*Ortega Serrano* przeciwko *Komisji*) przed Sądem ds. Służby Publicznej dotycząca prawa dostępu w rozporządzeniu o ochronie danych,
- sprawa T-382/08 (*Advance Magazine Publishers* przeciwko *UHRW*) przed Sądem Pierwszej Instancji dotycząca publicznego dostępu do dokumentów.

Sądy dopuściły Inspektora do udziału w pierwszych trzech sprawach. W sprawie F-48/08 samo odwołanie zostało uznane za niedopuszczalne, natomiast jeśli chodzi o sprawę T-382/08, sąd nie podjął jeszcze decyzji co do wniosku Inspektora.

Inspektor przedłożył uwagi co do istoty sprawy w trzech przypadkach.

- W sprawie C-518/07 Inspektor przedłożył uwagi interwenienta popierające Komisję;
- W sprawie C-28/08 P (*Komisja* przeciwko *Bavarian Lager*) Inspektor wydał odpowiedź na odwołanie Komisji (sprawa C-28/08 P) od wyroku Sądu Pierwszej Instancji z dnia 8 listopada 2007 r. w sprawie *Bavarian Lager* T-194/04. Odpowiedział także, jako strona postępowania, na uwagi interwenientów;
- W sprawie T-374/07 (*Pachtitis* przeciwko *Komisji i EPSO*) przedłożył uwagi interwenienta popierające Komisję.

3.6. Inne rodzaje działań

3.6.1. E-prywatność

Przez cały rok stałej uwagi Inspektora wymagał wniosek Komisji dotyczący zmiany dyrektywy o e-prywatności⁽⁴²⁾.

W dniu 2 września 2008 r. Inspektor przedstawił uwagi dotyczące wybranych kwestii związanych z przetwarzaniem danych o ruchu oraz z ochroną praw własności intelektualnej⁽⁴³⁾. Następnie w tym samym miesiącu Parlament Europejski przyjął rezolucję legislacyjną w sprawie dyrektywy o e-prywatności⁽⁴⁴⁾. Wśród istotnych zmian było objęcie dostawców usług społeczeństwa informacyjnego

⁽⁴²⁾ Zob. także sekcja 3.3.2. dotycząca poszczególnych opinii.

⁽⁴³⁾ Zob. sekcja 3.4.

⁽⁴⁴⁾ Rezolucja legislacyjna Parlamentu Europejskiego z dnia 24 września 2008 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników oraz dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy w dziedzinie ochrony konsumentów (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)).



Inspektor przedstawił Komisji Europejskiej, Parlamentowi i Radzie obszerne uwagi dotyczące przeglądu dyrektywy o prywatności i łączności elektronicznej

obowiązkiem powiadamiania o przypadkach naruszenia bezpieczeństwa.

Inspektor z zadowoleniem przyjął tę zmianę, a także poprawkę umożliwiającą osobom prawnym i prywatnym podejmowanie działań w przypadku stwierdzenia naruszenia jakiegokolwiek przepisu dyrektywy o e-prywatności. W dniu 17 września 2008 r. Inspektor przedstawił swoje zdanie na wysłuchaniu zorganizowanym przez posłów z różnych grup politycznych Parlamentu Europejskiego. Przy innych okazjach wymienił z posłami i innymi zainteresowanymi podmiotami poglądy na temat kwestii, takich jak powiadomienie o przypadkach naruszenia bezpieczeństwa, przetwarzanie adresów IP oraz normy przyczyniające się do opracowania produktów korzystnych z punktu widzenia ochrony prywatności.

W listopadzie 2008 roku Rada osiągnęła porozumienie polityczne w sprawie przeglądu przepisów dotyczących pakietu telekomunikacyjnego, w tym dyrektywy o e-prywatności. Rada wprowadziła zmiany w istotnych elementach wniosku i nie wyraziła zgody na wiele spośród poprawek przyjętych przez Parlament Europejski. Inspektor wyraził zastrzeżenia co do treści wspólnego stanowiska, gdyż usunięto z niego lub w istotny sposób osłabiono zabezpieczenia dla obywateli. W rezultacie poziom ochrony przyznanej osobom we wspólnym stanowisku jest znaczenie słabszy.

Dlatego też Inspektor zapowiedział wydanie drugiej opinii, którą ostatecznie przyjął 9 stycznia 2009 r. (zostanie ona omówiona w sprawozdaniu za rok 2009).

3.6.2. PNR

Tak jak w latach poprzednich Inspektor był ściśle zaangażowany w sprawy związane z PNR. W 2008 roku wiele energii poświęcił działaniom w następstwie wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu egzekwowania prawa⁽⁴⁵⁾, wewnętrznego systemu UE służącego gromadzeniu i wykorzystywaniu danych pasażerów linii lotniczych, którzy wjeżdżają na terytorium UE lub je opuszczają. Inspektor brał aktywny udział w pracach prowadzonych podczas prezydencji francuskiej; zakwestionował w szczególności niezbędność i proporcjonalność tego systemu. Wspomniane prace będą kontynuowane podczas prezydencji czeskiej i szwedzkiej.

Nieznana jest szacowana data przyjęcia omawianego wniosku przez Radę. Inspektor zamierza nadal dokładnie śledzić rozwój sytuacji i prawdopodobnie wyda drugą opinię.

3.6.3. Wdrożenie SIS i polityka dotycząca granic

Jak już wcześniej stwierdzono (sekcja 3.1), Inspektor przyjmuje szeroką interpretację swoich zadań doradczych dotyczących wniosków prawodawczych. Stara się on jednak różnicować intensywność wykonywania zadań doradczych w zależności od wpływu poszczególnych wniosków na ochronę danych osobowych. Obecnie niezwykle istotne są wnioski dotyczące przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Kluczowe zagadnienia w tej dziedzinie to wymiana informacji w ramach współpracy policji i wymiaru sprawiedliwości, a także kwestie dotyczące dużych systemów informacyjnych, takich jak Eurodac, wizowy system informacyjny (VIS) oraz system informacyjny Schengen drugiej generacji (SIS II). SIS II składa się z centralnej bazy danych zwanej „centralnym systemem informacyjnym Schengen” (CS-SIS), której zarządzanie operacyjne zapewnia Komisja i która połączona jest z krajowymi punktami dostępu określonymi przez każde państwo członkowskie (NI-SIS). Organy Sirene zapewniają wymianę wszelkich informacji uzupełniających (informacje związane z wpisami do SIS II, ale nie zachowywane w SIS II).

W dniu 30 czerwca 2008 r. Inspektor dwukrotnie zabrał głos podczas spotkania przy okrągłym stole zorganizowanego przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw

Wewnętrznych Parlamentu Europejskiego z udziałem przedstawicieli Parlamentu Europejskiego oraz parlamentów krajowych. Spotkanie to poświęcone było następującemu zagadnieniu: „Wolność i bezpieczeństwo a zintegrowane zarządzanie granicami Unii Europejskiej – wymiana poglądów na temat nowego systemu informacyjnego Schengen (SIS II), FRONTEKSU, EUROSUR-u, systemu wjazdu/wyjazdu i profilowania”.

W pierwszym wystąpieniu Inspektor poruszył kwestię „Wpływu migracji z SIS I+ do SIS II na ochronę danych”. Jeśli chodzi o jednostkę centralną, którą Inspektor ma nadzorować, podkreślił, że zamierza przeprowadzić audyt już na pierwszym etapie działań, po to by zapewnić narzędzie benchmarkingu na przyszłość. Przypomniał również, jak ważna dla zapewnienia płynnego przejścia z jednego do drugiego systemu jest współpraca z krajowymi organami ochrony danych i ze Wspólnym Organem Nadzorczym Schengen.

W drugim wystąpieniu podczas posiedzenia poświęconego „Ochronie wolności, bezpieczeństwa i prywatności w ramach przyszłego zarządzania granicami UE” Inspektor kilkakrotnie nawiązał do swoich uwag na temat pakietu dotyczącego zarządzania granicami. Przypomniał niektóre najważniejsze punkty tych uwag, np. to, że należy się zastanowić, zanim przedstawi się nowe wnioski, nie oceniwszy istniejących warunków. Poruszył również kwestię profilowania, które, choć w pewnych okolicznościach jest pożyteczne, wymaga odpowiednich zabezpieczeń, gdyż może wiązać się z ingerencją w prywatne życie obywateli.

3.6.4. Konferencja na temat ochrony danych i egzekwowania prawa (Trewir)

W dniach 26 i 27 maja 2008 r. Inspektor i Akademia Prawa Europejskiego (ERA) zorganizowali wspólnie konferencję w Trewirze poświęconą wymianie i ochronie danych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Na seminarium tym omówiono odnośne prawodawstwo UE. Analiza i debata skupiły się na głównych dokumentach dotyczących wymiany danych, takich jak konwencja z Prüm i najnowsza decyzja dotycząca włączenia jej w ramy prawne UE. Jeśli chodzi o ochronę danych, na wspomnianym seminarium zajęto się w szczególności decyzją ramową w sprawie ochrony danych w ramach współpracy policyjnej i sądowej w sprawach karnych.

Wśród innych kwestii znalazły się: rosnąca rola danych gromadzonych przez przedsiębiorstwa

⁽⁴⁵⁾ COM(2007) 654.

prywatne (linie lotnicze, banki, operatorów telekomunikacyjnych) w egzekwowaniu prawa, nowe rozwiązania technologiczne ułatwiające gromadzenie danych oraz ramy instytucjonalne ochrony danych. Na sesji końcowej dyskutowano o przyszłości po wejściu w życie traktatu lizbońskiego.

Konferencja zgromadziła ok. 100 uczestników z licznych państw członkowskich UE. Specjaliści od ochrony danych i egzekwowania prawa omówili ramy prawne wymiany i ochrony danych w chwili obecnej i bliskiej przyszłości. W wielu wystąpieniach podkreślano, że istotne jest łączenie perspektywy ochrony danych i egzekwowania prawa, gdyż są to niezbędne elementy dobrych rządów.



Udział Inspektora w konferencji ICT 2008 (Lyon, 25–27 listopada 2008 r.)

3.6.5. Badania i rozwój technologiczny w UE

Działania w zakresie badań i rozwoju technologicznego w UE – następujące na wczesnym etapie i pozwalające na skuteczną reakcję – umożliwiają uwzględnienie, wprowadzanie i propagowanie zasad prywatności i ochrony danych zgodnie z koncepcją „wbudowanej ochrony prywatności”. W 2008 roku Inspektor doprecyzował i usystematyzował swój ewentualny wkład w dziedzinie badań i rozwoju technologicznego w UE i skonsolidował rozpoczęte już działania.

Wkład Inspektora w program ramowy w zakresie badań oraz w zaproszenia do składania wniosków obejmuje:

- udział w warsztatach i konferencjach mających na celu określenie przyszłych wyzwań, które mogą mieć znaczenie dla polityki UE w zakresie badań i rozwoju technologicznego;
- udział w organach doradczych ds. badań naukowych utworzonych przez Komisję Europejską w związku z programem ramowym oraz dostarczanie opinii na tematy dotyczące ochrony danych;
- wspieranie Komisji Europejskiej w procesie oceny wniosków, w szczególności w odniesieniu do ewentualnych kwestii ochrony danych wiążących się z tymi wnioskami.

Inspektor mógłby również wydawać opinie dotyczące indywidualnych projektów w zakresie badań i rozwoju technologicznego na wniosek konsorcjum odpowiadającego za dany projekt lub z własnej inicjatywy.

Dokument strategiczny dotyczący B&R

W kwietniu 2008 roku Inspektor przyjął dokument strategiczny pt. „Europejski Inspektor Ochrony Danych a badania i rozwój technologiczny w UE”⁽⁴⁶⁾, w którym opisana została ewentualna rola, jaką jego instytucja mogłaby odegrać w projektach związanych z badaniami i rozwojem (B&R); w ramach siódmego programu ramowego w zakresie badań i rozwoju technologicznego (7. PR). W dokumencie tym przedstawiono kryteria selekcji projektów do działań Inspektora oraz sposób, w jaki może on wносить wkład w te projekty. W związku z tym, że Inspektor posiada status niezależnego organu, nie jest możliwy jego udział w projekcie w charakterze partnera konsorcjum.

W listopadzie 2008 roku Inspektor przygotował stoisko w ramach zorganizowanych w Lyonie targów poświęconych technologiom informacyjno-komunikacyjnym (TIK), uznawanym za największe europejskie targi TIK. Przy tej okazji Inspektor miał możliwość przedstawienia wspomnianego

⁽⁴⁶⁾ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

dokumentu strategicznego ok. 4500 zarejestrowanym delegatom oraz zapewnienia tym delegatom ukierunkowanych wskazówek co do najlepszych sposobów rozpatrywania kwestii ochrony danych, z którymi mogliby się spotkać w ramach prowadzonej przez siebie działalności badawczej.

Większość rodzajów wkładu Inspektora przewidzianych w nowym dokumencie strategicznym realizowano już w 2008 roku; dotyczyły one następujących działań:

- po przeanalizowaniu elementów unijnego projektu „Turbine”⁽⁴⁷⁾ (ang. *trusted revocable biometric identities*), którego celem są badania dotyczące danych biometrycznych, Inspektor postanowił pozytywnie odpowiedzieć na wniosek konsorcjum i sporządzi opinię dotyczącą tego projektu UE w 2010 roku;
- w roku 2008 Inspektor postanowił przyjrzeć się trwającemu projektowi *Bridge* (budowa identyfikacji radiowej na rzecz globalnego środowiska)⁽⁴⁸⁾. Inspektor przesłał Komisji Europejskiej zalecenia opracowane na podstawie oceny wynikającej z ustalonych faktów oraz spotkania z pracownikami Komisji odpowiedzialnymi za ten projekt. Zgodnie z zaleceniami Inspektora Komisja Europejska zainicjowała dodatkowe działania mające na celu wyjaśnienie kwestii związanych ze zgodnością działań badawczych prowadzonych w ramach tego projektu ze wspólnotowymi przepisami dotyczącymi ochrony danych, a także zwiększenie tej zgodności;
- W 2008 roku Inspektor przekazał wielu konsorcjom odpowiedzialnym za projekty UE w zakresie badań i rozwoju technologicznego dane punktów kontaktowych krajowych organów ds. ochrony danych i umożliwił nawiązanie kontaktu z nimi. Miało to zasadniczo służyć uzyskaniu dalszych szczegółowych informacji na temat prawa właściwego w zakresie ochrony danych oraz nawiązaniu odpowiednich kontaktów umożliwiających ewentualne powiadomienia o przetwarzaniu danych osobowych.

Grupy doradcze ds. badań naukowych utworzone przez Komisję Europejską

Aby dokładniej śledzić proces określania nowych kierunków działania w zakresie badań i rozwoju technologicznego UE, Inspektor zgodził się przyjmować rolę obserwatora lub w poszczególnych przypadkach uczestniczyć w działaniach nastę-

pujących grup doradczych ds. badań naukowych zarządzanych przez Komisję Europejską:

- RISEPTIS (badania i innowacje na rzecz bezpieczeństwa, prywatności i wiarygodności w społeczeństwie informacyjnym): w 2008 roku Inspektor przyjął zaproszenie z Dyrekcji Generalnej ds. Społeczeństwa Informacyjnego i Mediów Komisji Europejskiej do udziału w tej grupie w roli obserwatora; badania nad bezpieczeństwem i zaufaniem prowadzone przez tę grupę doradczą wysokiego szczebla w zakresie TIK dążą do zapewnienia wizjonerskich zaleceń odnoszących się do wyzwań w zakresie polityki i badań dotyczących bezpieczeństwa i zaufania w społeczeństwie informacyjnym;
- ESRIF (europejskie forum badań i innowacji w dziedzinie bezpieczeństwa): ESRIF zostało utworzone we wrześniu 2007 roku i jest europejską grupą strategiczną działającą w obszarze badań nad bezpieczeństwem cywilnym. Jej głównym celem jest opracowanie do 2009 roku średnio-terminowej i długoterminowej strategii badań i innowacji w zakresie bezpieczeństwa cywilnego z wykorzystaniem dialogu publiczno-prywatnego. Inspektor wziął udział w posiedzeniu podgrupy ESRIF poświęconym kwestiom innowacji;
- Inspektor w określonych przypadkach brał także udział w posiedzeniach grup doradczych Komisji Europejskiej zajmujących się wiarygodnymi systemami komputerowymi (ang. *„trusted computing”*), a także przyszłym wszechobecnym społeczeństwem informacyjnym.

3.6.6. Połączenie Google / DoubleClick a kwestie ochrony danych

W marcu 2008 roku Komisja Europejska zatwierdziła na mocy rozporządzenia w sprawie kontroli łączenia przedsiębiorstw nabycie przedsiębiorstwa dostarczającego technologię reklamy w Internecie – *DoubleClick* przez *Google* – właściciela jednej z najważniejszych wyszukiwarek internetowych. Firmy te zarządzają dużymi bazami danych zawierającymi dane osobowe związane z wyszukiwaniami prowadzonymi przez internautów i odwiedzanymi przez nich stronami. Połączone wykorzystanie tych baz wiąże się z delikatnymi i złożonymi kwestiami dotyczącymi prawa do ochrony danych osobowych.

Pod koniec stycznia 2008 roku Inspektor wziął udział w wysłuchaniu na temat ochrony danych w Internecie zorganizowanym przez parlamentarną Komisję LIBE. Ponadto doszło do wymiany listów między Inspektorem, jako doradcą instytucji wspólnotowych we wszystkich kwestiach związanych z ochroną danych, a komisarzem ds. konkurencji, Neelie

⁽⁴⁷⁾ <http://www.turbine-project.eu>

⁽⁴⁸⁾ <http://www.bridge-project.eu/>

Kroes. Przedstawiciele jego personelu spotkali się z odnośnym personelem Komisji i udzielili fachowej porady na temat kwestii ochrony danych, które mogą się pojawić przy okazji spraw dotyczących konkurencji, takich jak wspomniane połączenie przedsiębiorstw.

W tym kontekście Inspektor z pozytywnie ocenia wyjaśnienia Komisji zawarte w jednym z komunikatów prasowych, mówiące o tym, że jej decyzja opiera się wyłącznie na rozporządzeniu UE w sprawie kontroli łączenia przedsiębiorstw i nie narusza obowiązków połączonych podmiotów wynikających z unijnych i krajowych przepisów dotyczących ochrony danych.

Ponadto Inspektor, jako członek grupy roboczej art. 29 (grupy roboczej ds. ochrony danych), aktywnie uczestniczył w przygotowaniu dokumentu na temat ochrony danych i wyszukiwarek przyjętego przez tę grupę roboczą w kwietniu 2008 roku.

3.6.7. Udział w grupach ekspertów

Identyfikacja radiowa (RFID) – zainteresowane strony

Na mocy decyzji Komisji z dnia 28 czerwca 2007 r. utworzono grupę ekspertów do spraw identyfikacji radiowej⁽⁴⁹⁾. Grupa ta znana jest również jako „grupa ds. RFID skupiająca zainteresowane strony” (ang. *RFID-Stakeholders Group*). Zgodnie z art. 4 ust. 4 lit. b) wspomnianej decyzji Inspektor uczestniczy w działaniach tej grupy w charakterze obserwatora. Podczas jej czterech posiedzeń zorganizowanych w 2008 roku Inspektor uczestniczył w dyskusjach służących wypracowaniu zaleceń, które mają zostać wydane w 2009 roku. Działając w ramach tej grupy, Inspektor wniósł także wkład w analizę charakteru i skutków obecnego zwrotu ku „Internetowi przedmiotów”; jej rezultatem było opublikowanie we wrześniu 2008 roku⁽⁵⁰⁾ dokumentu roboczego przygotowanego przez personel Komisji; dokumentowi temu poświęcony będzie komunikat, którego publikacja przewidziana jest na koniec 2009 roku.

Grupa ekspertów ds. zatrzymywania danych

„Platforma ds. zatrzymywania danych elektronicznych w celu dochodzenia, wykrywania i ścigania poważnych przestępstw” jest grupą ekspertów, która powstała w dniu 25 marca 2008 r. na mocy decyzji Komisji⁽⁵¹⁾. W skład tej grupy

wchodzą: przedstawiciele organów ścigania, stowarzyszeń branży łączności elektronicznej, organów ds. ochrony danych, a także posłowie do Parlamentu Europejskiego i Europejski Inspektor Ochrony Danych. Grupa działa w charakterze zespołu konsultacyjnego⁽⁵²⁾. Grupa będzie ułatwiać wymianę wzorcowych rozwiązań i wносить wkład w dokonywaną przez Komisję ocenę kosztów i skuteczności dyrektywy 2006/24/WE (dyrektywa o zatrzymywaniu danych), a także w opracowywanie odpowiednich technologii mających znaczenie dla tej dyrektywy⁽⁵³⁾.

Pierwsze oficjalne posiedzenie wspomnianej grupy odbyło się 28 listopada 2008 r. (od 2007 roku zorganizowano cztery posiedzenia nieformalne). Obecnie toczą się dyskusje na temat kilku dokumentów dotyczących technicznych i prawnych aspektów zatrzymywania danych. Inspektor aktywnie uczestniczy w posiedzeniach wspomnianej grupy i będzie kontynuował swoje wsparcie w 2009 roku.

Historia kredytowa

Inspektor uczestniczy w charakterze obserwatora w utworzonej przez Komisję grupie ekspertów ds. historii kredytowej; pierwsze posiedzenie tej grupy odbyło się we wrześniu 2008 roku. Grupa skupia ekspertów z rejestrów kredytowych, krajowych stowarzyszeń konsumentów, banków i organów ds. ochrony danych (w tym organ ds. ochrony danych Francji i Finlandii). W maju 2009 roku grupa ta zakończy opracowywanie sprawozdania, które dotyczy konieczności ustanowienia w UE transgranicznej wymiany informacji kredytowych o osobach i warunków takiej wymiany. Niektóre aspekty tego projektu budzą zastrzeżenia związane z ochroną danych; chodzi tu na przykład o dokładny cel wymiany informacji oraz jakość danych, które mają być przekazywane. Wspólnie z innymi organami ds. ochrony danych, które są reprezentowane na forum wspomnianej grupy ekspertów, Inspektor zwrócił uwagę na te kwestie, tak by opracowywane przez grupę sprawozdanie było odpowiednio wyważone.

3.6.8. Wypadki morskie

W listopadzie 2008 r. Inspektor przedstawił – w odpowiedzi na uprzednią prośbę – skierowaną do konkretnego odbiorcy poradę w odniesieniu do wniosku dotyczącego dyrektywy ustanawiającej podstawowe zasady regulujące postępowanie dochodzeniowe w sprawie wypadków w sektorze transportu morskiego. Wniosek został już przyjęty

⁽⁴⁹⁾ Decyzja nr 467/2007/WE (Dz.U. L 176 z 6.7.2007, s. 25).

⁽⁵⁰⁾ http://ec.europa.eu/information_society/eeurope/i2010/docs/future_internet/swp_internet_things.pdf

⁽⁵¹⁾ Decyzja Komisji 2008/324/WE (Dz.U. L 111 z 23.4.2008, s. 11).

⁽⁵²⁾ Zob. art. 2 wspomnianej decyzji.

⁽⁵³⁾ Motyw 6 decyzji.

przez Komisję w 2005 roku i dotarł do trzeciego i ostatniego etapu procedury współdecyzji – komitetu pojednawczego. Prośba o poradę wystosowana została przez sprawozdawcę parlamentarnego, który był członkiem tego komitetu. Inspektor otrzymał różne opinie Rady i Parlamentu Europejskiego dotyczące konkretnego artykułu w przedmiotowym wniosku, który dotyczył gromadzenia i możliwego ujawniania danych osobowych. Sporządzona w związku z tym porada Inspektora pomogła komitetowi osiągnąć porozumienie w tej kwestii. Inspektor wyraził zadowolenie w związku z tą konsultacją, ponieważ po raz pierwszy zwrócono się do niego o opinię na tym etapie procesu prawodawczego.

3.6.9. Choroby zakaźne

Choroby zakaźne, takie jak gruźlica, odra i grypa nie uznają granic państwowych i mogą się szybko rozprzestrzeniać. Pojawiają się nowe choroby a inne wykształcają formy odporne na leki. Ponadto badane są nowe osiągnięcia naukowe dotyczące roli czynników chorobotwórczych przy przewlekłych schorzeniach, takich jak rak, choroby serca lub alergię. W odpowiedzi na te różne kwestie w 1999 roku zaczęła działać sieć w dziedzinie chorób zakaźnych⁽⁵⁴⁾. Sieć w dziedzinie chorób zakaźnych opiera się na współdziałaniu państw członkowskich i składa się z dwóch trzonów: nadzoru oraz systemu wczesnego ostrzegania i reagowania (EWRS). Inspektor zgłosił nieformalne uwagi do decyzji Komisji zmieniającej decyzję nr 2000/57/WE w sprawie systemu wczesnego ostrzegania i reagowania w celu zapobiegania chorobom zakaźnym i kontroli tych chorób.

3.6.10. Wspólnotowy kodeks celny oraz numer w systemie rejestracji i identyfikacji podmiotów gospodarczych (numer EORI)

Komisja Europejska zwróciła się do Inspektora o nieformalne konsultacje w związku z projektem zmiany rozporządzenia Komisji (EWG) nr 2454/93 z dnia 2 lipca 1993 r. ustanawiającego przepisy w celu wykonania rozporządzenia Rady (EWG) nr 2913/92 ustanawiającego Wspólnotowy kodeks celny (zwanym dalej „projektem”). Był to pierwszy przypadek konsultowania się z Inspektorem w ramach przyjmowania rozporządzenia Komisji, gdy Komisja jest wspomagana przez komitet (tym wypadku Komitet ds. Kodeksu Celnego). Inspektor

nie wydał opinii, ale wystosował do Komisji trzy pisma zawierające porady.

W nowym akcie prawnym zaproponowano podstawę prawną systemu rejestracji i identyfikacji podmiotów gospodarczych i innych osób, który umożliwi im jednokrotną rejestrację do celów wszystkich kontaktów z organami celnymi w całej Wspólnocie. Aby przechowywać i wymieniać dane rejestracyjne i identyfikacyjne podmiotów gospodarczych, a także innych osób, między organami celnymi oraz między Komisją a organami celnymi, zostanie stworzony elektroniczny system rejestracji i identyfikacji (EORI). Dane z systemów krajowych będą ponadto konsolidowane na szczeblu centralnym i przesyłane w regularnych odstępach czasu do państw członkowskich.

Inspektor udzielił Komisji porad w wielu kwestiach, dotyczących w szczególności:

- współnadzorczej roli Inspektora i krajowych organów ochrony danych osobowych;
- różnicy między „podmiotami gospodarczymi” a „innymi osobami” (osobami, których dane dotyczą), jeżeli chodzi o niezbędność i proporcjonalność działań związanych z przetwarzaniem. Ma to wpływ na podstawę legalności przetwarzania, okres przechowywania itd.;
- praw osoby, której dane dotyczą, zgody jako podstawy prawnej publikowania danych osobowych w Internecie oraz przyjmowania środków bezpieczeństwa.

3.7. Nowe zjawiska

3.7.1. Interakcje z technologią

Oczekuje się, że rozwój i wykorzystanie z nowych technologii przyczyni się do jakościowej zmiany społeczeństwa jako całości. Te nowe perspektywy określa się jako „wszechobecne społeczeństwo informacyjne”, „otoczenie inteligentne” lub „Internet przedmiotów”. Staną się one trwałe, tylko jeśli na najwcześniejszym etapie ich tworzenia odpowiednią uwagę poświęci się wyzwaniom, w szczególności kwestiom ochrony danych osobowych i prywatności. Gruntowna analiza trendów technologicznych, które stymulują przemianę społeczeństwa europejskiego w europejskie społeczeństwo informatyczne, jest jednym z kluczowych czynników powodzenia promowania zaufania do tego tworzącego się środowiska, co będzie miało decydujące znaczenie.

⁽⁵⁴⁾ Decyzja 2119/98/WE Parlamentu Europejskiego i Rady.



Technologia „cloud computing” integrująca silosy danych stanowi wyzwanie dla stosowania ram regulacyjnych UE dotyczących ochrony danych

„Cloud computing”

Już w sprawozdaniu rocznym za rok 2007 Inspektor wyraził poważne obawy dotyczące dotychczas nierozważanych kwestii prywatności i bezpieczeństwa w związku z rozwojem tzw. „cloud computing”⁽⁵⁵⁾. Nie odpowiedziano wciąż na potrzebę wdrożenia odpowiednich zabezpieczeń, aby zapewnić trwały rozwój tej powstającej technologii. Jednocześnie proponuje się coraz więcej usług wspieranych przez urządzenia systemu „cloud computing”, nie tylko użytkownikom biznesowym lub rządowym, lecz osobom prywatnym.

Zasada „cloud computing” stanowi prawdziwe wyzwanie dla odpowiedniego określenia prawa właściwego odnoszącego się do przetwarzania danych osobowych, odpowiedzialnych podmiotów i innych powiązanych skutków prawnych. Podany dalej

⁽⁵⁵⁾ Termin „cloud computing” („przetwarzanie w chmurze”) odnosi się do korzystania z opartej na Internecie technologii komputerowej, która umożliwia oferowanie różnorodnych usług. Jest to model informatyczny, dzięki któremu jako usługę w Internecie oferuje się dostęp do dynamicznie skalowalnych i często zwirtualizowanych zasobów. Użytkownicy nie muszą mieć wiedzy ogólnej, wiedzy fachowej ani kontroli nad infrastrukturą techniczną „w chmurze”, która ich wspiera.

przykład ilustruje elastyczność, którą może zaferować „cloud computing”, lecz również kwestie, które wywołuje w kontekście egzekwowania ram prawnych UE. Aby obniżyć koszt energii, działania „przetwarzania w chmurze” mogłyby być kierowane głównie do centrów danych, które są zasilane energią słoneczną i wystawione na promienie słoneczne w czasie, gdy otrzymano zlecenie przetwarzania; a te centra, które w danym momencie znajdują się będą po nieoświetlonej stronie Ziemi i będą zasilane innym rodzajem energii, mogłyby być mniej wykorzystywane. Chociaż jest to rozwiązanie atrakcyjne z punktu widzenia ekologii, przykład ten pokazuje również, że byłoby prawie niemożliwe określenie, gdzie nastąpi przetwarzanie danych i które elementy „chmury” będą w nim uczestniczyć. Można też sobie wyobrazić, że dane osobowe przechowywane w centrach danych trzeciego państwa mogłyby podlegać wymogowi okazania do celów sądowych i zostałyby ujawnione rządowi w jurysdykcji, w której umieszczone są serwery obsługujące technologię „cloud computing”.

Jednym z możliwych, już sugerowanych rozwiązań byłoby wprowadzenie obowiązku przetwarzania i

przechowywania danych osobowych jedynie na serwerach „chmury unijnej”, które byłyby fizycznie umieszczone na terytorium UE i działałyby w unijnych ramach regulacyjnych ochrony danych. Jednakże ten wymóg byłby niezgodny z podstawami tej obiecującej technologii oraz perspektywami wielkiej elastyczności i zdolności przystosowania się, które miałyby zapewniać „cloud computing”. Wydaje się on również nie brać pod uwagę tego, że ramy UE w zakresie ochrony danych *obowiązują* obecnie bez względu na miejsce przetwarzania tych danych, o ile przetwarzanie danych odbywa się w kontekście prowadzenia przez zakład administratora danych działalności w UE lub gdy są tam umieszczone wykorzystywane środki (zob. art. 4 dyrektywy 95/46/WE). Prawdą jest jednak, że obecna niejasna sytuacja w odniesieniu do „cloud computing” stwarza nowe wyzwania dla skutecznej realizacji i egzekwowania standardów ochrony danych.

Przed wysłaniem do „chmury” dane mogłyby oczywiście być szyfrowane, lecz mogłyby to stanowić zagrożenie dla wielkich możliwości przetwarzania oferowanych przez „cloud computing”, ponieważ po zaszyfrowaniu dane te nie mogą być przetwarzane⁽⁵⁶⁾. Istotnym warunkiem tworzenia zaufania do tych nowych środowisk będzie jednak większa świadomość wśród kluczowych podmiotów dotycząca istniejących zagrożeń oraz odpowiedzialności związanej z właściwym, a także skutecznym reagowaniem na nie.

Sekwencjonowanie DNA

W wyniku ogromnego wysiłku w zakresie badań i rozwoju, którego dokonano w ramach projektu poznania ludzkiego genomu.⁽⁵⁷⁾ geny ludzkie zostały w 2001 roku pomyślnie i prawie całkowicie zsekwencjonowane. Zlokalizowano i zidentyfikowano około 3 miliardów par komplementarnych i pomiędzy 20 000 a 25 000 genów

Osiągnięcie celu Archon X Prize for Genomics⁽⁵⁸⁾ będzie jeszcze wymagało kilkuletnich wysiłków. W dziedzinie badań genetycznych pojawiło się jednak mnóstwo prywatnych podmiotów; proponują już one analizę genetyczną nakierowaną na zidentyfikowanie specyficznych cech i możliwych chorób za mniej niż 400 EUR.

⁽⁵⁶⁾ Zob. prace Carla Hewittsa, emerytowanego profesora w Massachusetts Institute of Technology (<http://carlhewitt.info/>).

⁽⁵⁷⁾ http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml

⁽⁵⁸⁾ Nagroda ta zostanie przyznana pierwszemu zespołowi, który potrafi zbudować i zastosować urządzenie umożliwiające zsekwencjonowanie 100 ludzkich genomów w ciągu nie więcej niż 10 dni przy kosztach nieprzekraczających 10 000 USD za genom (<http://genomics.xprize.org/>).

Ten niezwykle szybko rosnący przemysł jest głównie wspierany przez następujące tendencje technologiczne:

- rosnąca dostępność wielkiej zdolności przetwarzania potrzebnej dla analizy olbrzymiej ilości danych, którą stymuluje rozwój wzajemnie powiązanych centrów danych;
- efekty dodatkowe i punkty zwrotne w dziedzinie analizy DNA na skutek projektu poznania genomu ludzkiego;
- inne tendencje technologiczne już opisane w poprzednich sprawozdaniach rocznych Inspektora, takie jak nieograniczona szerokość pasma oraz nieograniczone zasoby pamięci masowej.

Usługi w zakresie analizy genetycznej oferowane przez wspomniane firmy opierają się na ustalaniu z naukową ścisłością związków pomiędzy informacją genetyczną osoby, której dane dotyczą, a możliwymi powiązanymi cechami lub chorobami. Te związki przyczynowe opierają się na licznych elementach, takich jak analiza statystyczna i dostępność sprawozdań w zakresie badań i rozwoju, co można streścić jako zdolność tych firm do dostępu do wiarygodnych obszernych baz danych zawierających informacje naukowe.

Jak ostatnio podkreślono w decyzji Europejskiego Trybunału Praw Człowieka w sprawie dotyczącej wykorzystania DNA do celów egzekwowania prawa⁽⁵⁹⁾, próbki genetyczne mogą ujawnić „bardzo wrażliwe informacje o danej osobie, w tym informacje o jej zdrowiu”; dlatego należy je przetwarzać przy zachowaniu największych zabezpieczeń w zakresie prywatności i ochrony danych.

Coraz częściej analizy genetyczne oferuje się przez Internet, a zatem są one powszechnie dostępne w państwie i poza państwem, w którym umiejscowiona jest dana firma. Testy te, których dostępność była uprzednio głównie ograniczona do mocno uregulowanych dziedzin medycyny i sądownictwa, są obecnie oferowane na skalę gospodarczą. Analizowana próbka DNA niekoniecznie należy do osoby, która ją wysyła, lecz mogła zostać przedstawiona przez kogokolwiek, komu udało się tę próbkę pobrać.

Obiecująca technologia błyskawicznego sekwencjonowania DNA i jej dostępność ponad granicami stanie się – jeżeli nie będziemy potrafili się z nią odpowiednio obchodzić – wyzwaniem dla tradycyjnie stosowanych zabezpieczeń ograniczających

⁽⁵⁹⁾ Sprawa S. i Marper przeciwko Zjednoczonemu Królestwu, 5 grudnia 2008 r.

dostęp do najbardziej wrażliwych danych osobowych i zrodzi istotne problemy dotyczące prywatności.

3.7.2. Nowe wydarzenia w polityce i prawodawstwie

Traktat z Lizbony

W roku 2008 rozpoczęto przemyślenia nad konsekwencjami wejścia w życie Traktatu z Lizbony. W tym kontekście Inspektor podsumował konsekwencje nowego traktatu dla ochrony danych, takie jak nowa podstawa prawna ochrony danych (art. 16 Traktatu o funkcjonowaniu Unii Europejskiej), jak również zniesienie struktury filarów. W wyniku odrzucenia Traktatu przez Irlandię w dniu 12 czerwca 2008 r. te działania nie były kontynuowane. Obecnie rysują się nowe perspektywy możliwego wejścia w życie Traktatu z Lizbony w końcu 2009 roku lub na początku 2010 roku.

Program działalności legislacyjnej i prac Komisji na rok 2009 i program sztokholmski

Program działalności legislacyjnej i prac Komisji na rok 2009 przyjął zogniskowane podejście i skoncentrował się na ograniczonej liczbie nowych inicjatyw dotyczących kierunków polityki. W ramach tego podejścia duży nacisk położono na oceny skutków przed przedstawieniem danego wniosku przez Komisję, jak również na przegląd istniejącego prawodawstwa UE i wniosków, które oczekują na rozpatrzenie.

Podejście to przejawia się również w stanowisku, jakie Komisja planuje zastosować w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W programie działalności legislacyjnej i prac Komisji na rok 2009 wymieniono zakończenie programu haskiego na rzecz wolności, bezpieczeństwa i sprawiedliwości (z listopada 2004 roku), jak też dalsze kroki w kierunku wspólnej polityki w sprawie migracji. Jednym z głównych elementów programu Komisji jest planowany nowy wieloletni program dotyczący przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który ma zostać przyjęty w ramach szwedzkiego przewodnictwa w Radzie (często nazywany programem sztokholmskim). W sprawozdaniu tzw. grupy doradczej ds. przyszłości na centralnym miejscu znalazła się równowaga między mobilnością, bezpieczeństwem a prywatnością. Sprawozdanie to, wraz z wprowadzoną w nim zasadą konwergencji, będzie jednym z podstawowych elementów programu sztokholmskiego.

Główne tendencje dotyczące egzekwowania prawa

W sprawozdaniu za rok 2007 odnotowano jako jedną z głównych tendencji działania prawodawcy dotyczące zwalczania przestępczości, a w szczególności walkę z terroryzmem i przestępczością zorganizowaną. Ta tendencja utrzymywała się w roku 2008.

Zaproponowano ponadto nowe instrumenty prawne jako uzupełnienie istniejących instrumentów prawnych, które nie zostały jeszcze w pełni wdrożone. Wywołało to pytania dotyczące konieczności takich nowych instrumentów i tego, czy nie trzeba się zamiast tego skupić na praktycznej realizacji już istniejących instrumentów. Zagadnienie te zostanie omówione przez Inspektora podczas dalszych dyskusji na temat propozycji UE w sprawie PNR.

W roku 2009 nadal będzie widoczna tendencja otwierania istniejących baz danych (europejskich baz danych, jak również baz krajowych) do celów egzekwowania prawa, mimo że pierwotne cele tych baz danych były inne. Kwestie pokrewne to interoperacyjność i wzajemne połączenie baz danych, jak też działania dotyczące tworzenia profili osób.

Decyzja ramowa w sprawie ochrony danych

Przyjęcie decyzji ramowej Rady 2008/977 w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych oznaczało w dziedzinie legislacji, że po raz pierwszy stworzono na szczeblu UE ogólne ramy prawne dla ochrony danych w tym obszarze. Decyzja ramowa nie ma jednak zastosowania do wszystkich właściwych sytuacji i nadal obowiązują inne instrumenty dotyczące ochrony danych w tej dziedzinie.

Przez cały czas trwania negocjacji dotyczących tego aktu prawnego był on jednym z głównych przedmiotów zainteresowania Inspektora, który poświęcił mu trzy opinie i sformułował uwagi na jego temat. W opiniach Inspektora uznano tę inicjatywę za znaczący krok naprzód w zakresie ochrony danych we współpracy policyjnej i sądowej oraz niezbędne uzupełnienie innych środków, które wprowadzono, by ułatwić transgraniczną wymianę danych osobowych dla potrzeb egzekwowania prawa. Jednocześnie Inspektor wielokrotnie wzywał do istotnego polepszenia tego wniosku, aby zapewnić wysokie standardy, jeżeli chodzi o oferowany poziom ochrony; ostrzegał również przed obniżeniem standardów ochrony danych. Ubolewał

w szczególności, że decyzja ramowa obejmuje jedynie dane policyjne i sądowe wymieniane między państwami członkowskimi, organami i systemami UE, a nie obejmuje danych krajowych.

Potrzebne są zatem dalsze kroki – na mocy Traktatu z Lizbony lub poza jego ramami – by zwiększyć poziom ochrony zapewniany przez nowy instrument. Inspektor zachęca zatem instytucje wspólnotowe, by jak najszybciej rozpoczęły rozważania nad dalszymi usprawnieniami w zakresie ochrony danych w kontekście egzekwowania prawa.

Przyszłość dyrektywy w sprawie ochrony danych

Dyskusje w sprawie przyszłości dyrektywy 95/46/WE odbywają się na różnych szczeblach. Dyskusje te skupiają się na wdrażaniu tej dyrektywy, nie wykluczając możliwości jej przyszłej zmiany. Prowadzony przegląd dyrektywy może stworzyć okazję do przemyśleń na temat potrzeby jej zmiany, aby zapewnić jej dalszą skuteczność, lub przyjęcie konkretnych przepisów, by zaradzić problemom związanym z ochroną danych, które powstały wskutek pojawienia się nowych technologii informacyjno-komunikacyjnych.

Rozpoczęto już wiele działań i zostaną one zakończone w roku 2009. Oprócz działań grupy roboczej art. 29 można wymienić następujące działania:

- Komisja ogłosiła, że zostaną przeprowadzone publiczne konsultacje w sprawie dyrektywy, w tym zostanie zorganizowana konferencja wszystkich zainteresowanych stron w maju 2009 roku.
- W roku ubiegłym działające w Zjednoczonym Królestwie Biuro Komisarza ds. Informacji (ICO) ogłosiło przetarg, aby ocenić mocne i słabe strony unijnego prawodawstwa dotyczącego ochrony danych i zalecić uaktualnienia, które zmniejszą związane z nim obciążenie administracyjne. Opracowanie to przeanalizuje unijną dyrektywę o ochronie danych i jej stosowanie w celu określenia lepszych sposobów zapewnienia skutecznej ochrony poszczególnych osób i społeczeństwa oraz zmniejszenia obciążeń organizacji. Opracowanie to ma zostać omówione podczas corocznej wiosennej konferencji europejskich komisarzy ds. ochrony danych w kwietniu 2009 roku i opublikowane w maju 2009 roku. Chociaż jedynie Komisja Europejska może zainicjować proces zmiany dyrektywy, ICO chce rozpocząć debatę

na temat mocnych i słabych stron, by zadbać o to, aby unijne prawodawstwo dotyczące ochrony danych skutecznie zaspokajało potrzeby organizacji i poszczególnych osób.

Zdrowie publiczne

UE ma ambitny program mający na celu polepszenie zdrowia obywateli w społeczeństwie informacyjnym; UE widzi w tym kontekście wielkie możliwości usprawnienia transgranicznej opieki zdrowotnej przez wykorzystanie technologii informatycznych. Zdrowie publiczne to nowy obszar zainteresowania Inspektora. Nacisk zostanie położony na systemy informacji zdrowotnej, opracowywanie systemów e-zdrowia, wtórne wykorzystywanie danych medycznych, sposób prowadzenia działalności legislacyjnej dotyczącej informacji szczególnie chronionych oraz pewne inne kwestie zasadnicze, także związane z krytyką w sektorze medycznym wobec przepisów prawa o ochronie danych.

Rozumie się samo przez się, że usprawnienie transgranicznej opieki zdrowotnej w połączeniu z wykorzystaniem osiągnięć technologii informacyjnej ma ogromny wpływ na ochronę danych osobowych. Skuteczniejsza, a więc coraz szersza wymiana danych medycznych, rosnące odległości między osobami i konkretnymi instytucjami, różnice w krajowych przepisach wykonawczych dotyczących zasad ochrony danych rodzą problemy związane z bezpieczeństwem danych i pewnością prawną. Ważną rolę będzie odgrywać zasada identyfikowalności.

Inne kwestie

W roku 2009 Inspektor skupi się na kilku konkretnych obszarach działania UE:

- związku między ochroną danych a gromadzeniem i wykorzystywaniem statystyk;
- działaniach odnoszących się do publicznego dostępu do dokumentów, takich jak zmiana rozporządzenia (WE) nr 1049/2001 w sprawie publicznego dostępu do dokumentów.

Szczególną uwagę poświęci się w 2009 roku sposobowi doradzania Komisji w przypadkach gdy nie przyjmuje ona wniosku (skierowanego do Rady lub Parlamentu Europejskiego), tylko podejmuje samodzielnie decyzję.

4. Współpraca

4.1. Grupa robocza art. 29

Grupę roboczą art. 29 utworzono na mocy art. 29 dyrektywy 95/46/WE. Jest to niezależny organ doradczy ds. ochrony danych osobowych w zakresie wspomnianej dyrektywy⁽⁶⁰⁾. Zadania grupy zostały określone w art. 30 dyrektywy i w skrócie można je przedstawić następująco:

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

Inspektor jest członkiem grupy roboczej art. 29 od początku 2004 roku. Art. 46 lit. g) rozporządzenia (WE) 45/2001 przewiduje, że Inspektor bierze

udział w działalności wspomnianej grupy roboczej. Zdaniem Inspektora jest to bardzo ważna platforma współpracy z krajowymi organami nadzoru. Jest również oczywiste, że ta grupa robocza powinna odgrywać jedną z głównych ról, jeśli chodzi o jednolite stosowanie dyrektywy oraz interpretowanie jej ogólnych zasad.

W lutym 2008 roku grupa robocza przyjęła nowy dwuletni program prac⁽⁶¹⁾. Postanowiła skupić się na czterech głównych tematach strategicznych i na kilku kwestiach tematycznych, które według niej są najbardziej istotne i najpilniejsze dla rozwoju ochrony danych.

Grupa robocza określiła trzy główne wyzwania:

- w jaki sposób zwiększyć wpływ dyrektywy 95/46/WE i rolę grupy roboczej;
- wpływ nowych technologii;
- zglobalizowane środowisko (międzynarodowy transfer danych, globalne zagadnienia dotyczące prywatności i jurysdykcji).

Istnieją zatem następujące główne tematy strategiczne bardziej szczegółowo opracowane w programie prac:

- lepsza realizacja dyrektywy 95/46/WE;
- zapewnienie ochrony danych podczas międzynarodowych transferów;
- zapewnienie ochrony danych w odniesieniu do nowych technologii;
- sprawienie, by grupa robocza art. 29 była skuteczniejsza.

⁽⁶⁰⁾ W skład grupy roboczej wchodzi przedstawiciele krajowych organów nadzoru z każdego państwa członkowskiego, przedstawiciel organu ustanowionego dla instytucji i organów wspólnotowych (tj. Inspektora) oraz przedstawiciel Komisji. Komisja zapewnia również sekretariat na potrzeby grupy roboczej. Krajowe organy nadzoru z Islandii, Norwegii i Liechtensteinu (jako partnerzy w ramach EOG) uczestniczą w obradach w charakterze obserwatorów.

⁽⁶¹⁾ Program prac na lata 2008–2009 przyjęty w dniu 18 lutego 2008 r. (WP 146).

W związku z tym programem prac grupa robocza poczyniła już w kilku dziedzinach istotne postępy, które zostały opisane poniżej:

- międzynarodowe transfery: pakiet dokumentów roboczych, aby ułatwić korzystanie z wiążących zasad dla przedsiębiorstw (WP 153-155) i bieżący monitoring kwestii związanych z danymi dotyczącymi przelotu pasażera (WP 151);
- nowe technologie: opinia 1/2008 w sprawie zagadnień ochrony danych odnoszących się do wyszukiwarek (WP 148) oraz opinia 2/2008 w sprawie przeglądu dyrektywy 2002/58/WE o prywatności i łączności elektronicznej (dyrektywy o e-prywatności) (WP 150);
- większa skuteczność grupy roboczej: mandat dla drugiego wspólnego zespołu dochodzeniowego dotyczący przestrzegania na szczeblu krajowym wymagań w zakresie ochrony danych w kontekście zatrzymywania danych o ruchu (WP 152);
- lepsza realizacja dyrektywy 95/46/WE: trwają prace dotyczące pojęć „administrator danych” i „podmiot przetwarzający dane” oraz kwestii „prawa właściwego”.

Grupa robocza zapewniła również, że z uwagą śledzono nowe wydarzenia w odniesieniu do zarządzania granicami UE, bezpieczeństwa i kontroli granicznej (US ESTA) oraz danych biometrycznych i wniosków wizowych.

W tym kontekście grupa robocza zajmowała również stanowisko w sprawie wniosków prawodawczych lub podobnych dokumentów. W niektórych przypadkach wnioski te były przedmiotem opinii Inspektora na podstawie art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 (zob. rozdział 3). Opinia Inspektora jest obowiązkowym elementem procesu prawodawczego UE, ale wkład grupy roboczej jest również niezwykle przydatny, zwłaszcza ze względu na fakt, że może dotyczyć kwestii szczególnie istotnych z perspektywy krajowej. Inspektor z zadowoleniem przyjmuje zatem te wkład, który jest zbieżny z jego własnymi opiniami.

W bardziej ogólnym ujęciu ścisła współpraca Inspektora z grupą roboczą zaowocowała dobrą synergią w wielu kwestiach, ale główny nacisk położono na wykonanie dyrektywy 95/46/WE i na wyzwania, które wiążą się z nowymi technologiami. Inspektor udzielił również silnego poparcia inicjatywom służącym ułatwieniu międzynarodowych przepływów danych (takim jak wiążące zasady dla przedsiębiorstw).

Zgodnie z art. 46 lit. f) ppkt (i) rozporządzenia (WE) nr 45/2001 Inspektor musi również współpracować z krajowymi organami nadzoru w stopniu umożliwiającym im wykonanie własnych obowiązków; polega to w szczególności na wymianie wszystkich użytecznych informacji i na zwracaniu się o pomoc lub na świadczeniu pomocy przy wykonywaniu powierzonych tym organom zadań. Współpraca taka dostosowywana jest do poszczególnych przypadków.

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

4.2. Grupa Robocza Rady ds. Ochrony Danych

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

Prezydencja niemiecka postanowiła na tej samej zasadzie kontynuować dyskusje dotyczące ewentualnych inicjatyw Komisji i innych stosownych tematów związanych z pierwszym filarem. W związku z tym w pierwszej połowie 2007 roku odbyły się dwa posiedzenia. Prezydencja portugalska przewidziała jedno dodatkowe posiedzenie, lecz zostało ono odwołane.

Prezydencja słoweńska zwołała jedno posiedzenie grupy roboczej w maju 2008 roku. Podczas tego posiedzenia zastępca Inspektora przedstawił jego opinię na temat przeglądu dyrektywy o e-prywatności, sprawozdanie roczne za rok 2007 oraz priorytety Inspektora w odniesieniu do konsultacji co do wniosków dotyczących nowych aktów prawodawczych w roku 2008.

Wymieniono również poglądy w sprawie dyrektywy 95/46/WE, głównie w odniesieniu do szeregu tematów, takich jak związek między ochroną danych na mocy tej dyrektywy a wolnością informacji i wolnością wyrażania opinii; potrzeba konkretnych przepisów dotyczących rozwoju technologicznego (nowe technologie stwarzające zagrożenie) oraz uproszczenie wymogów dotyczących zgłoszeń

i informacji (szczególnie w odniesieniu do małych i średnich przedsiębiorstw).

W wyniku tej wymiany poglądów stwierdzono, iż wydaje się, że wszyscy są ogólnie zadowoleni z dyrektywy 95/46/WE. Istnieje jednak ogólna potrzeba dalszej dyskusji po ewentualnej ratyfikacji Traktatu z Lizbony.

Grupa robocza nie spotykała się podczas prezydencji francuskiej, jednak prezydencja czeska zorganizowała ponownie jedno posiedzenie w marcu 2009 roku.

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

4.3. Skoordynowany nadzór nad systemem Eurodac

Współpraca z krajowymi organami ds. ochrony danych, mająca na celu wypracowanie skoordynowanego podejścia do nadzoru nad systemem Eurodac (zob. sekcja 2.8), choć zainicjowana została dopiero kilka lat temu, szybko się rozwija.

W skład grupy ds. koordynowania nadzoru nad systemem Eurodac (zwanej dalej „grupą”) wchodzi przedstawiciele krajowych organów ds. ochrony danych oraz Inspektora; odbyły się dwa posiedzenia tej grupy: w czerwcu i grudniu 2008 roku. W tym roku nacisk położono na realizację programu prac przyjętego przez grupę w grudniu 2007 roku.

Równocześnie obiektem zainteresowania stały się również ramy prawne będące podstawą działania tej grupy; Komisja Europejska podjęła się przeglądu rozporządzenia dublińskiego i rozporządzenia Eurodac w ogólnym kontekście środków azylowych⁽⁶²⁾.

Aby otrzymać informacje od różnych zainteresowanych stron, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego zorganizowała w dniu 29 maja 2008 r. spotkanie okrągłego stołu zatytułowane „System dubliński – luki i alternatywy”. Inspektor miał możliwość przedstawienia poglądów dotyczących

tej kwestii i określił m.in. w jaki sposób skoordynowane nadzorowanie Eurodac mogłoby przyczynić się do usprawnienia tego systemu.

Grupa jest świadoma tych zmian i chętna, by przyczynić się do rozwoju nowych instrumentów przez dzielenie się doświadczeniami na szczeblu krajowym i ocenianie tych doświadczeń.

Działania grupy w roku 2008

Podczas posiedzenia w czerwcu 2008 roku, zgodnie z art. 3 regulaminu wewnętrznego, grupa wybrała przewodniczącego i wiceprzewodniczącego. Było dwoje kandydatów: Peter Hustinx (Inspektor) na stanowisko przewodniczącego oraz Guro Slettemark (Inspektor Ochrony Danych z Norwegii) na stanowisko wiceprzewodniczącego. Kandydaci ci zostali wybrani jednogłosem większością ważnie oddanych głosów.

Podczas posiedzenia w grudniu 2007 roku grupa wybrała w ramach programu prac trzy tematy w celu głębszego przeanalizowania i sporządzenia sprawozdania. W 2008 roku grupa skupiła się na tych trzech tematach, pracując najpierw na szczeblu krajowym na podstawie standardowych kwestionariuszy. Celem jest następnie zgromadzenie i przeanalizowanie odpowiedzi, aby zapewnić wskazówki, gdy jest to celowe i pożyteczne.

• Informowanie osób, których dane dotyczą

W sprawozdaniu ze skoordynowanej kontroli wydanym w 2007 roku zasugerowano, że jedną z możliwych przyczyn niewielkiego korzystania z prawa do dostępu jest to, że osoby, których dane dotyczą, nie są świadome swoich praw. Grupa postanowiła przeanalizować, w jaki sposób informowane są osoby ubiegające się o azyl lub osoby, których dane umieszczono w systemie Eurodac z innego powodu. Celem tego przedsięwzięcia jest określenie i wymiana najlepszych praktyk w tej dziedzinie (używane języki, kwestia tego, czy wpływ informacji jest w jakiś sposób mierzony, itp.).

• Dzieci a Eurodac

Zgodnie z art. 4 rozporządzenia Eurodac dzieciom, które ukończyły 14 lat, należy pobierać odciski palców. Często powstaje problem określenia wieku dziecka, które nie posiada wiarygodnego dowodu tożsamości. Grupa zajmie się kwestią przepisów i metod ustanowionych przez krajowy organ Eurodac w celu określenia, czy osoba ubiegająca się o azyl jest niepełnoletnia i przeanalizuje, czy te przepisy

⁽⁶²⁾ W dniu 3 grudnia 2008 r. Komisja Europejska przedstawiła kilka wniosków „w celu zwiększenia w Unii praw osób, które ubiegają się o azyl”. Ten pakiet środków zawiera trzy wnioski, których celem jest dokonanie przeglądu warunków przyjmowania uchodźców w UE, rozporządzenia Dublin II i rozporządzenia Eurodac, które stanowią podstawę bazy danych Eurodac.

są zgodne z Konwencją Narodów Zjednoczonych o prawach dziecka.

W sierpniu 2008 roku rozpoczęto krajowe kontrole dotyczące tych dwóch tematów. W połowie 2009 roku oczekuje się sprawozdań odnoszących się do obu tematów.

• **DubliNet** ⁽⁶³⁾

Grupa opowiedziała się za tym, by trzecim tematem, który należałoby podjąć podczas skoordynowanej kontroli, było wykorzystanie DubliNetu, a w szczególności kwestie związane z bezpieczeństwem danych w tym kontekście. Grupa przeanalizuje następujące zagadnienia: jakie przepisy regulują wymianę danych za pośrednictwem DubliNetu na szczeblu krajowym? Jakie środki podejmuje się w celu zapewnienia ochrony danych osobistych podczas tej wymiany informacji? W jaki sposób uregulowane jest dalsze wykorzystywanie danych?

Wydaje się, że prace tej grupy w odniesieniu do tych wszystkich tematów prowadzone są w bardzo odpowiednim czasie z uwagi na zmianę rozporządzeń Eurodac i Dublin. Sprawozdania grupy powinny stanowić pożyteczny wkład w przegląd tych tekstów.

W grudniu 2008 roku zmieniono regulamin wewnętrzny grupy z powodu przyjęcia przez Inspektora nowych przepisów dotyczących zwrotu kosztów podróży, które mogą również obejmować dietyienne. Wymagało to zmiany przepisów wewnętrznych dotyczących tej grupy.

4.4. Trzeci filar

W ostatnich latach znacznie wzrosła potrzeba ścisłej współpracy między Inspektorem a innymi organami ds. ochrony danych w obszarze współpracy policyjnej i sądowej na skutek wielu inicjatyw unijnych i międzynarodowych, których celem jest gromadzenie danych osobowych i wspólne z nich korzystanie, czasami poprzez tworzenie i wzajemne łączenie baz danych.

Artykuł 46 lit. f) ppkt (ii) rozporządzenia (WE) 45/2001 przewiduje, że Inspektor współpracuje przede wszystkim z organami nadzoru w dziedzinie ochrony danych ustanowionymi na mocy tytułu VI Traktatu UE („trzeci filar”), mając na względzie

„poprawę spójności i zastosowania reguł i procedur, za zapewnienie zgodności z którymi są odpowiednio odpowiedzialne”. Te organy nadzoru to wspólne organy nadzoru (JSB) dla Schengen, Europolu, Eurojustu i Systemu Informacji Celnej (CIS). W skład większości tych organów wchodzi – częściowo ci sami – przedstawiciele krajowych organów nadzoru i są one wspierane przez wspólny sekretariat ds. ochrony danych przy Radzie Unii Europejskiej.

Inspektor współpracuje ponadto z krajowymi organami ds. ochrony danych, w szczególności przez udział w pracach Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości, której konferencja europejska powierzyła zadanie monitorowania rozwoju wydarzeń w zakresie egzekwowania prawa w odniesieniu do przetwarzania danych osobowych, przygotowywania wszelkich niezbędnych działań, które w tej dziedzinie powinna podjąć konferencja, a także działania w imieniu konferencji w sytuacji, gdy pilnie potrzebna jest szybka reakcja.

Inspektor aktywnie uczestniczył w posiedzeniach Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości w 2008 roku. Inspektor wiele razy wniósł wkład w debatę przez przedstawienie swoich opinii lub przez udział w pracy poszczególnych podgrup. Inspektora poproszono również o przedstawienie prezentacji na temat zmian, które spowoduje Traktat z Lizbony, w szczególności w odniesieniu do obszaru współpracy policyjnej i wymiaru sprawiedliwości. Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości rozpatrywała rozmaite delikatne kwestie, między innymi:

— w związku z wdrożeniem postanowień konwencji z Prüm do systemu prawnego UE Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości wystosowała pismo do przewodniczącego Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (LIBE) i przyjęła dokument przedstawiający stanowisko w sprawie szczegółowych przepisów i standardów zawartych w załączniku do głównego wniosku. W dokumentach tych grupa robocza podkreśliła, zgodnie z uwagami przedstawionymi przez Inspektora w jego opiniach, że brak jest solidnych ram ogólnych dla ochrony danych w trzecim filarze i wezwała do określenia jasnych zasad dotyczących niezależnego nadzoru, ograniczenia celu i przekazywania danych do państw trzecich;

— w związku z negocjacjami dotyczącymi decyzji ramowej w sprawie ochrony danych w trzecim filarze Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości przedstawiła obawy odnoszące się do jej ograniczonego zakresu zastosowania, a

⁽⁶³⁾ DubliNet jest bezpieczną elektroniczną siecią kanałów umożliwiających przesyłanie informacji między organami krajowymi zajmującymi się wnioskami o azyl. Zazwyczaj trafienie w systemie Eurodac powoduje wymianę danych dotyczących osoby ubiegającej się o azyl. Wymiana ta dokona się w ramach DubliNet.

także do braku forum doradczego krajowych i europejskich organów nadzoru w celu zapewnienia zharmonizowanego stosowania jej przepisów;

- Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości zajmowała się – wspólnie z grupą roboczą art. 29 – również kwestią danych dotyczących przelotu pasażera (PNR) i uczestniczyła w zainicjowanej przez Komisję Europejską dyskusji dotyczącej nowego wieloletniego programu w dziedzinie wolności, bezpieczeństwa i sprawiedliwości.

4.5. Konferencja europejska

Organy ds. ochrony danych z państw członkowskich UE oraz Rada Europy co roku spotykają się na wiosennej konferencji w celu omówienia spraw będących przedmiotem wspólnego zainteresowania oraz w celu wymiany informacji i doświadczeń dotyczących różnych tematów. Inspektor i jego zastępca uczestniczyli w konferencji w Rzymie w dniach 17 i 18 kwietnia 2008 r., której gospodarzem był włoski organ ds. ochrony danych (*Garante per la protezione dei dati personali*); ogólny temat konferencji brzmiał: „Perspektywy prywatności w Europie i poza Europą”.

Konferencja zajmowała się różnymi zjawiskami odnoszącymi się do bezpieczeństwa i nowych technologii. W przyjętym przez konferencję oświadczeniu⁽⁶⁴⁾ dotyczącym trzech komunikatów Komisji Europejskiej w tej sprawie widoczny był nacisk na zarządzanie granicami. W dokumencie tym wezwano, by przed wprowadzeniem nowych środków ograniczających prawa i swobody podróżnych dokonać oceny skuteczności istniejących środków. Podczas konferencji rozważano jednak również tematy praktyczne, takie jak ochrona danych osobowych dzieci oraz portugalskie doświadczenia w zakresie podnoszenia świadomości w szkołach. Inspektor zabrał głos w kwestii nowych wyzwań dla kręgów zaangażowanych w ochronę danych osobowych i możliwości, które stwarza Traktat z Lizbony.

Tuż przed konferencją zorganizowano warsztaty, aby podsumować wydarzenia w kontekście inicjatywy londyńskiej (zob. sekcja 4.7) i podzielić się wynikami z większością kolegów europejskich.

Następna konferencja europejska odbędzie się w Edynburgu w dniach 23 i 24 kwietnia 2009 r.; skupi się ona na doświadczeniach w związku z dyrektywą 95/46/WE.

⁽⁶⁴⁾ Dostępne na stronie internetowej Inspektora: część „Cooperation” zakładka „International Conference”.

Przedstawiciele personelu uczestniczyli w warsztatach poświęconych rozpatrywaniu spraw; zorganizowano je w Lublanie i Bratysławie w marcu i wrześniu 2008 roku. Ten interesujący mechanizm współpracy na poziomie personelu, służący wymianie najlepszych wzorców wśród europejskich organów ds. ochrony danych, działa już dziesiąty rok. Kolejne warsztaty poświęcone rozpatrywaniu spraw odbędą się w marcu 2009 roku w Pradze.

4.6. Konferencja międzynarodowa

Przedstawiciele organizacji ds. ochrony danych oraz komisarze ds. ochrony prywatności z Europy i innych części świata, w tym z Kanady, Ameryki Łacińskiej, Australii, Nowej Zelandii, Hongkongu, Japonii i innych jurysdykcji w regionie Azji/Pacyfiku od wielu lat spotykają się jesienią na corocznej konferencji. 30. Międzynarodowa Konferencja Komisarzy ds. Ochrony Danych i Prywatności odbyła się w Strasburgu w dniach 15–17 października 2008 r.; jej współgospodarzami – w ściślejszej współpracy z Radą Europy – byli: francuski organ ds. ochrony danych (CNIL) oraz federalny komisarz ds. ochrony danych i wolności informacji z Niemiec. W konferencji wzięli udział liczni delegaci z około 60 państw z całego świata.

Podczas konferencji, której ogólnym tematem była „Prywatność w świecie bez granic”, przewidziano sześć sesji plenarnych w półkolistej sali konferencyjnej Rady Europy: „Prywatność – przeszkoda czy też atut dla globalnego wzrostu gospodarczego?”, „Prywatność – zagrożona przestrzeń?”, „Bezpieczeństwo – w stronę ogólnoświatowej bazy danych identyfikacyjnych?”, „Mam na imię Clara i mam 14 lat, oto moje życie prywatne – moje osiągnięcia”, „Człowiek wspierany przez komputer: cyfrowy anioł czy cyfrowy diabeł?”, „Ograniczenia i nowe instrumenty regulacyjne – przyszłość prywatności”. Odbyła się również sesja zamknięta z udziałem komisarzy.

W konferencji tej uczestniczył Inspektor wraz ze swoim zastępcą. Inspektor był moderatorem panelu dyskusyjnego dotyczącego ograniczeń i nowych instrumentów regulacyjnych, a na sesji zamkniętej przedstawił sprawozdanie na temat inicjatywy londyńskiej.

Na zakończenie konferencji podkreślono potrzebę wiążących przepisów w zakresie ochrony danych w zglobalizowanym świecie. Bez takich międzynarodowych przepisów dla wszystkich uczestników procesu nie będzie możliwe stawienie czoła przyszłym wyzwaniom dotyczącym prywatności. Delegaci wezwali do wzmożonej międzynarodowej



Międzynarodowa konferencja komisarzy ds. ochrony danych i prywatności (Strasburg, 15–17 października 2008 r.)

współpracy organów ds. ochrony danych i podkreślili, że ochrona danych musi odgrywać bardziej znaczącą rolę w strategiach politycznych instytucji publicznych i prywatnych. Należy zapewnić ludziom właściwe środki ochrony ich prywatności.

Podczas konferencji przyjęto różne rezolucje w sprawie nowych technologii i potrzeby dialogu międzynarodowego ⁽⁶⁵⁾:

- rezolucję w sprawie prywatności dzieci w Internecie;
- rezolucję w sprawie ochrony prywatności w serwisach społecznościowych;
- rezolucję w sprawie zbadania możliwości ustanowienia międzynarodowego dnia lub tygodnia ochrony prywatności / ochrony danych;
- rezolucję w sprawie pilnej potrzeby ochrony prywatności w świecie bez granic oraz wypracowania wspólnej propozycji określenia międzynarodowych standardów prywatności i ochrony danych.

Podczas konferencji zaplanowano również utworzenie grupy sterującej ds. reprezentowania konferencji międzynarodowej na posiedzeniach organizacji międzynarodowych.

⁽⁶⁵⁾ Dostępne na stronie internetowej Inspektora: część „Cooperation” zakładka „International Conference”.

Następna konferencja międzynarodowa odbędzie się w Madrycie w dniach 11–13 listopada 2009 r., a jej gospodarzem będzie hiszpański organ ds. ochrony danych *Agencia de Protección de Datos*.

4.7. Inicjatywa londyńska

Na 28. międzynarodowej konferencji w Londynie w listopadzie 2006 roku przedstawiono oświadczenie zatytułowane „Przekazywanie informacji na temat ochrony danych i zwiększanie efektywności tego procesu”, które spotkało się z ogólnym poparciem organów ds. ochrony danych na całym świecie. Była to wspólna inicjatywa prezesa francuskiego organu ds. ochrony danych (CNIL), brytyjskiego komisarza ds. informacji oraz Inspektora (zwana od tamtej pory „inicjatywą londyńską”). Inspektor jako jeden z twórców tej inicjatywy będzie aktywnie uczestniczył w monitorowaniu stosownych działań wraz z krajowymi organami ds. ochrony danych ⁽⁶⁶⁾.

W kontekście inicjatywy londyńskiej zorganizowano wiele warsztatów w celu wymiany doświadczeń i najlepszych praktyk w różnych dziedzinach,

⁽⁶⁶⁾ Zob. sprawozdanie roczne za rok 2006, pkt 4.5 i 5.1.

takich jak komunikacja, egzekwowanie prawa oraz planowanie strategiczne.

W maju 2008 roku kanadyjski komisarz ds. ochrony prywatności był gospodarzem warsztatu w Montrealu poświęconego kwestiom zarządzania w krajowych organach ds. ochrony danych. Była to pierwsza okazja, by wspólnie przyjrzeć się zarządzaniu zasobami ludzkimi (szkolenia i wiedza fachowa), zasobami finansowymi (modele finansowania) oraz zapewnianiu skuteczności (zarządzanie operacyjne i struktura zarządzania), a także zarządzaniu stosunkami zewnętrznymi (inspektorzy ds. prywatności, sieci społeczeństwa obywatelskiego i sieci regionalne).

W październiku 2008 roku Inspektor dokonał przeglądu aktualnego stanu inicjatywy londyńskiej podczas sesji zamkniętej 30. międzynarodowej konferencji w Strasburgu.

Również w roku 2009 mają być organizowane warsztaty w celu wymiany najlepszych wzorców sposobów reagowania na naruszenia bezpieczeństwa.

4.8. Organizacje międzynarodowe

Organizacje międzynarodowe w wielu przypadkach są zwolnione ze stosowania prawa krajowego. W rezultacie często brakuje ram prawnych ochrony danych, nawet w odniesieniu do tych spraw, które wiążą się z gromadzeniem wysoce wrażliwych danych lub ich wymianą między organizacjami. Problem ten poruszono podczas międzynarodowej konferencji w Sydney w 2003 roku, podczas

której wydano rezolucję wzywającą, by „organy międzynarodowe i ponadnarodowe oficjalnie zobowiązały się do [...] stosowania głównych międzynarodowych instrumentów dotyczących ochrony danych i prywatności”.

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

Inspektor wsparł zorganizowaną przez Europejski Urząd Patentowy drugą edycję warsztatów w Monachium w marcu 2007 roku. Przedstawiciele różnych organizacji międzynarodowych omówili istotne dla wszystkich uczestników zagadnienia, takie jak rola inspektorów ochrony danych, sposoby tworzenia systemu ochrony danych oraz współpraca międzynarodowa z podmiotami stosującymi odmienne standardy ochrony danych.

Obecnie rozważane jest zorganizowanie trzeciej edycji warsztatów. Nastąpi to prawdopodobnie pod koniec 2009 lub na początku 2010 roku; warsztaty będą m.in. dotyczyć odpowiedzialnego wykorzystywania biometrii w różnych kontekstach.

5. Komunikacja

5.1. Wprowadzenie

Informacja i komunikacja odgrywają centralną rolę w eksponowaniu głównych działań Inspektora i poszerzaniu wiedzy zarówno o pracy Inspektora, jak i o ochronie danych w ogóle. Ma to tym bardziej strategiczne znaczenie, że EIOD jest instytucją wciąż stosunkowo młodą i dlatego świadomość jej kompetencji na szczeblu UE musi być dalej zwiększana.

Jeżeli spojrzymy wstecz na okres od pierwszego roku działalności Inspektora aż po rok 2008 – ostatni rok pierwszego mandatu – będziemy mogli w pełni ocenić dotychczas poczynione postępy. W początkowych latach działalności Inspektor wyraźnie skupiał swoje działania w zakresie komunikacji na zwiększeniu widoczności na mapie politycznej UE. W stosunkowo krótkim czasie dużo zrobiono, by osiągnąć ten cel. W oparciu o wypracowane w pierwszym roku metody rozwinięto strategię informacyjną zgodnie ze zwyczajową praktyką: stworzenie wyraźnie rozpoznawalnego stylu instytucji (logo, szata graficzna), zdefiniowanie celów ogólnych i szczegółowych, zidentyfikowanie kluczowych adresatów głównych działań Inspektora (zob. sekcja 5.2) oraz wybór narzędzi komunikacyjnych, które powinny być współmierne do każdej rozważanej grupy docelowej. Dalsze prace skupiły się głównie na opracowaniu zestawu narzędzi i wzorców komunikacyjnych, z których zazwyczaj korzystają organy publiczne (np. strona internetowa, biuletyn, broszury, dokumenty bazowe, przemówienia oraz uczestniczenie w konferencjach, komunikaty prasowe, konferencje prasowe, organizacja imprez zwiększających świadomość). Jednocześnie stworzono serwis prasowy, którego zadaniem była komunikacja zewnętrzną za pośrednictwem mediów (zob. sekcja 5.4).

Pięć lat po rozpoczęciu pracy widać, że nacisk położony na komunikację, w tym ukierunkowane podejście oraz opracowanie narzędzi i kanałów informacyjnych i komunikacyjnych, opłacił się i skutkuje zwiększeniem widoczności. Znaczącymi wskaźnikami sukcesu w tym względzie są w szczególności: większa liczba wniosków o udzielenie informacji i porad, wzrost liczby wizyt na stronie internetowej, stale rosnąca liczba odbiorców biuletynu, a także częste wnioski o wizyty studyjne w siedzibie instytucji i zaproszenia do wzięcia czynnego udziału w konferencjach. Ponadto bardziej systematyczny kontakt z mediami i – w jego następstwie – znaczący wzrost obecności działań Inspektora w mediach dodatkowo dowodzą, że Inspektor stał się punktem odniesienia dla problematyki ochrony danych.

Zwiększona widoczność Inspektora w strukturze instytucjonalnej ma bezpośrednie znaczenie dla pełnionych przez niego trzech głównych funkcji: funkcji nadzorczej w odniesieniu do wszystkich instytucji i organów wspólnotowych biorących udział w przetwarzaniu danych osobowych; funkcji konsultatywnej w odniesieniu do tych instytucji (Komisja, Rada i Parlament), które zaangażowane są w opracowywanie i przyjmowanie nowego prawodawstwa i polityk, które mogą mieć wpływ na ochronę danych osobowych; funkcji współpracy z krajowymi instytucjami nadzoru oraz różnymi organami nadzoru w ramach trzeciego filaru.

Specyficznym aspektem świadomości w zakresie ochrony danych w ramach funkcji nadzorczej jest współpraca między Inspektorem a inspektorami ochrony danych (DPO) w instytucjach i organach Wspólnoty. Ścisła współpraca z inspektorami ochrony danych jest istotnym sposobem udostępniania dobrych wzorców i skutecznej wspólnej pracy na rzecz zwiększania świadomości w zakresie problematyki ochrony danych wśród zainteresowanych stron z UE i wśród personelu UE. Inspektor pragnie

dalej pogłębiać tę współpracę, w szczególności przez zachęcanie do wspólnych działań i synergii, na przykład w kontekście organizowania imprez służących zwiększeniu świadomości, takich jak coroczny Dzień Ochrony Danych obchodzony 28 stycznia lub w sąsiedztwie tej daty.

Podnoszenie świadomości i polepszanie komunikacji w zakresie odpowiednich kwestii dotyczących ochrony danych były również ważnym celem inicjatywy londyńskiej (zob. również pkt 4.7.). Jednym z istotnych rezultatów pierwszego warsztatu w tym kontekście było utworzenie (z udziałem Inspektora) sieci urzędników ds. informacji. Organy ds. ochrony danych wykorzystują tę sieć do wymiany najlepszych wzorców i do realizowania określonych projektów, takich jak podejmowanie wspólnych działań przy okazji istotnych wydarzeń.

Inną interesującą inicjatywą w kontekście lepszej komunikacji i skuteczniejszej ochrony danych jest projekt EuroPrise, który powstał w celu sprawdzenia możliwości wprowadzenia europejskiego systemu etykiet prywatności dla towarów i usług zgodnych z zasadami poszanowania prywatności. Projekt ten został pomyślnie zrealizowany przez Niezależne Centrum ds. Ochrony Prywatności w Szlezwiku-Holsztynie – regionalny organ ds. ochrony danych w Kilonii (Niemcy), przy współudziale szeregu innych zainteresowanych stron, między innymi kilku innych krajowych lub regionalnych organów ds. ochrony danych w Europie.

W lipcu 2008 roku Inspektor miał możliwość uczestniczenia w obchodach 30 rocznicy zainicjowania ochrony danych w Szlezwiku-Holsztynie; przy tej okazji przekazał również jednej z firm pierwszą europejską etykietę prywatności za opracowanie wyszukiwarki zgodnej z zasadami poszanowania prywatności. Celem tej imprezy było również ogólne poparcie europejskiej etykiety prywatności jako istotnego i potrzebnego mechanizmu służącego promowaniu produktów i usług informatycznych zgodnych z zasadami poszanowania prywatności. Inspektor uczestniczył również w przekazaniu kolejnych trzech europejskich etykiet prywatności podczas warsztatu EuroPrise w Sztokholmie w listopadzie 2008 roku ⁽⁶⁷⁾.

Inspektor postrzega europejską etykietę prywatności jako jeden ze szczególnie kreatywnych i obiecujących instrumentów służących promowaniu i zapewnianiu

⁽⁶⁷⁾ Zob.: „Ochrona danych w Szlezwiku-Holsztynie, w Europie i w globalnym społeczeństwie informacyjnym”, Kilonia, 14 lipca 2008 roku, oraz „Komentarz wstępny w sprawie prezentacji europejskich etykiet prywatności”, Sztokholm, 13 listopada 2008 roku, przemówienia dostępne na stronie internetowej Inspektora.



EuroPrise – uroczystość wręczenia pierwszej europejskiej etykiety prywatności (Kilonia, 14 lipca 2008 r.)

skutecznej ochrony. Z jednej strony instrument ten dobrze pasuje do kluczowego pojęcia „wbudowanej ochrony prywatności” jako skuteczny środek zapewnienia zgodnych z zasadami poszanowania prywatności i, tam gdzie to możliwe nawet wzmacniających prywatność, produktów i usług informatycznych. Z drugiej strony oferuje on wyraźną zachętę podmiotom, które opracowują i dostarczają takie produkty i usługi, aby inwestowały w lepszą ochronę prywatności i korzystały z tych inwestycji, gdy jest to uzasadnione. Jest to również wyraźnie korzystne dla użytkowników i wszystkich innych osób, które mają w tych kwestiach prawo do podjęcia decyzji opartych na znajomości faktów.

Następne części tego rozdziału opisują działania Inspektora w 2008 roku w zakresie przekazywania informacji; obejmowały one udział Inspektora w warsztatach i konferencjach, pracę służby prasowej i zewnętrzną komunikację z mediami, rozpatrywanie wniosków o udzielenie informacji, rozwijanie narzędzi do udostępniania informacji w Internecie (takich jak strona internetowa i biuletyn elektroniczny), przygotowywanie materiałów wydawniczych, wizyty studyjne oraz organizowanie imprez zwiększających świadomość.

5.2. Aspekty działań informacyjnych

Polityka informacyjna Inspektora musi być kształtowana z uwzględnieniem specyficznych aspektów, które mają znaczenie ze względu na krótki czas działania tej instytucji, jej rozmiar i zakres kompetencji. Wymaga ona zatem podejścia dostosowanego do potrzeb i wykorzystującego właściwe narzędzia, aby dotrzeć do odpowiednich odbiorców, a jednocześnie być w stanie dostosować się do rozmaitych ograniczeń i wymogów.

Główni odbiorcy i grupy docelowe

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

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

Stosowany język

Polityka informacyjna Inspektora musi również uwzględniać szczególnie charakter działalności tej instytucji.

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

W przypadku bardziej wyspecjalizowanych odbiorców (np. media, specjaliści w zakresie ochrony danych, zainteresowane podmioty z UE) stosowanie terminów technicznych i prawnych jest bardziej celowe. W tym sensie może być konieczne przekazywanie tych samych wiadomości przy użyciu dostosowanej formy

i stylu, odpowiadających odbiorcom docelowym (zróznicowanie między ogółem społeczeństwa a odbiorcami bardziej wyspecjalizowanymi).

Wpływ

Aby zapewnić jak największą skuteczność, styl informacyjny stosowany przez Inspektora opiera się na zasadzie: „nadmiar informacji osłabia przekaz”, która sugeruje, by unikać zalewu informacyjnego. Wykorzystanie tradycyjnych narzędzi informowania, takich jak komunikaty prasowe, celowo ogranicza się do kwestii o większym znaczeniu – do sytuacji, gdy uznaje się, że konieczne i właściwe jest zareagowanie i poinformowanie jak najszerszego kręgu odbiorców.

Mierzenie skutków działań w zakresie przekazywania informacji ma również decydujące znaczenie, aby ocenić skuteczność stosowanego podejścia oraz, w razie konieczności, przeorientować dane działanie. Dlatego też, z myślą o tym, w roku 2009 zostanie przeprowadzony przegląd strategii informacyjnej, która została ustalona w wyniku utworzenia instytucji Inspektora.

5.3. Przemówienia

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

Inspektor był często obecny na posiedzeniach Komisji Parlamentu Europejskiego ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) lub uczestniczył w podobnych wydarzeniach. W dniu 21 stycznia zabrał głos na otwartym seminarium dotyczącym fuzji Google i Double Click. W dniu 11 lutego przedstawił uwagi na temat projektu decyzji ramowej w sprawie ochrony danych w trzecim filarze. W dniu 26 marca przedstawił swoją opinię w sprawie aspektów bezpieczeństwa oraz biometrii w paszportach; streścił też swoje sprawozdanie roczne za rok 2007. W dniu 5 maja przedstawił opinię na temat zmiany dyrektywy w sprawie e-privacy. W dniu 29 maja wypowiedział się podczas spotkania okrągłego stołu dotyczącego dublińskiego systemu azylowego w odniesieniu do skoordynowanego nadzorowania systemu Eurodac. W dniu 2 czerwca zabrał głos podczas wysłuchania poświęconego publicznemu dostępowi do dokumentów. W dniu 30 czerwca dwukrotnie wypowiedział się podczas spotkania okrągłego stołu dotyczącego granic zewnętrznych. W dniu 8 września przedstawił



Peter Hustinx wygłasza przemówienie podczas międzynarodowej konferencji komisarzy ds. ochrony danych i prywatności (Strasburg, 15–17 października 2008 r.)

dotatkowe uwagi na temat zmiany dyrektywy w sprawie usługi powszechnej i dyrektywy w sprawie e-prywatności.

Inspektor brał również udział w innych posiedzeniach w Parlamencie Europejskim. W dniu 26 lutego wypowiedział się na posiedzeniu Komisji Zatrudnienia na temat kwestii dotyczących zabezpieczenia społecznego. W dniu 14 maja zabrał głos na posiedzeniu z udziałem sekretarza generalnego i dyrektorów generalnych Parlamentu poświęconym przestrzeganiu przepisów rozporządzenia (WE) nr 45/2001. W dniu 17 września omówił z posłami do Parlamentu Europejskiego z różnych komisji i grup politycznych rozmaite kwestie dotyczące zmiany dyrektywy o e-prywatności. W dniu 6 listopada zabrał głos na seminarium Służby Prawnej Parlamentu na temat aktualnych kwestii na styku pierwszego i trzeciego filaru.

W dniu 25 marca na forum działającej w ramach Rady Multidyscyplinarnej Grupy ds. Przestępczości Zorganizowanej Inspektor przedstawił swoją opinię na temat wniosku w sprawie europejskiego systemu danych dotyczących przelotu pasażera (PNR). W dniu 11 września pojawił się po raz drugi na posiedzeniu tej grupy, aby przekazać swoje uwagi na temat

kwestii strategicznych przedstawionych przez prezydencję francuską. W dniu 30 września zabrał głos podczas konferencji w Paryżu dotyczącej badań w zakresie bezpieczeństwa, która została zorganizowana w ramach prezydencji francuskiej. W dniu 6 października wziął udział w podobnej konferencji w Nicei zatytułowanej „Internet przedmiotów”. W dniu 11 grudnia zabrał głos podczas seminarium dotyczącego publicznego dostępu do dokumentów, które zostało zorganizowane przez stałe przedstawicielstwo Finlandii w Brukseli.

Na liście kontaktów znalazły się również inne instytucje UE. W dniu 24 kwietnia Inspektor oraz jego zastępca złożyli wizytę w Sądzie ds. Służby Publicznej w Luksemburgu, aby przedstawić informacje na temat odpowiednich kwestii dotyczących ochrony danych. W dniu 12 czerwca Inspektor zabrał głos na posiedzeniu z udziałem sekretarza generalnego i dyrektorów generalnych Komisji Europejskiej poświęconym przestrzeganiu przepisów rozporządzenia (WE) nr 45/2001. W dniu 17 grudnia Inspektor wraz ze swoim zastępcą zabrał głos podczas zorganizowanego przez siebie w Brukseli seminarium z udziałem zainteresowanych podmiotów dotyczącego nadzoru instytucji UE.

W dniu 25 stycznia Inspektor wygłosił odczyt w Kolegium Europejskim w Brugii pt. „Ochrona danych osobowych w UE: zasady, uczestnicy i wyzwania”. W dniu 26 maja wziął udział w konferencji w Europejskiej Akademii Prawa w Trewirze dotyczącej ochrony danych w trzecim filarze. W dniu 10 czerwca odwiedził Europejski Instytut Uniwersytecki we Florencji i wygłosił odczyt pt. „Przepisy UE dotyczące ochrony danych w globalnej gospodarce: zagrożenia i groźby dla zbiorowego bezpieczeństwa i praw człowieka”.

Pod koniec stycznia Inspektor przebywał w USA i odbył szereg spotkań z urzędnikami federalnymi i innymi zainteresowanymi stronami zajmującymi się prywatnością. W dniu 28 stycznia wziął udział w konferencji w Duke University w Durham w Karolinie Północnej (USA) z okazji obchodów Dnia Prywatności Danych. W dniu 29 stycznia wygłosił przemówienie w Georgetown University w Waszyngtonie, DC. W dniu 30 stycznia wygłosił odczyt w Washington College of Law przy American University w Waszyngtonie, DC. W dniu 31 stycznia zabrał głos podczas spotkania zorganizowanego przez Instytut Europejski w Waszyngtonie, DC.

Inspektor spotykał się również z posłami do parlamentów krajowych. W dniu 5 marca zeznawał przed komisją Izby Lordów w Londynie w sprawie społeczeństwa kontrolowanego. W dniu 20 marca uczestniczył w seminarium dotyczącym kwestii związanych z prywatnością zorganizowanym przez Komisję ds. Sprawiedliwości senatu holenderskiego. W dniu 2 kwietnia wziął udział w posiedzeniu podkomisji Izby Lordów w Brukseli dotyczącym europejskiego systemu danych dotyczących przelotu pasażera. W dniu 4 kwietnia zabrał głos na szóstym kolokwium parlamentarnym Paryż – Berlin pt. „Zbiorowe bezpieczeństwo a wolności indywidualne” w Lyonie dotyczącym zapewnienia właściwej równowagi między bezpieczeństwem, mobilnością a prywatnością.

W ciągu tego roku Inspektor odwiedził także różne państwa członkowskie przy innych okazjach. W dniu 23 stycznia zabrał głos w Instytucie Nauk Politycznych w Paryżu podczas konferencji dotyczącej biometrii. W dniu 15 lutego uczestniczył w posiedzeniu komitetu doradczego rządu holenderskiego ds. bezpieczeństwa i prywatności, które odbyło się w Hadze. W dniu 3 marca zabrał głos na konferencji dla studentów wydziału prawa Uniwersytetu Erazma w Rotterdamie. W dniu 28 kwietnia przedstawił w Instytucie Oceny Technologii w Wiedniu swój dokument strategiczny pt. „Realizowane przez

UE programy badań i rozwoju technologicznego”. W dniu 6 maja zabrał głos podczas dziewiątej konferencji poświęconej ochronie danych, która odbyła się w Berlinie; tematem wystąpienia były strategiczne wyzwania dla ochrony danych w Europie”. W dniu 28 maja uczestniczył w panelu dyskusyjnym w Międzynarodowej Izbie Handlowej w Paryżu. W dniu 6 czerwca wygłosił przemówienie na temat opłat za korzystanie z sieci drogowej podczas konferencji w Genewie dotyczącej inteligentnych systemów transportowych. W dniu 20 czerwca wygłosił przemówienie na temat ochrony danych w UE w siedzibie węgierskiego organu ds. ochrony danych w Budapeszcie. W dniu 14 lipca uczestniczył w obchodach 30 rocznicy ochrony danych w Szlezwiku-Holsztynie i wygłosił przemówienie w Kilonii (zob. też sekcja 5.1).

W dniu 16 września zabrał głos podczas szczytu doradztwa korporacyjnego w Genewie. W dniu 23 września uczestniczył w debacie jawnej w Amsterdamie poświęconej kwestiom prywatności. W dniu 25 września wygłosił przemówienie podczas konferencji międzynarodowej sekcji amerykańskiego stowarzyszenia prawników, która odbyła się w Brukseli. W dniu 11 października uczestniczył w paryskiej konferencji poświęconej wyzwaniom w dziedzinie bezpieczeństwa i prywatności. W dniu 22 października zabrał głos na konferencji „Biometria 2008” w Londynie. W dniu 27 października zabrał głos podczas konferencji RSA w Londynie dotyczącej naruszania bezpieczeństwa i kwestii e-prywatności. W dniu 2 czerwca w Brukseli uczestniczył w konferencji na temat zarządzania granicami. W dniu 3 grudnia zabrał głos w kwestii „proporcjonalności” podczas londyńskiej konferencji dotyczącej wymiaru sprawiedliwości. W dniu 9 grudnia omówił kwestie prywatności i badań w zakresie bezpieczeństwa podczas posiedzenia podgrupy europejskiego forum badań i innowacji w dziedzinie bezpieczeństwa w Ispra.

Zastępca Inspektora przedstawił podobne prezentacje. W dniu 11 kwietnia przedstawił w *Centre d'Estudis* rządu katalońskiego prezentację dotyczącą roli ochrony danych w postępowaniach sądowych. W dniu 6 maja mówił o konfliktach między bezpieczeństwem a ochroną danych podczas międzynarodowego seminarium zorganizowanego przez kataloński organ ds. ochrony danych. W tym samym dniu w Barcelonie a 7 maja w Madrycie na posiedzeniu grupy radców prawnych wygłosił przemówienie na temat nadchodzących ewentualnych zmian w dyrektywach UE dotyczących ochrony danych. W dniu 20 maja w Madrycie wystąpił z prezentacją na seminarium szkoleniowym dla sędziów i prokuratorów na temat

wpływu ochrony danych w kontekście postępowań cywilnych. W dniu 22 maja omówił nową decyzję ramową w sprawie ochrony danych podczas międzynarodowego seminarium dla sędziów i prokuratorów w Toledo.

W dniu 9 września w Budapeszcie podczas corocznej konferencji europejskich firm specjalizujących się w niszczeniu danych poruszył temat przechowywania, wykasowywania danych oraz środków bezpieczeństwa w odniesieniu do danych osobowych. W dniu 4 października podczas corocznej konferencji Europejskiej Rady Adwokatów Karnistów w Bratysławie zaprezentował nowy europejski system przekazywania informacji z rejestrów karnych (ECRIS). W dniu 7 października przedstawił przyszłe wyzwania dla ochrony danych podczas seminarium zorganizowanego w Parlamencie Europejskim w Brukseli przez Grupę Porozumienia Liberatów i Demokratów na rzecz Europy. W dniu 28 października wypowiedział się na temat danych medycznych podczas posiedzenia publicznej sieci opieki zdrowotnej Andaluzji w Granadzie. W dniu 25 listopada przedstawił prezentację dotyczącą wpływu nowych technologii w dziedzinie bezpieczeństwa podczas seminarium zorganizowanego przez Centrum Studiów Polityki Europejskiej (CEPS) w Brukseli. W dniu 3 grudnia wypowiedział się na temat ochrony danych i informacji sądowych podczas warsztatu zorganizowanego przez Sąd Najwyższy kraju Basków w Bilbao. W dniu 12 grudnia w Hadze wypowiedział się na temat równowagi między bezpieczeństwem a ochroną danych podczas siódmej corocznej konferencji sieci międzynarodowego prawa karnego.

5.4. Kontakty z mediami

Służba prasowa

Służba prasowa odpowiada za zewnętrzną komunikację z mediami polegającą na regularnych kontaktach



Zespół ds. informacji

z dziennikarzami. Zajmuje się również wnioskami o udzielenie informacji i porad, o które zwraca się prasa, zainteresowane strony lub obywatele, redagowaniem komunikatów prasowych i biuletynów, a także organizowaniem konferencji prasowych, wizyt studyjnych oraz wywiadów udzielanych przez Inspektora lub jego zastępcę. Ponadto rzecznik prasowy kieruje elastycznym zespołem ds. informacji, który zapewnia wsparcie w zakresie działań informacyjnych i bierze udział w wydarzeniach o charakterze promocyjnym (w szczególności organizowanie Dnia Ochrony Danych i Dnia Otwartych Drzwi w Instytucjach Europejskich; zob. sekcja 5.9).

Kontakty z mediami

Inspektor chce w jak największym stopniu być dostępny dla dziennikarzy, aby umożliwić ogółowi społeczeństwa śledzenie jego pracy. Regularnie informuje media głównie za pośrednictwem komunikatów prasowych, wywiadów, dyskusji wyjaśniających tło wydarzeń oraz konferencji prasowych. Rozpatrywanie otrzymywanych regularnie pytań ze strony mediów (prośb o informacje lub komentarze) – głównie dotyczących kwestii interesujących szeroki ogół społeczeństwa – umożliwia dodatkowy z nimi kontakt.

W 2008 roku służba prasowa wydała 13 komunikatów prasowych, czyli średnio w całym roku co miesiąc ukazywał się jeden komunikat. Większość z tych komunikatów dotyczyła nowych opinii w sprawie aktów prawnych, mających istotne znaczenie z punktu widzenia ogółu społeczeństwa. Dotyczyły one m.in. następujących zagadnień: proponowanego przez UE systemu zarządzania granicami zewnętrznymi, technologii biometrycznych w paszportach, przeglądu dyrektywy o e-prywatności, publicznego dostępu do dokumentów UE, transatlantyckiej wymiany informacji do celów egzekwowania prawa oraz przyjęcia decyzji ramowej w sprawie ochrony danych w trzecim filarze. Komunikaty prasowe publikowane są w językach angielskim i francuskim na stronie internetowej Inspektora oraz w prowadzonej przez Komisję międzyinstytucjonalnej bazie danych obejmującej komunikaty prasowe (RAPID). Są one rozsyłane do regularnie aktualizowanej sieci kontaktowej 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



Peter Hustinx i Joaquín Bayo Delgado przedstawiają prasie sprawozdanie za 2007 rok

m.in. na stronach instytucji i organów UE, organizacji pozarządowych, instytucji naukowych i firm informatycznych.

W roku 2008 Inspektor udzielił około 25 wywiadów dziennikarzom z całej Europy oraz z państw trzecich reprezentującym prasę, radio i telewizję oraz media elektroniczne. Zaowocowało to wieloma cytatami i artykułami w prasie krajowej (np. „Daily Telegraph”, BBC, „New York Times”, różne gazety niemieckie i holenderskie, Węgierska Agencja Prasowa), w prasie międzynarodowej i prasie UE (np. „The Economist”, „European Voice”, „Euractiv”), w publikacjach i na stronach internetowych zajmujących się kwestiami ochrony danych i technologii informatycznych, jak też w radiu i telewizji (np. Deutsche Welle, Telewizja Holenderska, Radio 1 RAI, Polskie Radio). Wywiady te dotyczyły następujących kwestii: europejskiego systemu danych dotyczących przelotu pasażera, dyrektywy w sprawie zatrzymywania danych, proponowanego przez UE systemu zarządzania granicami zewnętrznymi, amerykańskiego programu znoszenia wiz, systemu informacyjnego Schengen (SIS), prywatności w opiece zdrowotnej oraz adekwatności ochrony danych na szczeblu UE.

5.5. Prośby o udzielenie informacji

Liczba składanych przez ogół społeczeństwa próśb o udzielenie informacji lub pomoc wzrosła do ponad 180 w 2008 roku (dla porównania w roku 2007 otrzymano 160 wniosków). Prośby te pochodziły od różnych osób i podmiotów, m.in. od zainteresowanych stron, które działają w środowisku unijnym lub których praca wiąże się z ochroną danych (firmy prawnicze, firmy konsultingowe, lobbysci, organizacje pozarządowe, stowarzyszenia, wyższe uczelnie, itd.), oraz od obywateli zwracających się o dodatkowe informacje dotyczące problematyki ochrony danych lub o pomoc w rozwiązaniu wątpliwości lub problemów napotykanym w praktyce. Wnioski te kierowane są głównie na główny adres poczty elektronicznej Inspektora, a od czasu do czasu przychodzą zwykłą pocztą.

Prośby o informację to szeroka kategoria, która obejmuje między innymi ogólne pytania dotyczące polityk i prawodawstwa UE w zakresie ochrony danych zarówno w UE, jak i na szczeblu krajowym, ale także bardziej szczegółowe pytania i pytania o charakterze technicznym dotyczące konkretnych aspektów mających związek

z prywatnością i z ochroną danych osobowych. W 2008 roku otrzymano na przykład prośby o informacje dotyczące zdarzeń związanych z naruszeniem bezpieczeństwa, technologii biometrycznych, technologii identyfikacji radiowej (RFID), prywatności w Internecie – w tym społeczności sieciowych, e-monitoringu i rejestrowania rozmów telefonicznych, przetwarzania obrazów, uruchomienia Google Street View, przeglądu pakietu UE dotyczącego łączności elektronicznej, przekazywania danych osobowych do państw trzecich, a także przepisów Traktatu z Lizbony dotyczących ochrony danych osobowych.

Warto zauważyć, że znaczna liczba prośb o udzielenie informacji otrzymanych od ogółu społeczeństwa dotyczy kwestii krajowych, w odniesieniu do których Inspektor nie ma żadnych kompetencji. W takich przypadkach wysyła się odpowiedź, w której precyzuje się mandat Inspektora oraz zaleca się, by odbiorca zwrócił się do odpowiedniego organu, zazwyczaj do krajowego organu danego państwa członkowskiego ds. ochrony danych.

Wnioski, które nie dotyczą jedynie udzielenia informacji i które z tego względu wymagają pogłębionej analizy rozpatrywane są zazwyczaj przez urzędników odpowiedzialnych za konkretną sprawę. W roku 2008 dotyczyły one kwestii takich jak: dane PNR, SIS, ochrona danych w związku z wymianą transatlantycką, biometria w systemie Eurodac, ochrona danych w postępowaniach karnych, wiążące zasady dla przedsiębiorstw oraz powiązanie ochrony danych z prawem konkurencji.

Podobnie jak w latach poprzednich większość otrzymanych wniosków sporządzono w języku angielskim, w mniejszym stopniu w językach: francuskim, niemieckim, włoskim i hiszpańskim. Dzięki temu służba prasowa szybko udzielała odpowiedzi, bez problemu mieszcząc się w limicie 15 dni roboczych. Tylko kilka wniosków sporządzono w innych językach urzędowych UE, co sprawiło, że potrzebna była pomoc służby tłumaczeniowej Rady.

5.6. Wizyty studyjne

W ramach działań, których celem jest większe uwidocznienie Inspektora, a także współdziałanie z kręgami akademickimi, Inspektor gościł grupy studentów specjalizujących się w dziedzinie prawa europejskiego, problematyce ochrony danych lub w kwestiach związanych z bezpieczeństwem systemów informatycznych. Przykładowo w marcu

2008 roku Inspektor spotkał się z grupą studentów prawa międzynarodowego i europejskiego z Uniwersytetu Tilburskiego.

Również inne grupy zorganizowane odwiedziły siedzibę Inspektora, w tym w maju 2008 roku delegacja Komisji Sprawiedliwości Izby Reprezentantów parlamentu holenderskiego. Także przedstawiciele duńskiej organizacji IT-Political Association spotkali się w lutym z Inspektorem, aby omówić wpływ aktualnych inicjatyw z zakresu zatrzymywania danych i nadzoru na zagadnienia dotyczące prywatności i ochrony danych.

5.7. Internetowe narzędzia informacyjne

Strona internetowa

Strona internetowa pozostaje najważniejszym narzędziem informacyjnym Inspektora. Jest ona również środkiem, który umożliwia odwiedzającym wgląd do wszelkich różnorodnych dokumentów sporządzonych w ramach działań Inspektora (opinii dotyczących kontroli wstępnych i wniosków dotyczących prawodawstwa UE, uwag, priorytetów w pracy, publikacji, przemówień, komunikatów prasowych, biuletynów, informacji na temat wydarzeń, itd.). Z tego względu strona internetowa jest prawie codziennie uaktualniana i zamieszczane są na niej odpowiednie dokumenty i informacje.

Zmiany zawartości strony

Zgodnie z zapowiedzią w sprawozdaniu rocznym za 2007 rok w roku 2008 opracowano narzędzia informacyjne, aby jeszcze bardziej ulepszyć zawartość strony internetowej i lepiej zaspokoić oczekiwania osób ją odwiedzających.

Między innymi opracowano słowniczek terminów dotyczących ochrony danych osobowych. Słowniczek zawiera 75 terminów przy których zamieszczone są linki do zewnętrznych i wewnętrznych stron witryny internetowej Inspektora, co umożliwia uzyskanie dodatkowych informacji. Słowniczek ma być głównie narzędziem, które pomaga osobom odwiedzającym stronę internetową w lepszym zrozumieniu działań i prac Inspektora, jak również szerszego kontekstu zagadnień związanych z ochroną danych. Jednocześnie opracowano też sekcję „Pytania i odpowiedzi”. Miała ona służyć w szczególności objaśnieniu mandatu, kompetencji i obszarów działania Inspektora oraz spełniać funkcje bieżącego przewodnika w odniesieniu do najczęściej zadawanych pytań. Sekcja zapewnia informacje uzupełniające oraz, jeżeli zajdzie

taka potrzeba, praktyczne wytyczne dotyczące takich zagadnień, jak obowiązki i kompetencje Inspektora, prawodawstwo w zakresie ochrony danych na szczeblu UE, prawa osoby, której dane dotyczą, przepisy regulujące przetwarzanie danych osobowych i ich przekazywanie.

Uruchomienie tych dwóch nowych sekcji zaplanowano na początek 2009 roku. Jako uzupełnienie sekcji „Pytania i odpowiedzi” przygotowuje się również dokument dotyczący najczęściej zadawanych pytań; ma on zapewnić odpowiedzi skierowane do odbiorców o różnym profilu i do konkretnych grup docelowych (np. pracownicy UE, osoby odwiedzające, osoby ubiegające się o wolne stanowiska w instytucjach i organach Wspólnoty).

Rozwój techniczny

Aby usprawnić działanie uruchomionej w 2007 roku strony internetowej Inspektora, w 2008 roku wprowadzono ulepszenia techniczne w celu ułatwienia nawigacji. Dotyczyło to stron zawierających dużą liczbę dokumentów, w szczególności strony, na której zamieszczony był wykaz opinii Inspektora dotyczących kontroli wstępnych; stronę tę trzeba było na nowo opracować i podzielić, aby zapewnić sprawne działanie witryny.

Oprócz polepszenia ogólnego działania strony internetowej dodano do niej funkcję wyszukiwania. Ta nowa funkcja umożliwia odwiedzającym łączenie szukanych terminów i przeprowadzanie konkretnych wyszukiwań w dokumentach PDF. To wyszukiwanie zaawansowane trzeba będzie jednak dostosować w 2009 roku, aby uzyskać lepsze i bardziej wiarygodne wyniki.

W styczniu 2008 roku zainstalowano narzędzie statystyczne dostarczające danych na temat ruchu i nawigacji. Dane statystyczne wskazują, że od dnia 1 lutego do dnia 31 grudnia 2008 r. zarejestrowano 81841 wejść na stronę, z kulminacją wynoszącą 10095 wejść w maju, w czasie gdy opublikowane zostało sprawozdanie roczne za rok 2007. Oprócz strony głównej i strony zawierającej funkcję wyszukiwania zaawansowanego, najczęściej odwiedzanymi stronami witryny były strony dotyczące wiadomości, komunikatów prasowych oraz sprawozdań rocznych.

W ramach Międzyinstytucjonalnego Komitetu ds. Redagowania Treści Internetowych (CEiii) administrator strony internetowej Inspektora nadal brał udział w dyskusjach dotyczących opracowania

międzyinstytucjonalnego narzędzia wyszukiwania, które należy w przyszłości udostępnić na europejskiej stronie internetowej.

W roku 2009 strona internetowa zostanie zaktualizowana, aby uwzględnić mianowanie Inspektora i Zastępcy Inspektora na drugą kadencję. Przygotowywane są również usprawnienia techniczne, w szczególności w zakresie funkcji zaawansowanego wyszukiwania, a także polepszenia wyglądu strony. Zostanie ponadto rozpoczęta analiza dotycząca możliwej restrukturyzacji głównej strony internetowej, by stała się ona bardziej dynamiczna i lepiej uwzględniała bieżące informacje na temat działań Inspektora.

Biuletyn

Biuletyn Inspektora jest nadal skutecznym narzędziem służącym podniesieniu świadomości w odniesieniu do bieżących działań Inspektora i zwróceniu uwagi na najnowsze uaktualnienia na stronie internetowej. Dostarcza on wiadomości na temat bieżących opinii Inspektora dotyczących wniosków prawodawczych UE i kontroli wstępnych oraz zawiera informacje o nadchodzących imprezach i konferencjach w terenie oraz o ostatnich wypowiedziach Inspektora. Biuletyny dostępne są na stronie internetowej Inspektora, na której można również zamówić automatycznie ich subskrypcję.

W 2008 roku opublikowano pięć wydań biuletynu Inspektora; ukazywały się one średnio co dwa miesiące. Biuletyn publikowany jest w języku angielskim i francuskim.

Liczba subskrybentów wzrosła z 635 osób pod koniec 2007 roku do 880 osób pod koniec roku 2008. Należą do nich między innymi posłowie do Parlamentu Europejskiego, pracownicy UE oraz krajowych organów ds. ochrony danych, a także dziennikarze, przedstawiciele środowiska akademickiego, firmy telekomunikacyjne i prawnicze.

Wyraźny i stały wzrost liczby subskrypcji sprawił, że konieczne stało się ulepszenie publikacji przez nadanie jej wyglądu, który byłby bardziej przyjazny dla odbiorcy. Celem jest również zmiana struktury biuletynu, by polepszyć jego czytelność.

Z myślą o tym w roku 2008 rozpoczęto prace przygotowawcze przy udziale agencji ds. komunikacji, która specjalizuje się w publikowaniu informacji na temat polityki europejskiej; celem jest określenie potrzeb i przeanalizowanie sposobów realizacji. W roku 2009 będą nadal kontynuowane prace służące urzeczywistnieniu tego projektu.

5.8. Publikacje

Sprawozdanie roczne

Sprawozdanie roczne to podstawowa publikacja Inspektora. Ukazuje się ono zazwyczaj wiosną i jest przeglądem działań Inspektora w trakcie roku sprawozdawczego w głównych obszarach operacyjnych nadzoru, konsultacji i współpracy. Opisuje również osiągnięcia w zakresie komunikacji zewnętrznej, a także działania dotyczące administracji, budżetu i personelu.

Sprawozdanie to może zwłaszcza zainteresować różne grupy i osoby na szczeblu międzynarodowym, europejskim i krajowym – ogólnie osoby, których dane dotyczą, a w szczególności pracowników KE, system instytucjonalny UE, organy ds. 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 przedstawił swoje sprawozdanie roczne za rok 2007 Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego w dniu 26 marca 2008 r.

Następnie w połowie maja zorganizowano konferencję prasową, aby przedstawić to sprawozdanie mediom. Podczas konferencji prasowej podkreślono znaczenie Traktatu z Lizbony dla zwiększenia ochrony danych osobowych. Inspektor skorzystał z tej okazji, by podkreślić, że nowy traktat należy postrzegać jako możliwość wykazania przez administrację UE, że skuteczna ochrona danych osobowych jest jedną z fundamentalnych wartości leżących u podstaw polityk UE.

Broszura informacyjna

W związku z ustanowieniem urzędu Inspektora pod koniec 2004 roku opracowano dwie różne broszury mające na celu podniesienie świadomości w odniesieniu do tej nowej instytucji. Jedną z broszur przedstawia Inspektora z instytucjonalnego punktu widzenia, natomiast druga opisuje prawa osób, których dane przetwarzane przez instytucje i organy Wspólnoty.

W roku 2008 rozpoczęto opracowywanie zaktualizowanej wersji broszury informacyjnej, która scala dwie istniejące broszury, zwłaszcza z myślą o kończącej się w styczniu 2009 roku pierwszej kadencji Inspektora. Ta konieczna aktualizacja będzie również okazją do stworzenia unowocześnionej broszury. Ten nowy materiał informacyjny ukaże

w sposób dynamiczny i bezpośredni kluczowe aspekty działań Inspektora oraz ochrony danych osobowych na szczeblu UE, jak też dostarczy praktycznych informacji.

5.9. Przedsięwzięcia zwiększające świadomość

Udział Inspektora w imprezach mających związek z UE stanowi doskonałą okazję do zwiększania wiedzy na temat praw przysługujących osobom, których dane dotyczą oraz na temat obowiązków instytucji i organów Wspólnoty w zakresie prywatności i ochrony danych osobowych.

Dzień Ochrony Danych

Państwa członkowskie Rady Europy oraz instytucje europejskie obchodziły w dniu 28 stycznia 2008 r. po raz drugi Dzień Ochrony Danych. Data ta upamiętnia rocznicę uchwalenia konwencji Rady Europy nr 108 – pierwszego prawnie wiążącego instrumentu międzynarodowego dotyczącego ochrony danych, który przyjęto w 1981 roku.

Wydarzenie to sprawiło, że Inspektor miał okazję skupić się na podniesieniu świadomości pracowników UE oraz każdej zainteresowanej osoby w zakresie ich praw i obowiązków w odniesieniu do ochrony danych. W tym celu w Parlamencie Europejskim, w Komisji Europejskiej oraz w siedzibie Rady działało przez trzy kolejne trzy dni stoisko informacyjne. Inspektor przedstawił w skrócie swoją rolę nadzorczą, konsultatywną i operacyjną, jak też swoje osiągnięcia i bieżące działania. Stoisko



Stoisko Inspektora w Komisji Europejskiej podczas Dnia Ochrony Danych (Bruksela, 30 stycznia 2008 r.)

Inspektora zorganizowano przy współpracy inspektorów ochrony danych odpowiednich instytucji, którzy również przedstawili swoje działania.

Pracownicy Inspektora gościli około 250 odwiedzających. Rozdano różne materiały informacyjne przedstawiające działalność Inspektora, a także wiele rozmaitych upominków promocyjnych. Odwiedzający mieli również możliwość sprawdzenia swojej wiedzy na temat ochrony danych w krótkim quizie oraz wzięcia udziału w losowaniu nagród.

Celem następnej edycji Dnia Ochrony Danych będzie dalsze rozwijanie tej szczególnej imprezy, zwłaszcza poprzez większą współpracę z siecią inspektorów ochrony danych i zapewnienie szerszej gamy materiałów informacyjnych.

Dzień Otwartych Drzwi w instytucjach UE

W dniu 7 czerwca 2008 r. biuro Inspektora uczestniczyło również, jak czyni to każdego roku, w Dniu Otwartych Drzwi w instytucjach Unii Europejskiej zorganizowanym w Parlamencie Europejskim w Brukseli.

Stoisko Inspektora zostało umieszczone w głównym gmachu Parlamentu Europejskiego a jego pracownicy odpowiadali na pytania odwiedzających dotyczące roli i działań Inspektora.

Odwiedzającym rozdawano różnorodne materiały informacyjne przedstawiające działalność Inspektora, a także różne upominki promocyjne (długopisy, naklejki, kubki, nośniki USB z logo Inspektora). Na miejscu zaproszono również do uczestniczenia w quizie na temat roli Inspektora i ochrony danych



Stoisko Inspektora w Parlamencie Europejskim podczas dnia otwartych drzwi UE (Bruksela, 7 czerwca 2008 r.)

na szczeblu Wspólnoty oraz umożliwiono wzięcie udziału w losowaniu nagród.

5.10. Priorytety na rok 2009

W roku 2009 działania informacyjne i komunikacyjne Inspektora skupią się na następujących priorytetach:

- **dalsze ulepszenie strony internetowej:** oprócz opublikowania nowych treści strona internetowa zostanie ulepszona pod względem technicznym i graficznym, aby ułatwić nawigację, sprawić, by zawartość była atrakcyjniejsza wizualnie oraz zapewnić lepszą widoczność i natychmiastowy dostęp do wiadomości; trzeba będzie również uaktualnić odpowiednie fragmenty strony internetowej w następstwie mianowania Inspektora i jego zastępcy na następną kadencję (2009–14);
- **doprowadzenie do końca udoskonalenia biuletynu** w celu zapewnienia czytelnikom nowoczesnego i przyjaznego narzędzia informacji;
- **ostateczne zredagowanie nowej broszury informacyjnej** dotyczącej Inspektora i ochrony danych osobowych w instytucjach i organach Wspólnoty;
- **dalsze sprecyzowanie kompetencji Inspektora:** wśród obywateli, którzy słyszeli o Inspektorze, jest wiele osób, które nie całkiem znają jego kompetencje i mają tendencję do postrzegania tego urzędu jako europejskiego organu koordynacyjnego w zakresie ochrony danych, do którego można się zwrócić przy napotkaniu problemów na szczeblu krajowym; należy odpowiednio sprostować to nieporozumienie; jednym z pierwszych kroków będzie lepsze sprecyzowanie roli Inspektora w nowej broszurze informacyjnej oraz na stronie internetowej, w szczególności w sekcji „Pytania i odpowiedzi”.
- **usprawnienie polityki prasowej Inspektora,** w szczególności jeżeli chodzi o publikowanie komunikatów prasowych oraz rozpatrywanie wniosków o udzielenie informacji, wywiadów, komentarzy itd. składanych przez media; zostaną zredagowane wewnętrzne wytyczne dotyczące publikowania komunikatów prasowych; zostanie również sprecyzowany sposób rozpatrywania przez Inspektora wniosków składanych przez prasę, aby wyraźnie ustalić jak i za pośrednictwem jakiego kanału (-ów) powinny one docierać.

6. Administracja, budżet i personel

6.1. Wprowadzenie

Aby dalej kontynuować pomyślnie rozpoczętą działalność i – w związku z tym – wypełniać przydzielone mu nowe zadania, Inspektor uzyskał dodatkowe zasoby zarówno budżetowe (wzrost z 4 955 726 EUR w 2007 roku do 5 307 753 w 2008 roku), jak i osobowe (wzrost z 29 do 33 pracowników).

Otoczenie administracyjne jest stopniowo rozszerzane zgodnie z priorytetami ustalonymi na dany rok z uwzględnieniem potrzeb i rozmiarów instytucji. Inspektor przyjął nowe przepisy wewnętrzne⁽⁶⁸⁾ niezbędne do prawidłowego funkcjonowania instytucji. Komitet pracowniczy ściśle angażuje się w proces przyjmowania przez EIOD ogólnych przepisów wykonawczych dotyczących regulaminu pracowniczego oraz innych przepisów wewnętrznych.

Współpraca z innymi instytucjami – Parlamentem Europejskim, Radą i Komisją Europejską – uległa dalszej poprawie, co pozwoliło uzyskać znaczne korzyści skali.



Dział ds. personelu, budżetu i administracji

⁽⁶⁸⁾ W załączniku I znajduje się wykaz umów i decyzji administracyjnych.

6.2. Budżet

Budżet przyjęty przez władzę budżetową na rok 2008 wynosił 5 307 753 EUR. Stanowi to wzrost o 7,1% w porównaniu z budżetem na 2007 rok.

W odniesieniu do budżetu w 2008 roku zastosowano nową terminologię budżetową. Opiera się ona na doświadczeniu Inspektora z okresu kilku lat dotychczasowej działalności, uwzględnia szczególne potrzeby tej instytucji oraz zapewnia przejrzystość wymaganą przez władzę budżetową.

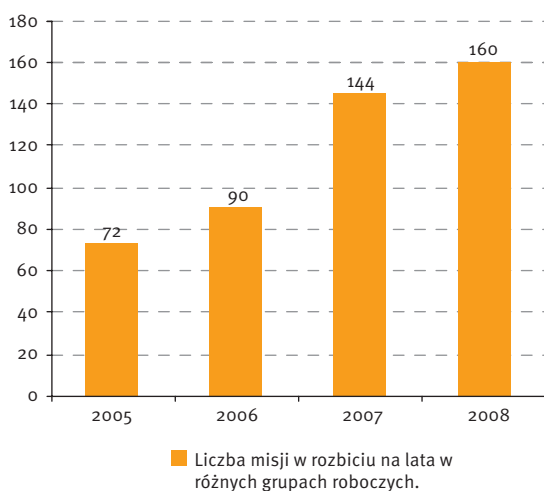
W odniesieniu do wykonania swojego budżetu Inspektor stosuje przepisy wewnętrzne Komisji w stopniu, w jakim przepisy te mają zastosowanie do struktury i skali jego instytucji, i w przypadku braku przepisów szczegółowych. Wraz z przyjęciem nowej decyzji, która uwzględnia wzrastające ilości dokumentów finansowych osiągnięto znaczną poprawę, jeśli chodzi o konstruowanie i składanie tych dokumentów. Wykorzystanie nowej terminologii budżetowej gwarantuje przejrzystość i łatwość obsługi.

Usprawniono kilka wewnętrznych procesów obsługi, aby dostosować instytucję do stale zwiększającej się liczby dokumentów finansowych.

Komisja nadal udzielała Inspektorowi wsparcia, zwłaszcza w zakresie rachunkowości; księgowy Komisji został bowiem mianowany także księgowym EIOD.

W swoim sprawozdaniu za rok budżetowy 2007 Europejski Trybunał Obrachunkowy stwierdził po przeprowadzeniu kontroli, że nie ma żadnych uwag.

Istotną część budżetu dotyczy tłumaczeń pisemnych. Opinie Inspektora na temat wniosków prawodawczych tłumaczone są na 23 języki urzędowe UE. Opinie te publikowane są w *Dzienniku*



Rozwój liczby misji

Urzędowym Unii Europejskiej. Od 2005 roku liczba opinii, podobnie jak liczba innych dokumentów do tłumaczenia, stale wzrasta. Opinie na temat kontroli wstępnych i inne publikowane dokumenty tłumaczone są zwykle tylko na języki robocze Inspektora.

Liczba misji z udziałem członków i personelu Inspektora wzrosła dwukrotnie od 2005 roku. Jest to logiczną konsekwencją intensywniejszych działań tej instytucji. Zespół administracyjny Inspektora zarządza stroną finansową misji; pomocy udziela mu Biuro Administracji i Rozliczania Należności Indywidualnych (PMO).

6.3. Zasoby ludzkie

Jeśli chodzi o zadania w zakresie zarządzania personelem Inspektora (składającym się z dwóch osób mianowanych i 33 pracowników), instytucja ta korzysta ze skutecznej pomocy służb Komisji.

6.3.1. Rekrutacja

Rosnąca widoczność działalności Inspektora oznacza dla niego większe obciążenie pracą, a także poszerzenie zakresu zadań. Na kwestię znacznego wzrostu obciążenia pracą w 2008 roku zwrócono uwagę w poprzednich rozdziałach. W tym kontekście bardzo istotne znaczenie mają oczywiście zasoby ludzkie.

Inspektor postanowił jednak ograniczyć rozszerzanie zakresu zadań i zwiększanie liczebności personelu, stosując wzrost kontrolowany, tak by nowi pracownicy zostali w pełni wdrożeni do pracy i odpowiednio wyszkoleni oraz by mogli

się odpowiednio zintegrować z zespołem. Dlatego też w 2008 roku Inspektor postulował utworzenie tylko czterech stanowisk (trzy stanowiska administratorów i jedno stanowisko asystenta). Wniosek dotyczący zwiększenia liczby personelu z 29 w 2007 roku do 33 w 2008 roku został zatwierdzony przez władzę budżetową. Na początku 2008 roku opublikowano ogłoszenia o naborze i w ciągu roku wszystkie stanowiska zostały obsadzone.

Cenna była pomoc Komisji w tym względzie, zwłaszcza udzielona przez Biuro Administracji i Rozliczania Należności Indywidualnych (PMO) oraz służbę medyczną.

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

6.3.2. Program stażowy

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

Zasadniczy program obejmuje dwa pięcioletnie okresy stażu rocznie (od marca do lipca oraz od października do lutego); w każdym okresie uczestniczy średnio dwoje stażystów. Staże te przynoszą nader pozytywne rezultaty.

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

Wszyscy stażyści, odbywający staże płatne i bezpłatne, uczestniczyli zarówno w pracach teoretycznych, jak i praktycznych, zdobywając doświadczenie z pierwszej ręki.

Na podstawie porozumienia o gwarantowanym poziomie usług podpisanego w 2005 roku Inspektor korzysta z pomocy administracyjnej Biura ds. Staży Dyrekcji Generalnej ds. Edukacji i Kultury w Komisji, które udziela mu stale cennego wsparcia dzięki bogatemu doświadczeniu swoich pracowników. We wrześniu 2008 roku podpisano nowe porozumienie o gwarantowanym poziomie usług, co ulepszyło wiele praktyk administracyjnych, w szczególności płatność dotacji oraz inne zagadnienia finansowe.

6.3.3. Program dla oddelegowanych ekspertów krajowych

Realizacja programu dla oddelegowanych ekspertów krajowych rozpoczęła się w styczniu 2006 roku po ustanowieniu jesienią 2005 roku jego podstaw prawnych i organizacyjnych⁽⁶⁹⁾.

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

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

W 2008 roku oddelegowano dwóch ekspertów krajowych: jeden pochodził z hiszpańskiego organu ds. ochrony danych a drugi z greckiego organu ds. ochrony danych; zastąpili oni poprzednich ekspertów krajowych – brytyjskiego i węgierskiego.

6.3.4. Struktura organizacyjna

Od 2004 roku struktura organizacyjna EIOD nie uległa zmianie: jedna sekcja – licząca obecnie 8 osób – jest odpowiedzialna za administrację, personel i budżet; pozostałych 25 pracowników zajmuje się operacyjną stroną zadań związanych z ochroną danych. Pracują oni pod bezpośrednim zwierzchnictwem Inspektora lub jego zastępcy w dwóch głównych dziedzinach: zajmują się mianowicie nadzorem i konsultacjami. Wzrastające obciążenie pracą było impulsem do stworzenia nowej funkcji koordynatora. W tym celu wyznaczono ośmiu koordynatorów w zespołach odpowiedzialnych za konsultacje i za nadzór, natomiast rzecznik prasowy koordynuje niewielki zespół ds. informacji.

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

6.3.5. Dialog społeczny

Zgodnie z art. 9 regulaminu pracowniczego urzędników Wspólnot Europejskich w dniu 8 lutego 2006 r. Inspektor przyjął decyzję w sprawie utworzenia komitetu pracowniczego. Konsultacje prowadzone z tym komitetem obejmują szereg ogólnych przepisów wykonawczych dotyczących regulaminu pracowniczego oraz innych przepisów wewnętrznych przyjmowanych przez Inspektora. W 2008 roku komitet pracowniczy zorganizował dla personelu pozabiurowe działania w sferze socjalnej.

6.3.6. Szkolenia

W roku 2008 kontynuowano proces rozszerzania i udoskonalania wiedzy, kompetencji i postaw pracowników, tak by każdy z nich mógł optymalnie przyczynić się do realizacji celów instytucji. Zgodnie z wewnętrzną decyzją dotyczącą szkoleń opracowano plan szkolenia w oparciu i potrzeby personelu określone na podstawie ankiety przeprowadzonej wśród pracowników.

Określone w ogólnych kierunkach główne obszary uczenia się, załączone do wewnętrznej decyzji dotyczącej szkoleń, stały się priorytetami w 2008 roku. Obejmowały one obowiązkowe szkolenia dla nowych pracowników, niezbędne szkolenia dla potrzeb konkretnych funkcji oraz kursy językowe.

Zgodnie z celem, by pracownikom Inspektora zapewnić doskonałe umiejętności w dziedzinie ochrony danych, umożliwiono im uczestniczenie

⁽⁶⁹⁾ Decyzja EIOD z 10 listopada 2005 r.

w profesjonalnych szkoleniach zewnętrznych z zakresu bezpieczeństwa informacji. Zachęcano również do udziału w seminariach i sesjach informacyjnych z dziedziny ochrony danych.

Aby przyzwyczaić nowych pracowników do samodzielnej pracy i umożliwić ich rozwój osobisty i zawodowy wdrożono – oprócz ustanowionego już wcześniej dnia informacyjnego – program opieki nad nowymi pracownikami przez mentorów.

Personel Inspektora korzysta z kursów szkoleniowych organizowanych przez inne instytucje europejskie (mianowicie Komisję Europejską i Parlament Europejski) oraz organy międzyinstytucjonalne (Europejską Szkołę Administracji – EAS).

Inspektor nadal uczestniczył w pracach komitetów międzyinstytucjonalnych (międzyinstytucjonalna grupa robocza EAS, międzyinstytucjonalny komitet ds. szkoleń językowych, itd.); celem było dzielenie się wspólnym podejściem w sektorze, w którym instytucje mają zasadniczo podobne potrzeby, oraz umożliwienie korzyści skali.

W 2008 roku EIOD wraz z innymi instytucjami podpisał nowy protokół w sprawie harmonizacji kosztów międzyinstytucjonalnych kursów językowych.

6.3.7. Działania socjalne

Zaplanowano zorganizowanie dnia informacyjnego dla nowo zatrudnionych współpracowników. W dniu tym Inspektor i jego zastępca osobiście witają wszystkich nowych pracowników. Pracownicy ci spotykają się ze swoim mentorem, a także z członkami działu administracyjnego; udzielają im oni informacji na temat specyficznych cech instytucji oraz przekazują przewodnik administracyjny Inspektora. Inspektor chce doprowadzić do podpisania umowy o współpracy z Komisją w celu ułatwienia integracji nowych współpracowników i ich aklimatyzacji, np. przez zapewnienie im porad prawnych w zakresie spraw prywatnych (kontraktów związanych z wynajęciem mieszkania, kupnem domu itd.).

Inspektor bierze udział – w charakterze obserwatora – w obradach komitetu doradczego Parlamentu Europejskiego ds. bezpieczeństwa i ochrony w miejscu pracy; ma to na celu polepszenie otoczenia pracy – rozpoczęto analizę kwestii dobrego samopoczucia w pracy.

Inspektor nadal rozwijał współpracę międzyinstytucjonalną w zakresie zaplecza socjalnego:

dzieci pracowników Inspektora mogą korzystać ze żłobków, pozaszkolnej opieki nad dziećmi oraz rekreacyjnych ośrodków opieki nad dziećmi będących w gestii Komisji, mają także możliwość nauki w szkołach europejskich. Mogą też brać udział w mikołajkach organizowanych w Parlamencie Europejskim.

6.3.8. Protokół w sprawie przywilejów i immunitetów Wspólnot Europejskich

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

6.4. Funkcje kontrolne

6.4.1. Kontrola wewnętrzna

Ocena ryzyka i wdrożenie systemu kontroli wewnętrznej

Ocena ryzyka w odniesieniu do działań Inspektora pozostaje wciąż we wczesnym stadium. Inspektor zamierza poczynić postępy w tej dziedzinie, tak by utrzymać ryzyko dla swojej instytucji na minimalnym poziomie.

Inspektor przyjął wcześniej konkretne procedury kontroli wewnętrznej, które uznano za najbardziej odpowiadające potrzebom tej instytucji ze względu na jej rozmiar i prowadzone przez nią działania. Ma to na celu zapewnienie kierownictwu i personelowi wystarczającej pewności odnośnie do realizacji celów instytucji oraz zarządzania ryzykiem, które wiąże się z jego działalnością.

Wewnętrzna ocena warunków kontroli wewnętrznej

Podczas oceny przeprowadzonej przez służby Inspektora wykazano, że system kontroli wewnętrznej funkcjonuje prawidłowo i efektywnie, a także sformułowano pewne zalecenia w odniesieniu do przyszłych usprawnień. Realizacja tych zaleceń była priorytetem w roku 2008. Wewnętrzne sprawozdanie dotyczące kontroli wewnętrznych wykazało wysoki stopień realizacji zaleceń kontroli wewnętrznej (80%).

Roczne sprawozdanie z działalności i poświadczenie wiarygodności

Inspektor przyjął do wiadomości roczne sprawozdanie z działalności wraz z poświadczeniem wiarygodności podpisanym przez oddelegowanego urzędnika zatwierdzającego. Ogólnie rzecz biorąc, obecne systemy kontroli wewnętrznej zapewniają, zdaniem Inspektora, wystarczającą pewność co do legalności i prawidłowości operacji, za które instytucja ta odpowiada.

Inspektor będzie dbać o to, by oddelegowany urzędnik zatwierdzający kontynuował działania na rzecz zagwarantowania wystarczającej pewności, że oświadczenie załączone do sprawozdania rocznego faktycznie opiera się na odpowiednich systemach kontroli wewnętrznej.

6.4.2. Audyt wewnętrzny

Na mocy porozumienia o współpracy administracyjnej z 2004 roku przedłużonego w roku 2006 na audytora EIOD wyznaczono wewnętrznego audytora Komisji. W związku z tym w roku 2006 przeprowadzono pierwszy audyt, a we wrześniu 2007 roku otrzymano sprawozdanie z pierwszego audytu sporządzone przez służbę audytu wewnętrznego (IAS). Potwierdziło ono zdolność systemu kontroli wewnętrznej EIOD do zagwarantowania wystarczającej pewności odnośnie do realizacji celów tej instytucji. W procesie oceny wskazano jednak pewne aspekty, w których wymagana jest poprawa. W niektórych z tych przypadków podjęto natychmiastowe działania, a inne działania będą podejmowane stopniowo w przyszłości w miarę ewoluowania zadań powierzonych Inspektorowi.

Na podstawie planu działania sporządzonego w początkach 2008 roku podjęto realizację zaleceń IAS uzgodnionych przez Inspektora.

W grudniu 2008 roku IAS przeprowadził audyt uzupełniający. Nie otrzymano jeszcze sprawozdania z tego audytu.

6.4.3. Bezpieczeństwo

Mając na uwadze stopień poufności wymagany w niektórych dziedzinach jego działalności, Inspektor przyjął w 2008 roku decyzję w sprawie środków bezpieczeństwa mających zastosowanie w tej instytucji. Decyzja określa podstawowe zasady i minimalne normy bezpieczeństwa, które mają być we właściwy sposób przestrzegane przez wszystkich pracowników. Ta kompleksowa decyzja obejmuje

środki dotyczące zarządzania poufnością informacji, bezpieczeństwa teleinformatycznego, a także warunków bezpieczeństwa osób i pomieszczeń.

6.4.4. Inspektor ochrony danych

W 2008 roku kontynuowano proces wskazywania operacji, podczas których przetwarzane są dane osobowe, oraz ustalenia, które z tych operacji podlegają kontroli wstępnej. Ukończono spis operacji wewnętrznych. Spis ten jest praktycznym narzędziem mającym na celu ukierunkowanie procedury powiadamiania. Inspektor ze względu na swoją szczególną sytuację opracował uproszczoną procedurę powiadamiania mającą zastosowanie w przypadku spraw podlegających kontroli wstępnej.

Na tej podstawie w roku 2008 rozpoczęto pierwszą procedurę powiadamiania. Zredagowano ponadto różne oświadczenia o ochronie danych osobowych (komunikaty dla personelu), w których zamieszczono informacje zawarte w art. 11 i 12 rozporządzenia (WE) No 45/2001.

Aby umożliwić osobom, których dane dotyczą, korzystanie z ich praw, stworzono w tym celu specjalny adres poczty elektronicznej.

Uczestniczenie w spotkaniach sieci inspektorów ochrony danych umożliwiło wymianę wspólnych doświadczeń oraz omówienie kwestii horyzontalnych.

6.5. Infrastruktura

Zgodnie z porozumieniem o współpracy administracyjnej siedziba Inspektora znajduje się w budynku należącym do Parlamentu Europejskiego, który ponadto wspiera Inspektora głównie w zakresie infrastruktury informatycznej i telefonicznej. Inspektor pomieścił wszystkich nowych pracowników, dostosowując przestrzeń roboczą. W roku 2008 osiągnięto w wyniku tych działań optymalne pełne wykorzystanie przyznanej przestrzeni biurowej.

Inspektor nadal samodzielnie zarządzał zasobami umeblovania i sprzętu informatycznego przy wsparciu ze strony służb Parlamentu Europejskiego.

6.6. Otoczenie administracyjne

6.6.1. Pomoc administracyjna i współpraca międzyinstytucjonalna

Inspektor korzysta ze współpracy międzyinstytucjonalnej w zakresie wielu zagadnień dotyczących

administracji na mocy porozumienia o współpracy administracyjnej zawartego z sekretarzami generalnymi Komisji, Parlamentu Europejskiego i Rady w 2004 roku i przedłużonego w 2006 roku na okres trzech lat. Współpraca ta ma istotne znaczenie dla Inspektora i jego działań ze względu na zwiększenie wydajności i uzyskanie korzyści skali. Pozwala również uniknąć mnożenia infrastruktur administracyjnych oraz ograniczyć jałowe wydatki administracyjne, a jednocześnie zapewnia administrację usługami publicznymi na wysokim poziomie.

Na tej podstawie kontynuowano w 2008 roku współpracę międzyinstytucjonalną z różnymi dyrekcjami generalnymi Komisji (ds. Personelu i Administracji; Budżetu; Służbą Audytu Wewnętrznego; Dyrekcją ds. Edukacji i Kultury), Biurem Administracji i Rozliczania Należności Indywidualnych, z różnymi służbami Parlamentu Europejskiego (służbami ds. technologii informacyjnych – w szczególności w związku z pracami nad nową wersją strony internetowej Inspektora; również w zakresie wyposażania pomieszczeń, ochrony budynków, druku, poczty, sprzętu telefonicznego, zaopatrzenia, itd.) oraz z Radą (w zakresie prac translatorskich).

Porozumienia o gwarantowanym poziomie usług podpisane na początku działalności z różnymi instytucjami i ich wydziałami są regularnie aktualizowane. We wrześniu 2008 roku Inspektor podpisał nowe porozumienie o gwarantowanym poziomie usług ze służbą medyczną Komisji.

Inspektor podpisał ponadto porozumienie o przekazaniu Biuru Administracji i Rozliczania Należności Indywidualnych (PMO) uprawnień w odniesieniu do bieżących działań odnoszących się do zarządzania prawami emerytalnymi. Przygotowywane są umowy obejmujące nowe dziedziny.

Uzyskano bezpośredni dostęp z siedziby Inspektora do niektórych aplikacji Komisji służących do zarządzania finansami; ma to ułatwić współpracę pomiędzy wydziałami Komisji a Inspektorem oraz usprawnić wymianę informacji pomiędzy służbami.

W roku 2008 zakończono opracowywanie – we współpracy z odpowiednimi służbami Parlamentu Europejskiego – nowej wersji strony internetowej Inspektora. Jednak uruchomienie dalszych, już opracowanych funkcji internetowych spowodowały pewne problemy związane z konkretnym oprogramowaniem wybranym do realizacji. Inspektor ma nadzieję, że w ciągu 2009 roku projekt zostanie zakończony.

W 2008 roku nadal uczestniczono w międzyinstytucjonalnych zaproszeniach do składania ofert dotyczących kursów ogólnych i kursów językowych, ubezpieczeń i dostawy meblowania, co pozwoliło Inspektorowi zwiększyć wydajność w wielu dziedzinach administracji i poczynić postępy na drodze do większej niezależności. Jeśli chodzi o dostawę materiałów biurowych, Inspektor uczestniczył w zorganizowanym przez Parlament Europejski przetargu.

Inspektor nadal brał udział w pracach różnych międzyinstytucjonalnych komitetów. Szczególnie aktywnie uczestniczył w pracach *Comité de Gestion Assurances maladies* (CGAM), *Comité de Préparation pour les Questions Statutaires* (CPQS) oraz *Comité du Statut*, w których to organach Inspektor jest reprezentowany w różnych grupach roboczych. Jednak ze względu na niewielki rozmiar instytucji, udział taki musiał się ograniczyć do prac tylko kilku komitetów. Uczestnictwo w działalności tych komitetów sprawiło, że Inspektor stał się bardziej widoczny dla innych instytucji, a także pobudziło stałą wymianę informacji i dobrych wzorców.

6.6.2. Przepisy wewnętrzne

Kontynuowano proces przyjmowania nowych przepisów wewnętrznych niezbędnych do prawidłowego funkcjonowania instytucji, a także nowych ogólnych przepisów wykonawczych dotyczących regulaminu pracowniczego (zob. załącznik I).

W przypadku gdy przepisy te odnoszą się do dziedzin, w których Inspektor korzysta ze wsparcia Komisji, są one podobne do przepisów Komisji, jednak zostały dostosowane w sposób uwzględniający charakter biura Inspektora. Nowo zatrudnieni pracownicy otrzymują na powitanie przewodnik administracyjny zawierający wszystkie przepisy wewnętrzne Inspektora oraz informacje o szczególnych cechach tej instytucji. Dokument ten jest regularnie aktualizowany.

W 2008 roku przyjęto pięć ważnych decyzji wewnętrznych:

- Przepisy z dnia 16 czerwca 2008 r. dotyczące zwrotu wydatków ponoszonych przez osoby spoza służb Inspektora zaproszone do uczestniczenia w posiedzeniach w charakterze ekspertów;
- Decyzja oddelegowanego urzędnika zatwierdzającego z dnia 8 sierpnia 2008 r. dotycząca archiwizacji dokumentów finansowych i dokumentów uzupełniających;

- Decyzja Inspektora z dnia 2 października 2008 r. dotycząca ogólnych zasad wykonawczych art. 45a regulaminu pracowniczego (certyfikacja);
- Decyzja Inspektora z dnia 16 grudnia 2008 r. w sprawie przyjęcia środków bezpieczeństwa w biurze Inspektora;
- Decyzja Inspektora z dnia 19 grudnia 2008 r. w sprawie mianowania wewnętrznego urzędnika ds. bezpieczeństwa w biurze Inspektora.

Biuro Inspektora jest stosunkowo młodą instytucją, lecz szybko się rozwija. W związku z tym przepisy i procedury, które były właściwe w pierwszych latach działalności mogą okazać się mniej skuteczne w przyszłości przy większej i bardziej złożonej strukturze. Dlatego też obecne przepisy zostaną ocenione dwa lata po ich przyjęciu; mogą zatem ulec odpowiedniej zmianie.

6.6.3. Zarządzanie dokumentami

Pomimo pewnego opóźnienia powstałego na skutek niespodziewanych trudności trwa wdrażanie nowego systemu zarządzania pocztą elektroniczną (GEDA); powinno się ono zakończyć w roku 2009 i jest wspierane przez służby Parlamentu Europejskiego. Ma to być pierwszy krok na drodze do stworzenia systemu zarządzania przepływem spraw, który lepiej wesprze działania Inspektora.

6.7. Cele na rok 2009

Cele ustalone na rok 2008 zostały w pełni osiągnięte. W 2009 roku Inspektor będzie kontynuował rozpoczętą wcześniej konsolidację oraz pogłębiał niektóre aspekty swojej działalności.

Inspektor będzie kontynuował przyjmowanie nowych wewnętrznych zasad finansowych dostosowanych do wielkości instytucji. Jeśli chodzi o oprogramowanie finansowe, Inspektor będzie kontynuował działania w celu nabycia narzędzi umożliwiających mu dostęp do danych finansowych ze swojej siedziby.

Bardzo istotna dla Inspektora będzie dalsza współpraca administracyjna oparta na przedłużonym

porozumieniu administracyjnym. Inspektor zamierza podpisać z Komisją (Adminfo) porozumienie o współpracy, aby ułatwić integrację nowych współpracowników i ich aklimatyzację. Jednocześnie Inspektor będzie nadal pracował nad rozwojem otoczenia administracyjnego i przyjmował ogólne przepisy wykonawcze dotyczące regulaminu pracowniczego.

Inspektor zamierza zainicjować ogólny konkurs w dziedzinie ochrony danych organizowany wraz z Europejskim Urzędem Doboru Kadr (EPSO), aby pozyskać wysoko wykwalifikowanych pracowników.

Jeśli chodzi o oprogramowanie do zarządzania zasobami ludzkimi (głównie delegacjami: MIPs oraz urlopami i szkoleniami: Syslog), Inspektor również podejmie wszelkie niezbędne działania w celu nabycia programów umożliwiających mu dostęp do danych ze swojej siedziby.

Inspektor planuje przeprowadzenie gruntownej oceny ryzyka, aby oszacować, czy istniejące normy kontroli wewnętrznej odpowiadają aktualnym wzorcom działania instytucji.

Wprowadzanie ulepszeń określonych podczas oceny systemu kontroli wewnętrznej, a także zaleceń służby audytu wewnętrznego, będzie nadal uważane za ważny priorytet.

Inspektor ochrony danych będzie nadal czuwał nad stosowaniem przepisów rozporządzenia (WE) nr 45/2001 na poziomie wewnętrznym. Zostanie stworzony rejestr powiadomień.

Przyszli pracownicy będą potrzebować dodatkowej powierzchni biurowej. W 2009 roku Inspektor rozpocznie negocjacje ze służbami Parlamentu Europejskiego na temat przydzielenia wystarczającej powierzchni odpowiadającej jego przyszłym potrzebom.

Inspektor zamierza – z pomocą Parlamentu Europejskiego – ostatecznie zakończyć wdrażanie nowego systemu zarządzania pocztą elektroniczną i zakończyć tworzenie nowej strony internetowej.

Załącznik A

Ramy prawne

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

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

Informacje ogólne

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

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

Stosowne zasady, o których mowa w art. 286 Traktatu WE, zostały określone w rozporządzeniu (WE) nr 45/2001

Parlamentu Europejskiego i Rady o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych; rozporządzenie to weszło w życie w 2001 roku⁽⁷⁹⁾. Rozporządzenie to przewidywało również ustanowienie niezależnego organu kontrolnego zwanego „europejskim inspektorem ochrony danych”, któremu, zgodnie z Traktatem, postawiono konkretne zadania i nadano konkretne uprawnienia.

Traktat z Lizbony, podpisany w grudniu 2007 roku i podlegający ratyfikacji przez wszystkie państwa członkowskie, pod wieloma względami zwiększa 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 Unii Europejskiej, która obecnie jest wiążąca prawnie. Również art. 16 Traktatu o funkcjonowaniu UE zajmuje się ochroną danych jako jednym z tematów horyzontalnych. Wynika z tego jasno, że ochrona danych uważana jest za jeden z podstawowych elementów „dobrych rządów”. Niezależny nadzór jest zasadniczą częścią tej ochrony.

Rozporządzenie (WE) nr 45/2001

Przyglądając się uważniej temu rozporządzeniu, należy przede wszystkim odnotować, że ma ono zastosowanie do „przetwarzania danych osobowych przez instytucje i organy wspólnotowe, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu”. Oznacza to, że z zadań i uprawnień Inspektora w zakresie nadzoru wyłączone są jedynie te czynności, które znajdują się całkowicie poza obszarami wchodzącymi w skład „pierwszego filaru”.

Definicje zawarte w tym rozporządzeniu i jego zasadnicza treść są spójne z podejściem przyjętym w dyrektywie 95/46/WE. Można stwierdzić, że rozporządzenie (WE) nr 45/2001 stanowi wdrożenie tej dyrektywy na poziomie europejskim. Wynika stąd, że rozporządzenie to dotyczy ogólnych zasad, takich jak zgodne z prawem i rzetelne przetwarzanie, proporcjonalność i użycie zgodne z przyjętymi celami, szczególnie kategorie danych wrażliwych, informacje przekazywane osobie,

⁽⁷⁹⁾ Dz.U. L 8 z 12.1.2001, s. 1.

której dane dotyczą, prawa osoby, której dane dotyczą, obowiązki administratorów danych – uwzględniając w stosownych przypadkach szczególne okoliczności na poziomie UE – a także nadzór, stosowanie prawa i środki odwoławcze. Oddzielny rozdział dotyczy ochrony danych osobowych i prywatności w kontekście wewnętrznych sieci telekomunikacyjnych. Rozdział ten faktycznie wdraża na poziomie europejskim dyrektywę 97/66/WE o prywatności i łączności.

Interesującym aspektem tego rozporządzenia jest zobowiązanie instytucji i organów Wspólnoty do wyznaczenia co najmniej jednej osoby jako inspektora ochrony danych. Zadaniem tych inspektorów jest zapewnienie – w sposób niezależny – wewnętrznego stosowania przepisów rozporządzenia, w tym właściwego powiadamiania o operacjach przetwarzania. We wszystkich instytucjach i w większości organów Wspólnoty są obecnie tacy inspektorzy a niektórzy z nich działają już od kilku lat. Oznacza to, że w celu wdrożenia tego rozporządzenia wykonano istotną pracę pomimo braku organu nadzoru. Inspektorom tym może także być łatwiej doradzać lub interweniować na wczesnym etapie, jak również pomagać w wypracowywaniu sprawdzonych rozwiązań. Ponieważ formalnym obowiązkiem inspektora ochrony danych jest współpraca z EIOD, współdziałanie w ramach tej sieci współpracy i jej rozwój są bardzo istotne i wartościowe (zob. sekcja 2.2).

Zadania i uprawnienia Inspektora

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

Przedstawione zadania, obowiązki i uprawnienia są zasadniczo zbieżne z analogicznymi elementami działalności krajowych organów nadzoru i obejmują: wysłuchiwanie i badanie skarg, prowadzenie innych dochodzeń, informowanie administratorów danych i

podmiotów danych, przeprowadzanie kontroli wstępnych, jeżeli operacje przetwarzania obciążone są konkretnym ryzykiem, itp. Rozporządzenie to uprawnia Inspektora do uzyskania dostępu do stosownych informacji i pomieszczeń, w przypadku gdy jest to niezbędne dla prowadzonych dochodzeń. Inspektor może również nakładać kary i przekazać daną sprawę do rozpoznania Trybunałowi Sprawiedliwości. Te czynności nadzorcze zostały omówione bardziej wyczerpująco w rozdziale 2 niniejszego sprawozdania.

Niektóre zadania mają charakter specjalny. Zadanie polegające na doradztwie Komisji i innym instytucjom Wspólnoty w zakresie nowego prawodawstwa – uwydatnione w art. 28 ust. 2 przez nałożenie na Komisję formalnego obowiązku konsultowania się z Inspektorem w przypadku przyjmowania wniosku prawodawczego odnoszącego się do ochrony danych osobowych – dotyczy także projektów dyrektyw i innych środków, które mają mieć zastosowanie na poziomie krajowym lub mają być wdrażane do prawa krajowego. Jest to zadanie o znaczeniu strategicznym umożliwiające Inspektorowi analizę na wczesnym etapie wpływu na prywatność oraz omówienie wszelkich możliwych alternatywnych rozwiązań, również w ramach „trzeciego filaru” (współpracy policyjnej i sądowej w sprawach karnych). Istotnymi zadaniami są również: monitorowanie rozwoju sytuacji w stosownych dziedzinach w aspektach mogących mieć wpływ na ochronę danych osobowych oraz zabieranie głosu w sprawach rozpatrywanych przez Trybunał Sprawiedliwości. Te czynności konsultacyjne Inspektora omówiono obszerniej w rozdziale 3 niniejszego sprawozdania.

Obowiązek współpracy z krajowymi organami nadzoru oraz organami nadzoru działającymi w „trzecim filarze” ma podobny wpływ. Inspektor jest członkiem grupy roboczej art. 29 (grupy roboczej ds. ochrony danych) utworzonej w celu doradzania Komisji Europejskiej oraz opracowywania zharmonizowanych polityk, dzięki czemu może wносить na tym poziomie swój wkład. Współpraca z organami nadzoru działającymi w „trzecim filarze” umożliwia Inspektorowi śledzenie rozwoju sytuacji w tym zakresie, a także wnoszenie wkładu w opracowywanie bardziej spójnych i konsekwentnych ram ochrony danych osobowych, niezależnie od „filaru” lub konkretnego kontekstu. Współpracy tej poświęcono więcej miejsca w rozdziale 4 niniejszego sprawozdania.

Załącznik B

Wyciąg z rozporządzenia (WE) nr 45/2001

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 osobę, której dane dotyczą o wyniku w odpowiednim czasie;
- b) przeprowadza dochodzenia zarówno z własnej inicjatywy, jak i na podstawie skarg oraz informuje osoby, których dane dotyczą 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) 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 na mocy tytułu 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, ustanowionej na mocy 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) uchwała swój regulamin wewnętrzny.

Art. 47 – Uprawnienia

1. Europejski inspektor ochrony danych może:
 - a) doradzać osobom, których dane dotyczą w kwestii korzystania z ich praw;
 - b) przekazać sprawę administratorowi danych w przypadku domniemanego naruszenia przepisów rządzących przetwarzaniem danych osobowych i

- w miarę potrzeb zaproponować środki prawne dla usunięcia tego naruszenia i dla poprawy ochrony osób, których dane dotyczą;
- 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 danych 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 danych 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

7. PR	siódmy program ramowy w zakresie badań i rozwoju technologicznego
ARES	zaawansowany system rejestrów
B & R	badania i rozwój
CCL	wspólny wykaz przechowywanych dossier
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
CoA	Trybunał Obrachunkowy
CPCS	system współpracy w zakresie ochrony konsumentów
CPVO	Wspólnotowy Urząd Ochrony Odmian Roślin
CRS	komputerowy system rezerwacji
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
DG JLS	Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa
DIGIT	Dyrekcja Generalna ds. Informatyki
DPA	organ ds. ochrony danych
DPC	koordynator ds. ochrony danych (wyłącznie w Komisji Europejskiej)
DPO	inspektor ochrony danych
EBC	Europejski Bank Centralny
EBI	Europejski Bank Inwestycyjny
ECRIS	europejski system przekazywania informacji z rejestrów karnych
EFK	Europejska Fundacja Kształcenia
EFSA	Europejski Urząd ds. Bezpieczeństwa Żywności
EKES	Europejski Komitet Ekonomiczno-Społeczny
EKPC	europejska konwencja praw człowieka
EMCDDA	Europejskie Centrum Monitorowania Narkotyków i Narkomanii
EMEA	Europejska Agencja Leków
EMPL	Komisja Zatrudnienia i Spraw Socjalnych działająca w Parlamencie Europejskim
EMSA	Europejska Agencja ds. Bezpieczeństwa na Morzu
ENISA	Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji
EPSO	Europejski Urząd Doboru Kadr
ESA	Europejska Szkoła Administracji
ETO	Europejski Trybunał Obrachunkowy
ETS	Europejski Trybunał Sprawiedliwości

EU	Unia Europejska
EUMC	Europejskie Centrum Monitorowania Rasizmu i Ksenofobii
Eurofound	Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy
EWS	system wczesnego ostrzegania
FIDE	identyfikująca baza danych rejestru celnego
FRA	Agencja Praw Podstawowych Unii Europejskiej
IAS	służba audytu wewnętrznego
IGC	konferencja międzyrządowa
IMI	system wymiany informacji w ramach rynku wewnętrznego
IMS	usługa zarządzania tożsamością
JSB	wspólny organ nadzorczy
KR	Komitet Regionów
LIBE	Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych działająca w Parlamencie Europejskim
MoU	protokół ustaleń
NSA	Krajowa Władza Bezpieczeństwa
OECD	Organizacja Współpracy Gospodarczej i Rozwoju
OHC	Centrum Zdrowia w Miejscu Pracy
OLAF	Europejski Urząd ds. Zwalczenia Nadużyć Finansowych
PEP	osoba zajmująca eksponowane stanowisko polityczne
PMO	Urząd Administrowania i Wypłacania Należności Indywidualnych działający w Komisji Europejskiej
PNR	dane dotyczące przelotu pasażera
RFID	identyfikacja radiowa
SIS	system informacyjny Schengen
SWIFT	Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych
TIM	system zarządzania czasem
trzeci filar	współpraca policyjna i sądowa w sprawach karnych
UHRW	Urząd Harmonizacji Rynku Wewnętrznego
VIS	wizowy system informacyjny
WCB	Wspólne Centrum Badawcze
WE	Wspólnoty Europejskie
WP 29	grupa robocza art. 29
WPPJ	Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości

Załącznik D

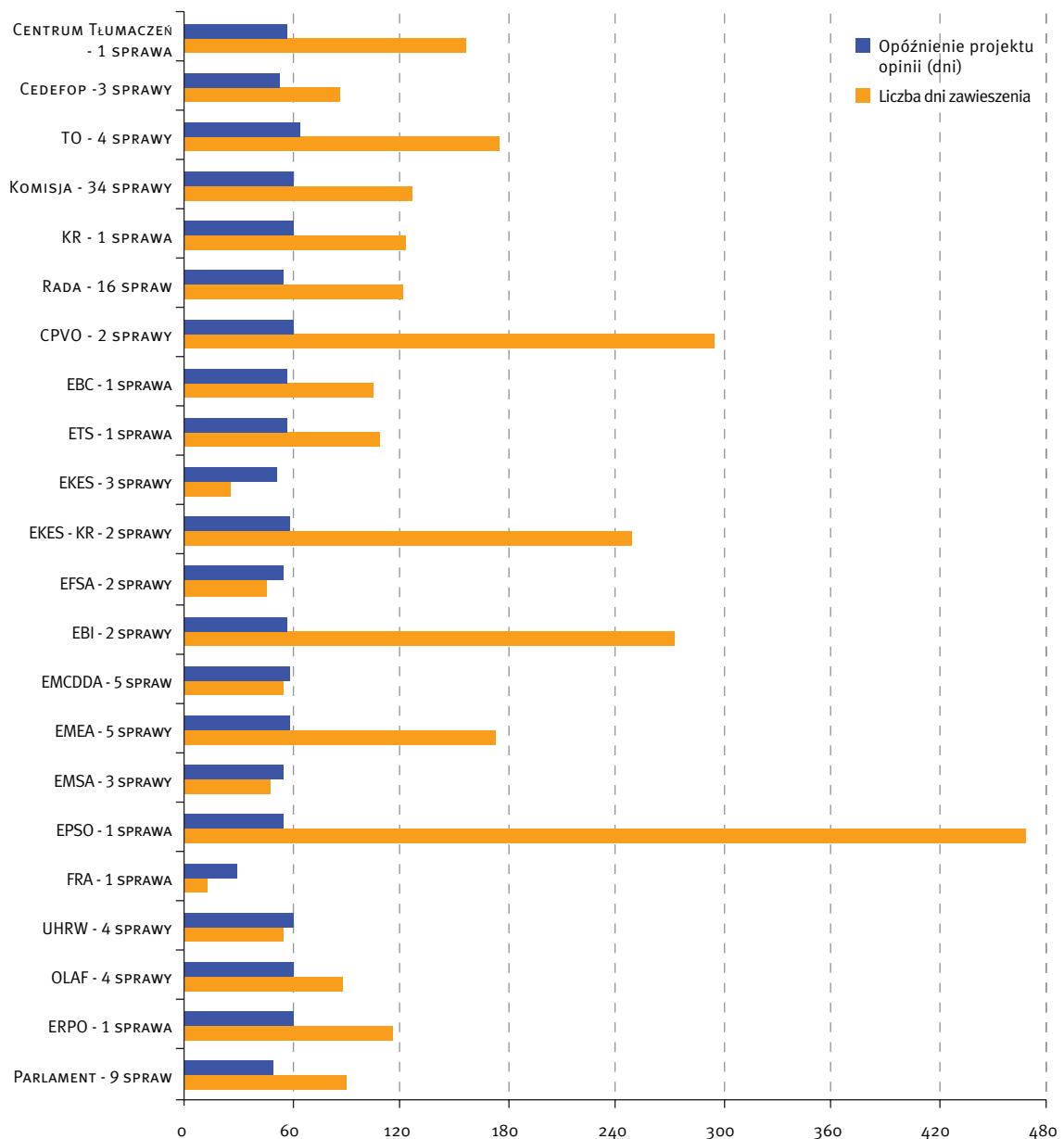
Lista inspektorów ochrony danych (DPO)

Organizacja	Imię i nazwisko	E-mail
Parlament Europejski	Jonathan STEELE	dg5data-protection@europarl.europa.eu
Rada Unii Europejskiej	Pierre VERNHES	data.protection@consilium.europa.eu
Komisja Europejska	Philippe RENAUDIÈRE	data-protection-officer@ec.europa.eu
Trybunał Sprawiedliwości Wspólnot Europejskich	Marc SCHAUSS	dataprotectionofficer@curia.europa.eu
Trybunał Obrachunkowy	Jan KILB	data-protection@eca.europa.eu
Europejski Komitet Ekonomiczno-Społeczny	Maria ARSENE	data.protection@eesc.europa.eu
Komitet Regionów	Petra CANDELLIER	data.protection@cor.europa.eu
Europejski Bank Inwestycyjny	Jean-Philippe MINNAERT	dataprotectionofficer@eib.org
Europejski Rzecznik Praw Obywatelskich	Loïc JULIEN	dpo-euro-ombudsman@ombudsman.europa.eu
Europejski Inspektor Ochrony Danych	Giuseppina LAURITANO	giuseppina.lauritano@edps.europa.eu
Europejski Bank Centralny	Martin BENISCH	DPO@ecb.int
Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF)	Laraine LAUDATI	laraine.laudati@ec.europa.eu
Centrum Tłumaczeń dla organów Unii Europejskiej	Benoît VITALE	data-protection@cdt.europa.eu
Urząd Harmonizacji Rynku Wewnętrznego (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 (EMA)	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)	Andreas MITRAKAS	dataprotection@enisa.europa.eu
Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy (Eurofund)	Markus GRIMMEISEN	mgr@eurofound.europa.eu
Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA)	Cécile MARTEL	cecile.martel@emcdda.europa.eu
Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA)	Claus REUNIS	dataprotectionofficer@efsa.europa.eu
Europejska Agencja ds. Bezpieczeństwa na Morzu (EMSA)	Małgorzata NESTEROWICZ	malgorzata.nesterowicz@emsa.europa.eu
Europejska Agencja Odbudowy (EAR)	Richard LUNDGREN	richard.lundgren@ear.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	hubert.monet@ec.europa.eu
Europejska Agencja ds. Bezpieczeństwa i Ochrony Zdrowia w Miejscu Pracy (OSHA)	Terry TAYLOR	taylor@osha.europa.eu
Wspólnotowa Agencja Kontroli Rybołówstwa (CFCA)	Rieke ARNDT	rieke.arndt@cfca.europa.eu

Organizacja	Imię i nazwisko	E-mail
Organ Nadzoru Europejskiego GNSS	Christina TSALI	christina.tsali@gsa.europa.eu
Europejska Agencja Kolejowa (ERA)	Zografia PYLORIDOU	zograpia.pyloridou@era.europa.eu
Agencja Wykonawcza ds. Zdrowia i Konsumentów (PHEA)	Eva LÄTTI	eva.latti@ec.europa.eu
Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC)	Elisabeth ROBINO	elisabeth.robino@ecdc.europa.eu
Europejska Agencja Ochrony Środowiska (EAA)	Gordon McINNES	gordon.mcinnnes@eea.europa.eu
Europejski Fundusz Inwestycyjny (EIF)	Jobst NEUSS	j.neuss@eif.org
Europejska Agencja Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych (Frontex)	Sakari VUORENSOLA	sakari.vuorensola@frontex.europa.eu
Europejska Agencja Bezpieczeństwa Lotniczego (EASA)	Arthur BECKAND	arthur.beckand@easa.europa.eu
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@ext.ec.europa.eu
Europejska Agencja Chemikaliów (ECHA)	Minna HEIKKILA	minna.heikkila@echa.europa.eu

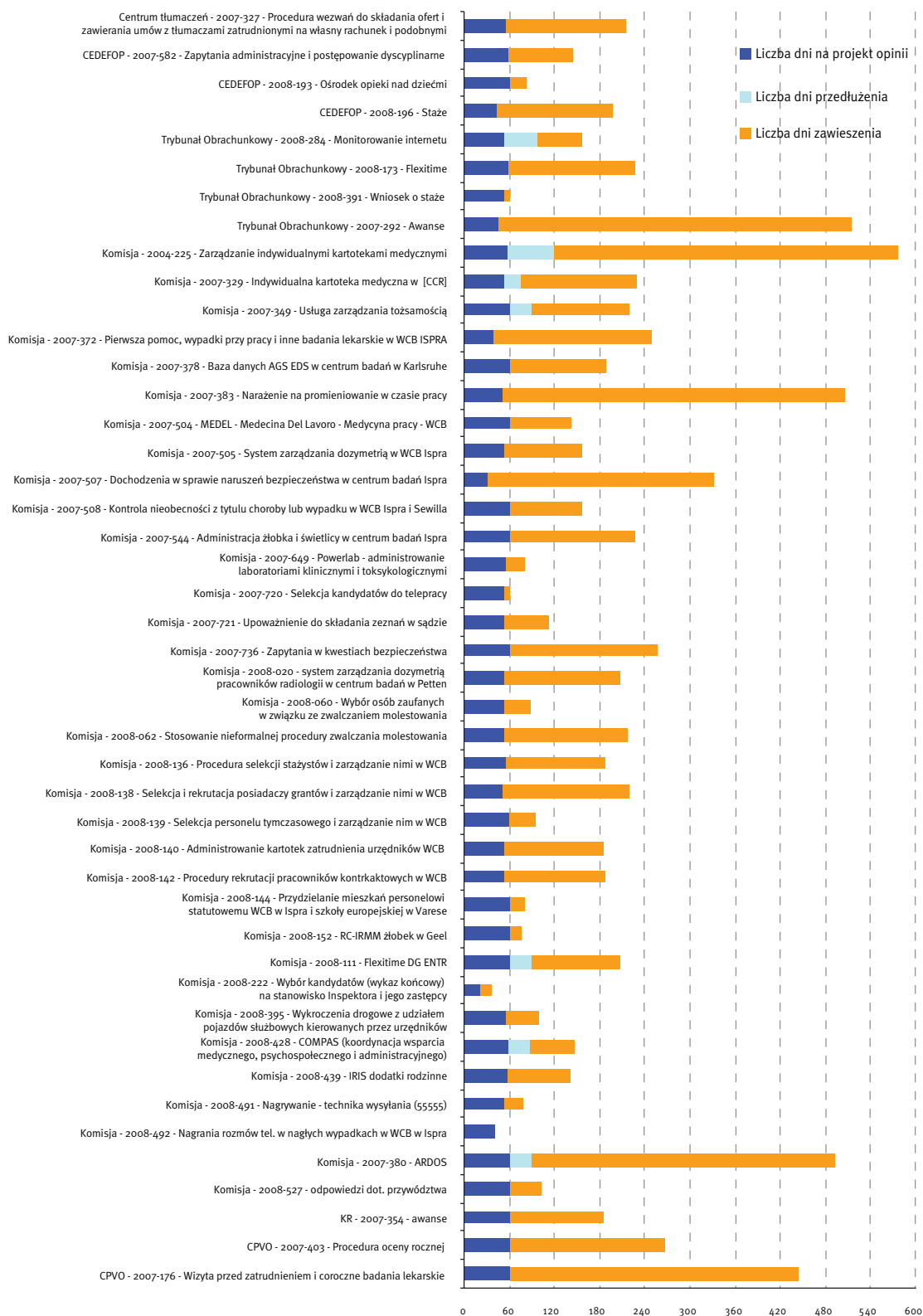
Załącznik E

Czas trwania kontroli wstępnej w poszczególnych sprawach i instytucjach

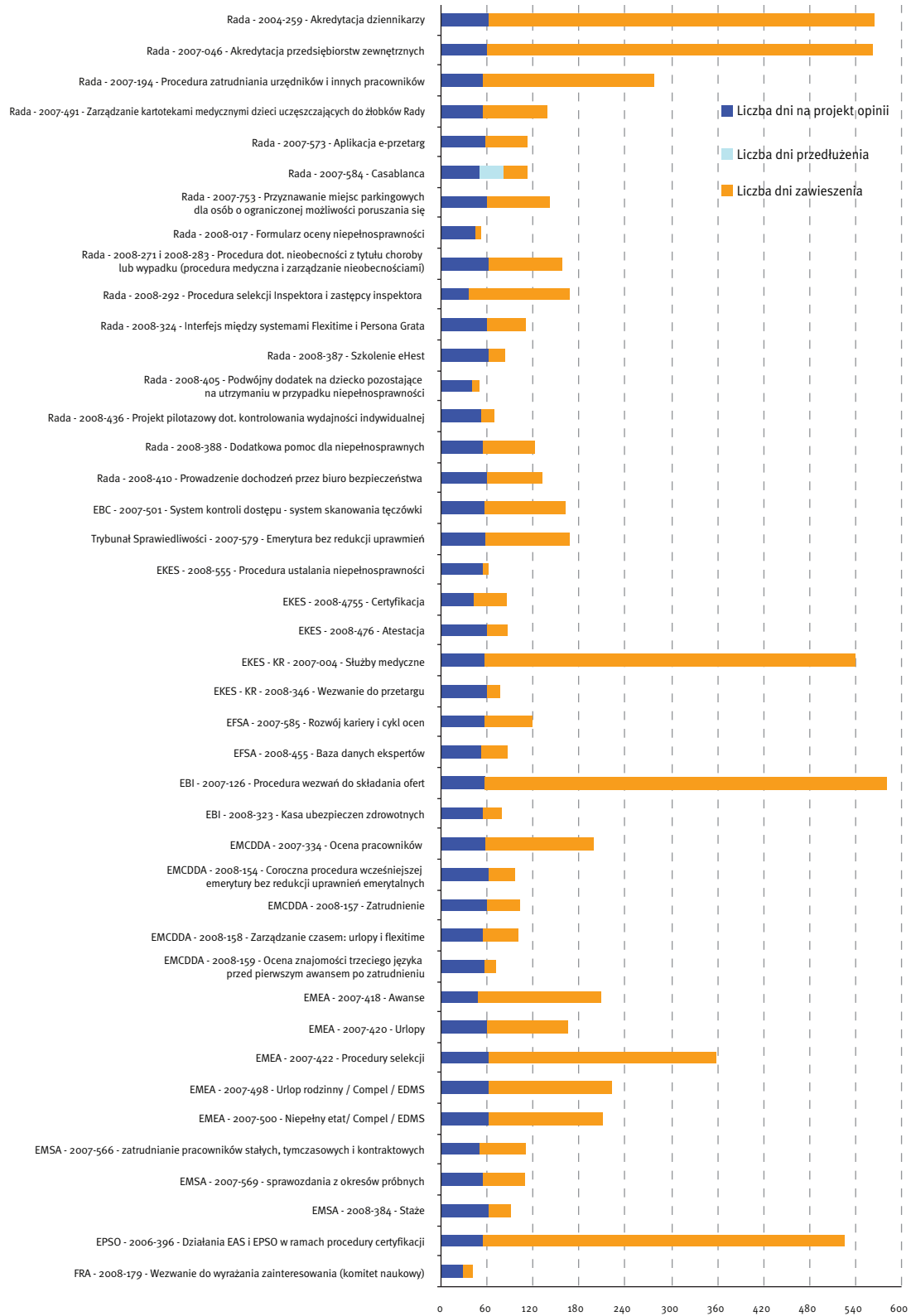


NB: Delays for the draft opinions do not include the month of August in ex-post cases received before 1/09/08. Suspension days include the suspension for comments on the draft, normally 7 to 10 days.

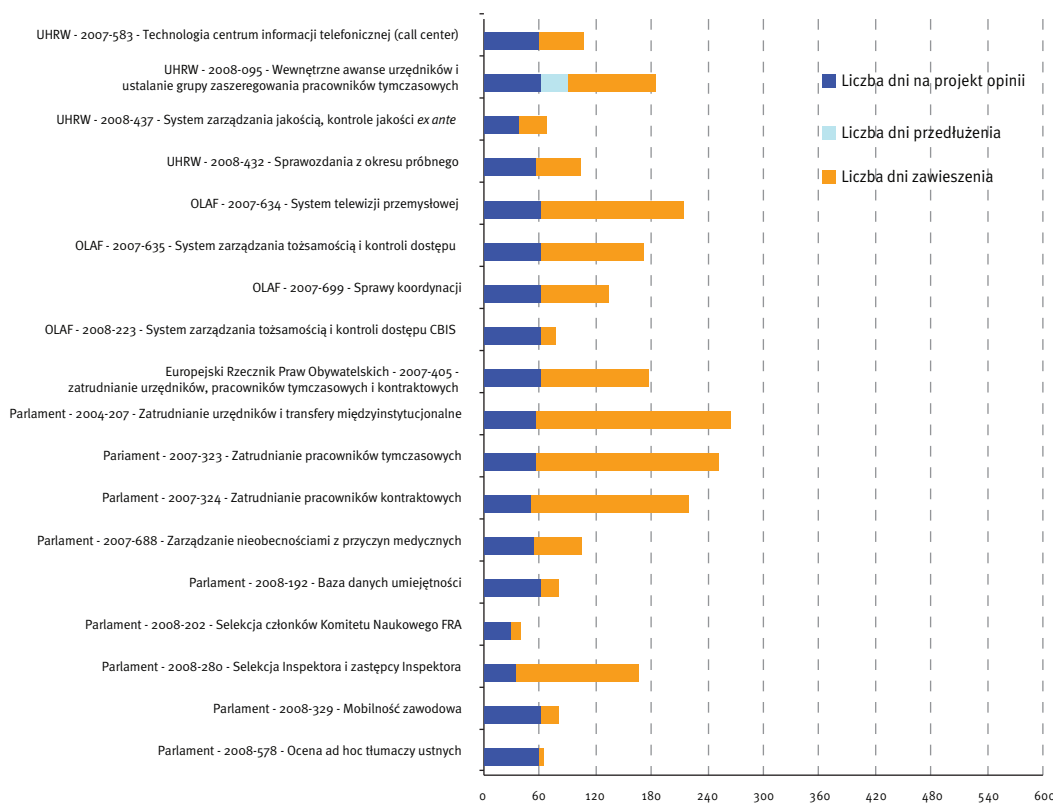
Opinions issued in 2008 (I)



Opinions issued in 2008 (2)



Opinions issued in 2008 (3)



NB: Days taken for the draft opinions do not include the month of August in ex-post cases received before 1/09/08. Suspension days include the suspension for comments on the draft, normally 7 to 10 days.

Załącznik F

Wykaz opinii wydanych w wyniku kontroli wstępnej

Baza danych ARDOS – Komisja

Opinia z dnia 15 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie bazy danych ARDOS (sprawa 2007-380)

„Reakcja zwrotna dotycząca umiejętności przywódczych” – Komisja

Opinia z dnia 15 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie opcjonalnej procedury „Reakcja zwrotna dotycząca umiejętności przywódczych” stosowanej przez Europejską Szkołę Administracji (ESA) w związku z prowadzonymi przez nią kursami w dziedzinie zarządzania (sprawa 2008-527)

Dochodzenia prowadzone przez biuro ds. bezpieczeństwa – Rada

Opinia z dnia 12 grudnia 2008 r. w sprawie powiadomienia dotyczącego prowadzenia dochodzeń przez biuro ds. bezpieczeństwa (sprawa 2008-410)

Procedury przetargowe – Europejski Bank Inwestycyjny

Opinia z dnia 5 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedur przetargowych (sprawa 2007-126)

Ocena tłumaczy ustnych – Parlament

Opinia z dnia 5 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny tłumaczy ustnych (sprawa 2008-578)

Nabór stażystów – Cedefop

Opinia z dnia 5 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru stażystów (sprawa 2008-196)

Flexitime – Trybunał Obrachunkowy

Opinia z dnia 5 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przetwarzania danych systemu zarządzania i kontroli Flexitime (sprawa 2008-173)

IRIS: Dodatki rodzinne – Komisja

Opinia z dnia 5 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie sprawy „IRIS: dodatki rodzinne” (sprawa 2008-439)

COMPAS – Komisja

Opinia z dnia 4 grudnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „koordynacji wsparcia medycznego, psychospołecznego i administracyjnego (COMPAS)” (sprawa 2008-428)

Certyfikacja – Europejski Komitet Ekonomiczno-Społeczny

Opinia z dnia 26 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury certyfikacji (sprawa 2008-475)

Uzupełniająca pomoc dla osób niepełnosprawnych

Opinia z dnia 25 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie uzupełniającej pomocy dla osób niepełnosprawnych (sprawa 2008-388)

Sprawozdania z okresu próbnego – UHRW

Opinia z dnia 25 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie sprawozdań z okresu próbnego (sprawa 2008-432)

Akredytacja – Europejski Komitet Ekonomiczno-Społeczny

Opinia z dnia 25 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury akredytacji (sprawa 2008-476)

Awans pracowniczy – Trybunał Obrachunkowy

Opinia z dnia 24 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury awansu pracowniczego (sprawa 2007-292)

Rejestrowanie rozmów telefonicznych do dyspozytorni technicznej – Komisja

Opinia z dnia 19 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rejestrowania rozmów telefonicznych prowadzonych na linii zarezerwowanej dla dyspozytorni technicznej dotyczących podejmowania czynności w budynkach KE w Brukseli (sprawa 2008-491)

Orzekanie o inwalidztwie – Europejski Komitet Ekonomiczno-Społeczny

Opinia z dnia 19 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie orzekania o inwalidztwie (sprawa 2008-555)

Indywidualna dokumentacja medyczna – Komisja

Opinia z dnia 18 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania indywidualną dokumentacją medyczną Bruksela – Luksemburg (sprawa 2004-225)

Dobór kierowników – UHRW

Opinia z dnia 12 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie doboru kierowników (sprawa 2008-435)

Nieobecność na skutek choroby lub wypadku – Rada

Opinia z dnia 11 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury w przypadku nieobecności na skutek choroby lub wypadku (sprawy 2008-271 i 2008-283)

Baza danych z nazwiskami ekspertów – EFSA

Opinia z dnia 11 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie bazy danych EFSA z nazwiskami ekspertów (sprawa 2008-455)

Obserwacja Internetu – Trybunał Obrachunkowy

Opinia z dnia 10 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie obserwacji Internetu (sprawa 2008-284)

Awans zawodowy urzędników oraz ponowne zaszeregowanie pracowników zatrudnionych na czas określony – UHRW

Opinia z dnia 7 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wewnętrznego awansu zawodowego urzędników oraz ponownego zaszeregowania pracowników zatrudnionych na czas określony (sprawa 2008-95)

Narażenie na promieniowanie – Komisja

Opinia z dnia 5 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie danych dotyczących narażenia na promieniowanie podczas wykonywania zawodu (sprawa 2007-385)

Wykroczenia drogowe – Komisja

Opinia z dnia 3 listopada 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wykroczeń drogowych z udziałem pojazdów służbowych Komisji zarządzanych przez Office Infrastructures et Logistique de Bruxelles (OIB) (sprawa 2008-395)

Szkolenie eHest – Rada

Opinia z dnia 22 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie szkolenia eHEST (komputerowego szkolenia w zakresie bezpieczeństwa w nieprzyjaznym środowisku) (sprawa 2007-387)

Kontrole jakości – UHRW

Opinia z dnia 22 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie kontroli jakości (sprawa 2008-437)

Dobór Inspektora i jego zastępcy – Parlament Europejski i Rada

Opinia z dnia 21 października 2008 r. w sprawie doboru Inspektora i jego zastępcy (sprawy 2008-280 i 2008-292)

Rejestrowanie wywołań alarmowych w siedzibie WCB ISPRA – Komisja

Pismo z dnia 13 października 2008 w odpowiedzi na powiadomienie dotyczące przeprowadzenia kontroli wstępnej w zakresie rejestrowania wywołań alarmowych w siedzibie WCB ISPRA (sprawa 2008-492)

Stypendyści we Wspólnym Centrum Badawczym – Komisja

Opinia z dnia 9 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie selekcji, doboru i zarządzania w odniesieniu do stypendystów we Wspólnym Centrum Badawczym (WCB) (sprawa 2008-138)

Stażyści w WCB – Komisja

Opinia z dnia 9 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury doboru i zarządzania w odniesieniu do stażystów we Wspólnym Centrum Badawczym (WCB) (sprawa 2008-136)

Procedura naboru pracowników kontraktowych w WCB – Komisja

Opinia z dnia 9 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury naboru pracowników kontraktowych we Wspólnym Centrum Badawczym (sprawa 2008-142)

Akta dotyczące naboru urzędników w WCB – Komisja

Opinia z dnia 9 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie „Zarządzania aktami dotyczącymi naboru urzędników w WCB (transfery i laureaci otwartych konkursów)” (sprawa 2008-140)

Dochodzenia dotyczące bezpieczeństwa – Komisja

Opinia z dnia 2 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie dochodzeń dotyczących bezpieczeństwa (sprawa 2007-736)

Projekt pilotażowy dotyczący nadzorowania indywidualnej wydajności – Rada

Opinia z dnia 1 października 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie projektu pilotażowego dotyczącego nadzorowania indywidualnej wydajności: dalsze przetwarzanie danych osobowych w systemie przepływu pracy (sprawa 2008-436)

Sieć osób zaufania (molestowanie) – Komisja

Opinia z dnia 30 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wdrożenia przez kierownictwo i przez sieć osób zaufania nieformalnej procedury walki z molestowaniem moralnym i molestowaniem seksualnym w Komisji Europejskiej (procedury zwalczania molestowania) (sprawa 2008-062)

Nabór stażystów – EMSA

Opinia z dnia 29 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru stażystów w ramach planu stażów w EMSA (sprawa 2008-384)

Podwójny dodatek na dziecko pozostające na utrzymaniu – Rada

Opinia z dnia 29 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie podwójnego dodatku na dziecko pozostające na utrzymaniu (sprawa 2008-405)

Staż – Trybunał Obrachunkowy

Opinia z dnia 19 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wniosków o staże płatne lub bezpłatne (sprawa 2008-391)

Mobilność w ramach kariery zawodowej – Parlament

Opinia z dnia 17 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie mobilności w ramach kariery zawodowej (sprawa 2008-329)

Korzystanie z poddostawców przez kasę chorych – EBI

Opinia z dnia 16 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie częściowego korzystania z poddostawców przez kasę chorych (sprawa 2008-323)

Akredytowanie dziennikarzy – Rada

Opinia z dnia 16 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie akredytowania dziennikarzy biorących udział w posiedzeniach Rady Europejskiej (sprawa 2004-259)

Akredytowanie pracowników firm zewnętrznych – Rada

Opinia z dnia 16 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie akredytowania pracowników firm zewnętrznych biorących udział w posiedzeniach Rady Europejskiej (sprawa 2007-046)

Interfejs Flexitime / PersonaGrata – Rada

Opinia z dnia 16 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie interfejsu Flexitime / PersonaGrata (DGA3) (sprawa 2008-324)

Zaproszenia do składania ofert i do kontraktów – Komitet Regionów i Europejski Komitet Ekonomiczno-Społeczny

Opinia z dnia 15 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie operacji przetwarzania danych w celu zarządzania zaproszeniami do składania ofert i do kontraktów (sprawa 2008-346)

Interfejs Flexitime w ramach systemu zarządzania czasem w Dyrekcji Generalnej ds. Przedsiębiorczości i Przemysłu – Komisja

Odpowiedź z dnia 15 września 2008 r. na powiadomienie dotyczące przeprowadzenia kontroli wstępnej w zakresie interfejsu flexitime w ramach systemu zarządzania czasem w dyrekcji generalnej ds. przedsiębiorczości i przemysłu (sprawa 2008-111)

System zarządzania danymi dozymetrycznymi – Komisja

Opinia z dnia 3 września 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu zarządzania danymi dozymetrycznymi pracowników narażonych na promieniowanie w WCB-IE w Petten (sprawa 2008-020)

Dochodzenia dotyczące bezpieczeństwa w Ispra – Komisja

Opinia z dnia 31 lipca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie dochodzeń dotyczących bezpieczeństwa we Wspólnym Centrum Badawczym ISPRA (sprawa 2007-507)

Wspólny serwis medyczno-socjalny – Komitet Regionów i EKES

Opinia z dnia 4 lipca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wspólnego serwisu medyczno-socjalnego (sprawa 2007-004)

System zarządzania tożsamością i dostępem – OLAF

Opinia z dnia 30 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu zarządzania tożsamością i dostępem CBIS (sprawa 2008-223)

Centrum opieki dziennej – Cedefop

Opinia z dnia 20 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie centrum opieki dziennej (sprawa 2008-193)

Nabór personelu – EMCDDA

Opinia z dnia 20 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru personelu (sprawa 2008-157)

Urlopy i system flexitime – EMCDDA

Opinia z dnia 20 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania urlopami i systemem flexitime (sprawa 2008-158)

Nabór personelu – Europejska Agencja Leków

Opinia z dnia 19 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie bazy danych EMEA (Access) dotyczącej doboru personelu oraz procedur selekcji i doboru (sprawa 2007-422)

Wcześniejsze przechodzenie na emeryturę – EMCDDA

Opinia z dnia 16 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie stosowanej co roku procedury dotyczącej wcześniejszego przechodzenia na emeryturę bez zmniejszania praw emerytalnych (sprawa 2008-154)

Baza danych dotycząca umiejętności zawodowych – Parlament

Opinia z dnia 13 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie bazy danych dotyczącej umiejętności zawodowych (sprawa 2008-192)

Dobór pracowników tymczasowych w WCB i zarządzanie nimi – Komisja

Opinia z dnia 9 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie doboru pracowników tymczasowych w WCB i zarządzania nimi (sprawa 2008-139)

Badania lekarskie — Wspólnotowy Urząd Ochrony Odmian Roślin (CPVO)

Opinia z dnia 4 czerwca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oględzin medycznych przeprowadzanych przed zatrudnieniem i corocznych badań lekarskich pracowników CPVO (sprawa 2007-176)

Parking dla osób niepełnosprawnych – Rada

Opinia z dnia 29 maja 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przydzielania i rezerwacji miejsc parkingowych dla osób niepełnosprawnych (sprawa 2007-753)

Przydzielanie mieszkań za pośrednictwem ALER – Komisja

Opinia z dnia 26 maja 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przydzielania mieszkań za pośrednictwem ALER pracownikom statutowym WCB Ispra oraz szkoły europejskiej w Varese (sprawa 2008-144)

Ośrodek opieki nad dziećmi (żłobek) przy WCB – Instytucie Materiałów Referencyjnych i Pomiarów w Geel – Komisja

Opinia z dnia 23 maja 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie operacji przetwarzania danych osobowych dotyczących ośrodka opieki nad dziećmi (żłobka) przy WCB – Instytucie Materiałów Referencyjnych i Pomiarów w Geel (sprawa 2008-152)

Trzeci język – EMCDDA

Opinia z dnia 20 maja 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny umiejętności personelu w zakresie pracy w trzecim języku (sprawa 2008-159)

System CCTV – OLAF

Opinia z dnia 19 maja 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu CCTV w OLAF (sprawa 2007-634)

Dobór kandydatów na stanowiska Inspektora i zastępcy Inspektora – Komisja

Opinia z dnia 16 maja 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie stworzenia wykazu zakwalifikowanych kandydatów na stanowisko Europejskiego Inspektora Ochrony Danych i na stanowisko zastępcy Inspektora (sprawa 2008-222)

Procedura doboru komitetu naukowego agencji – FRA

Opinia z dnia 29 kwietnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury doboru członków komitetu naukowego agencji (połączone sprawy 2008-179 i 2008-222)

Osoby zaufania w ramach walki z molestowaniem – Komisja

Opinia z dnia 29 kwietnia w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru osób zaufania w ramach walki z molestowaniem moralnym i molestowaniem seksualnym w Komisji Europejskiej (sprawa 2008-60)

Zaplecze opieki nad dziećmi w WCB Ispra – Komisja

Opinia z dnia 21 kwietnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie administrowania zapleczem opieki nad dziećmi w WCB Ispra (żłobek / świetlica) (sprawa 2007-544)

Urlop rodzinny – EMEA

Opinia z dnia 14 kwietnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie urlopów rodzinnych / bazy danych personelu Compel / elektronicznego systemu zarządzania dokumentami (EDMS) (sprawa 2007-498)

Roczna procedura oceny – CPVO

Opinia z dnia 14 kwietnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rocznej procedury oceny (sprawa 2007-403)

System zarządzania tożsamością i dostępem – OLAF

Opinia z dnia 7 kwietnia 2007 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu zarządzania tożsamością i dostępem (sprawa 2007-635)

Sprawy związane z koordynacją – OLAF

Opinia z dnia 7 kwietnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie spraw związanych z koordynacją (sprawa 2007-699)

Wnioski o pracę w niepełnym wymiarze godzin – Europejska Agencja Leków

Opinia z dnia 1 kwietnia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie wniosków o pracę w niepełnym wymiarze godzin (sprawa 2007-500)

Upoważnienia do występowania w charakterze świadków – Komisja

Opinia z dnia 28 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie upoważnień do występowania w charakterze świadków (sprawa 2007-721)

Przechodzenie na emeryturę bez zmniejszenia praw – Trybunał Sprawiedliwości

Opinia z dnia 17 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przechodzenia na emeryturę bez zmniejszenia praw emerytalnych (sprawa 2007-579)

Nabór urzędników i transfery międzyinstytucjonalne – Parlament

Opinia z dnia 13 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru urzędników i transferów międzyinstytucjonalnych (sprawa 2004-207)

Nabór pracowników zatrudnionych na czas określony – Parlament

Opinia z dnia 13 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru pracowników zatrudnionych na czas określony (sprawa 2007-323)

Nabór pracowników kontraktowych – Parlament

Opinia z dnia 13 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru pracowników kontraktowych (sprawa 2007-384)

Ocena niepełnosprawności – Rada

Opinia z dnia 7 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie kwestionariusza oceny niepełnosprawności (sprawa 2008-17)

Działania Europejskiej Szkoły Administracji i EPSO w ramach certyfikacji – Komisja

Opinia z dnia 7 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie działań Europejskiej Szkoły Administracji i EPSO w ramach certyfikacji (sprawa 2006-396)

Zarządzanie nieobecnościami z przyczyn choroby – Parlament

Opinia z dnia 4 marca 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania nieobecnościami z przyczyn choroby (sprawa 2007-688)

Awans zawodowy pracowników zatrudnionych na czas określony – EMEA

Opinia z dnia 20 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie awansu zawodowego pracowników zatrudnionych na czas określony (sprawa 2007-418)

System kontroli z zastosowaniem technologii skanowania tęczówki – Europejski Bank Centralny

Opinia z dnia 14 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rozszerzenia uprzednio istniejącego systemu kontroli dostępu z zastosowaniem technologii skanowania tęczówki w odniesieniu do obszarów, w obrębie których prowadzona jest działalność gospodarcza wymagająca zachowania szczególnych zabezpieczeń (sprawa 2007-501)

Postępowania administracyjne oraz postępowania dyscyplinarne – Cedefop

Opinia z dnia 13 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie przetwarzania danych w ramach postępowań administracyjnych i dyscyplinarnych (sprawa 2007-582)

Sprawdzanie nieobecności w WCB Ispra oraz w Sewilli – Komisja

Opinia z dnia 6 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie sprawdzania nieobecności w pracy na skutek choroby lub wypadku – dossier Wspólnego Centrum Badawczego w Ispra i w Sewilli (dyrekcja generalna) (sprawa 2007-508)

System zarządzania danymi dozymetrycznymi – Komisja

Opinia z dnia 6 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie systemu zarządzania danymi dozymetrycznymi w DG WCB Ispra (sprawa 2007-505)

Usługa zarządzania tożsamością – Komisja

Opinia z dnia 6 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie usługi zarządzania tożsamością (sprawa 2007-349)

Kandydaci chcący korzystać z telepracy – Komisja

Opinia z dnia 6 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru pracowników chcących korzystać z telepracy (sprawa 2007-720)

Indywidualna dokumentacja medyczna w WCB – Komisja

Opinia z dnia 6 lutego 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie indywidualnej dokumentacji medycznej we Wspólnym Centrum Badawczym w Ispra i w Sewilli (sprawa 2007-329)

Rozwój kariery i cykl ocen – EFSA

Opinia z dnia 25 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rozwoju kariery i cyklu ocen (sprawa 2007-585)

CASABLANCA – Rada

Opinia z dnia 25 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie dossier „CASABLANCA” (zarządzanie działaniami w ramach kształcenia zawodowego” (sprawa 2007-584)

Badania lekarskie w WCB w Ispra – Komisja

Opinia z dnia 25 stycznia 2008 r. dotycząca pierwszej pomocy, wypadków przy pracy i innych badań lekarskich w WCB (Wspólne Centrum Badawcze) w Ispra (sprawa 2007-372)

Procedura zatrudniania – Rada

Opinia z dnia 25 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury zatrudniania urzędników i innych pracowników Sekretariatu Generalnego Rady (sprawa 2007-194)

Medycyna pracy – Komisja

Opinia z dnia 23 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie medycyny pracy w DG WCB Ispra (sprawa 2007-504)

Zarządzanie oprogramowaniem PowerLab – Komisja

Opinia z dnia 17 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania oprogramowaniem laboratoriów klinicznych i toksykologicznych (Power Lab) w DG WCB (sprawa 2007-649)

Kontrakt z niezależnym tłumaczem pisemnym – Centrum Tłumaczeń

Opinia z dnia 17 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedur przetargowych i sporządzenia kontraktu z niezależnym tłumaczem pisemnym (sprawa 2007-327)

Dokumentacja medyczna dzieci uczęszczających do żłobka – Rada

Opinia z dnia 17 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie zarządzania dokumentacją medyczną dzieci uczęszczających do żłobka Sekretariatu Generalnego Rady (SGR) (sprawa 2007-491)

Ocena personelu – EMCDDA

Opinia z dnia 11 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie oceny personelu / procedury oceny (sprawa 2007-334)

Technologia centrum telefonicznego – UHRW

Opinia z dnia 11 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie technologii centrum telefonicznego (sprawa 2007-583)

Przetargi elektroniczne – Rada

Opinia z dnia 10 stycznia 2008 r. w sprawie powiadomienia dotyczącego składanej drogą elektroniczną aplikacji przetargowej obejmującej procedury zamówień publicznych Rady (sprawa 2007-573)

Baza danych AGS-EDV w WCB-ITU w Karlsruhe — Komisja

Opinia z dnia 10 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie bazy danych AGS-EDV w WCB-ITU w Karlsruhe (sprawa 2007-378)

Nabór pracowników – Europejski Rzecznik Praw Obywatelskich

Opinia z dnia 9 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru pracowników (urzędników, pracowników zatrudnionych na czas określony, pracowników kontraktowych) (sprawa 2007-405)

Sprawozdania z okresu próbnego – Europejska Agencja ds. Bezpieczeństwa na Morzu

Opinia z dnia 7 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie sprawozdań z okresu próbnego (sprawa 2007-569)

Rejestrowanie urlopów – Europejska Agencja Leków

Opinia z dnia 7 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie rejestrowania urlopów pracowników zatrudnionych na czas określony, personelu pomocniczego i pracowników kontraktowych, ekspertów krajowych i stażystów (sprawa 2007-420).

Awans – Komitet Regionów

Opinia z dnia 7 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie procedury awansu urzędników (sprawa 2007-354)

Nabór pracowników – Europejska Agencja ds. Bezpieczeństwa na Morzu

Opinia z dnia 7 stycznia 2008 r. w sprawie powiadomienia dotyczącego przeprowadzenia kontroli wstępnej w zakresie naboru stałych pracowników, pracowników zatrudnionych na czas określony i pracowników kontraktowych (sprawa 2007-566)

Załącznik G

Wykaz opinii w sprawie wniosków prawodawczych

Europejska strategia w dziedzinie e-sprawiedliwości

Opinia z dnia 19 grudnia w sprawie komunikatu Komisji dotyczącego europejskiej strategii w dziedzinie e-sprawiedliwości

Transgraniczna opieka zdrowotna

Opinia z dnia 2 grudnia 2008 r. w sprawie wniosku dotyczącego dyrektywy w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej

Grupa kontaktowa wysokiego szczebla UE – USA ds. wymiany informacji

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

Dostępność informacji o majątku dłużnika

Opinia z dnia 22 września 2008 r. na temat zielonej księgi Komisji w sprawie skutecznego wykonywania orzeczeń w Unii Europejskiej: dostępność informacji o majątku dłużnika – COM(2008) 128 wersja ostateczna

ECRIS

Opinia z dnia 16 września 2008 r. na temat wniosku dotyczącego decyzji Rady w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2008/XX/WSiSW

Publiczny dostęp do dokumentów

Opinia z dnia 30 czerwca 2008 r. na temat wniosku dotyczącego rozporządzenia w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. C 2 z 7.1.2009, s. 7)

Ochrona dzieci korzystających z Internetu

Opinia z dnia 23 czerwca 2008 r. na temat wniosku dotyczącego decyzji w sprawie ustanowienia wieloletniego wspólnotowego programu ochrony dzieci korzystających z Internetu i z innych technologii komunikacyjnych (Dz.U. C 2 z 7.1.2009, s. 2)

Statystyki europejskie

Opinia z dnia 20 maja 2008 r. na temat wniosku dotyczącego rozporządzenia w sprawie statystyk europejskich (COM(2007) 625 wersja ostateczna), (Dz.U. C 308 z 3.12.2008, s. 1)

Bezpieczeństwo drogowe

Opinia z dnia 8 maja 2008 r. na temat wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady wprowadzającej ułatwienia w transgranicznym egzekwowaniu prawa dotyczącego bezpieczeństwa drogowego (Dz.U. C 310 z 5.12.2008, s. 9)

Eurojust

Opinia z dnia 25 kwietnia 2008 r. na temat inicjatywy mającej na celu przyjęcie decyzji Rady w sprawie wzmocnienia Eurojustu i zmiany decyzji 2002/187/WSiSW (Dz.U. C 310 z 5.12.2008, s. 1)

Komputerowe systemy rezerwacji

Opinia z dnia 11 kwietnia 2008 r. na temat wniosku dotyczącego rozporządzenia w sprawie kodeksu postępowania dla komputerowych systemów rezerwacji (Dz.U. C 233 z 11.9.2008, s. 1)

E-prywatność

Opinia z dnia 10 kwietnia 2008 r. w sprawie wniosku dotyczącego dyrektywy zmieniającej m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywę o prywatności i łączności elektronicznej), (Dz.U. C 181 z 18.7.2008, s. 1)

Zabezpieczenia i dane biometryczne w paszportach

Opinia z dnia 26 marca 2008 r. na temat wniosku dotyczącego rozporządzenia zmieniającego rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie (Dz. U. C 200 z 6.8.2008, s. 1)

System wymiany informacji rynku wewnętrznego (IMI)

Opinia z dnia 22 lutego 2008 r. dotycząca decyzji Komisji z dnia 12 grudnia 2007 r. w sprawie wdrożenia systemu wymiany informacji rynku wewnętrznego (IMI) pod względem ochrony danych osobowych (2008/49/WE) (Dz.U. C 270 z 25.10.2008, s. 1)

Załącznik H

Skład sekretariatu EIOD

Wydziały pod bezpośrednim zwierzchnictwem Inspektora lub zastępcy inspektora:• **Nadzór**

Sophie LOUVEAUX
Administrator / urzędnik ds. prawnych
Koordynator ds. stosunków z DPO i kontroli wstępnych

Rosa BARCELÓ
Administrator / urzędnik ds. prawnych

Zsuzsanna BELENYESSY
Administrator / urzędnik ds. prawnych

Eva DIMOVNÉ KERESZTES
Administrator / urzędnik ds. prawnych
Koordynator ds. inspekcji

Maria Veronica PEREZ ASINARI
Administrator / urzędnik ds. prawnych
Koordynator ds. środków administracyjnych

Jarosław LOTARSKI
Administrator / urzędnik ds. prawnych
Koordynator ds. skarg

Tereza STRUNCOVA
Administrator / urzędnik ds. prawnych

Isabelle CHATELIER
Administrator / urzędnik ds. prawnych

Delphine HAROU (*)
Asystent ds. nadzoru

Xanthi KAPSOSIDERI
Asystent ds. nadzoru

Sylvie LONGRÉE
Asystent ds. nadzoru

Kim Thien LÊ
Asystent ds. sekretariatu

Thomas GREMEL
Asystent ds. nadzoru

György HALMOS (*)
Ekspert krajowy / urzędnik ds. prawnych
(do września 2008)

Athena BOURKA
Ekspert krajowy / urzędnik ds. technologii
(od września 2008)

Manuel GARCIA SANCHEZ
Ekspert krajowy / urzędnik ds. technologii
(od września 2008)

• **Polityka i informacja**

Hielke HIJMANS
Administrator / urzędnik ds. prawnych
Koordynator ds. konsultacji i postępowań sądowych

Laurent BESLAY
Administrator / urzędnik ds. technologii
Koordynator ds. bezpieczeństwa i technologii

Bénédicte HAVELANGE
Administrator / urzędnik ds. prawnych
Koordynator ds. dużych systemów informatycznych i polityki dotyczącej granic

Alfonso SCIROCCO
Administrator / urzędnik ds. prawnych

Michaël VANFLETEREN
Administrator / urzędnik ds. prawnych

Anne-Christine LACOSTE
Administrator / urzędnik ds. prawnych
Koordynator ds. grupy roboczej art. 29

Herke KRANENBORG
Administrator / urzędnik ds. prawnych

Katarzyna CUADRAT-GRZYBOWSKA
Administrator / urzędnik ds. prawnych

Nathalie VANDELLE (*)
Administrator / urzędnik ds. kontaktów z prasą
Koordynator zespołu ds. informacji

Martine BLONDEAU (*)
Asystent ds. dokumentacji

Andrea BEACH
Asystent ds. sekretariatu

Francisco Javier MOLEÓN GARCIA
Asystent ds. dokumentacji

Gerard VAN BALLEGOIJ
Stażysta (październik 2008 – styczeń 2009)

Athina FRAGKOULI
Stażystka (październik 2008 – luty 2009)

Sarah THOME
Stażystka (październik 2008 – luty 2009)

(*) zespół ds. informacji



Europejski inspektor ochrony danych i jego zastępca wraz z zespołem

Sekcja Personel/Budżet/Administracja

Monique LEENS-FERRANDO

Kierownik sekcji

- **Zasoby ludzkie**

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

Anne LEVÉCQUE
Asystent ds. zasobów ludzkich

Vittorio MASTROJENI
Asystent ds. zasobów ludzkich

- **Budżet i finanse**

Tonny MATHIEU
Administrator / kwestie finansowe

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

Załącznik I

Wykaz porozumień administracyjnych i decyzji

Porozumienie administracyjne podpisane przez Sekretarza Generalnego Parlamentu Europejskiego, Sekretarza Generalnego Rady i Sekretarza Generalnego Komisji oraz przez Europejskiego Inspektora Ochrony Danych (24/6/2004). W dniu 11 grudnia 2006 r. podpisano przedłużenie obowiązywania tego porozumienia.

Wykaz porozumień o gwarantowanym poziomie usług zawartych przez Inspektora z innymi instytucjami

- Porozumienia o gwarantowanym poziomie usług zawarte z Komisją (Biuro ds. Szkoleń DG ds. Edukacji i Kultury; Dyrekcja Generalna ds. Personelu i Administracji oraz Dyrekcja Generalna ds. Zatrudnienia, Spraw Społecznych i Równości Szans)
- Porozumienie o gwarantowanym poziomie usług zawarte z Radą
- Porozumienie o gwarantowanym poziomie usług zawarte z Europejską Szkołą Administracji (ESA)
- Porozumienie administracyjne zawarte pomiędzy Europejskim Inspektorem Ochrony Danych a Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA);
- Porozumienie w sprawie harmonizacji kosztów międzyinstytucjonalnych kursów językowych
- Dwustronne porozumienia między Parlamentem Europejskim i Europejskim Inspektorem Ochrony Danych w sprawie wdrożenia porozumienia administracyjnego z dnia 24 czerwca 2004 r., przedłużonego w dniu 11 grudnia 2006 r.

Wykaz decyzji przyjętych przez Inspektora

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

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

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

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

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

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

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

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

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

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

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

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

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

Decyzja Inspektora z dnia 7 listopada 2005 r. ustanawiająca szczególne dla Europejskiego Inspektora Ochrony Danych procedury kontroli wewnętrznej

Decyzja Inspektora z dnia 10 listopada 2005 r. określająca zasady oddelegowania do Europejskiego Inspektora Ochrony Danych ekspertów krajowych

Decyzja z dnia 16 stycznia 2006 r. zmieniająca decyzję Inspektora z dnia 22 czerwca 2005 r. w sprawie przyjęcia wspólnych zasad ubezpieczenia urzędników Wspólnot Europejskich od ryzyka wypadku i choroby zawodowej

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

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

Decyzja Inspektora z dnia 8 lutego 2006 r. w sprawie utworzenia komitetu pracowniczego w ramach Europejskiego Inspektora Ochrony Danych

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

Decyzja Inspektora z dnia 30 stycznia 2007 r. w sprawie mianowania inspektora ochrony danych w ramach Europejskiego Inspektora Ochrony Danych

Decyzja Inspektora z dnia 30 marca 2007 r. w sprawie przyjęcia ogólnych przepisów wykonawczych dotyczących systemu oceniania pracowników

Decyzja Inspektora z dnia 18 lipca 2007 r. w sprawie przyjęcia polityki w zakresie szkoleń wewnętrznych

Decyzja Inspektora z dnia 1 października 2007 r. w sprawie mianowania księgowego w ramach Europejskiego Inspektora Ochrony Danych

Decyzja Inspektora z dnia 1 października 2007 r. w sprawie wdrożenia art. 4 załącznika VIII regulaminu pracowniczego w zakresie dotyczącym uprawnień emerytalnych

Decyzja Inspektora z dnia 1 października 2007 r. w sprawie wdrożenia art. 11 i 12 załącznika VIII regulaminu pracowniczego w zakresie dotyczącym przenoszenia uprawnień emerytalnych

Decyzja Inspektora z dnia 1 października 2007 r. w sprawie wdrożenia art. 22 ust. 4 załącznika XIII regulaminu pracowniczego w zakresie dotyczącym uprawnień emerytalnych

Decyzja Inspektora z dnia 12 września 2007 r. w sprawie zasad i warunków prowadzenia dochodzeń wewnętrznych w sprawie zapobiegania nadużyciom finansowym, korupcji oraz każdej innej nielegalnej działalności naruszającej interesy Wspólnot

Decyzja Inspektora z dnia 9 listopada 2007 r. w sprawie mianowania audytora wewnętrznego w ramach Europejskiego Inspektora Ochrony Danych

Decyzja Inspektora z dnia 26 listopada 2007 r. w sprawie przyjęcia ogólnych przepisów wykonawczych dotyczących awansu zawodowego

Przepisy z dnia 16 czerwca 2008 r. dotyczące zwrotu wydatków ponoszonych przez osoby spoza służb Inspektora zaproszone do uczestniczenia w posiedzeniach w charakterze ekspertów

Decyzja oddelegowanego urzędnika zatwierdzającego z dnia 8 sierpnia 2008 r. dotycząca archiwizacji dokumentów finansowych i dokumentów uzupełniających

Decyzja Inspektora z dnia 2 października 2008 r. dotycząca ogólnych zasad wykonawczych art. 45a regulaminu pracowniczego (certyfikacja)

Decyzja Inspektora z dnia 16 grudnia 2008 r. w sprawie przyjęcia środków bezpieczeństwa w biurze Europejskiego Inspektora Ochrony Danych

Decyzja Inspektora z dnia 19 grudnia 2008 r. w sprawie mianowania wewnętrznego urzędnika ds. bezpieczeństwa w biurze Europejskiego Inspektora Ochrony Danych

Urząd Publikacji Unii Europejskiej

Sprawozdanie za 2008 r.

Luksemburg: Urząd Publikacji Unii Europejskiej

2008 — 130 str. — 21 × 29.7 cm

ISBN 978-92-95073-17-3

Jak otrzymać publikacje UE

Publikacje płatne:

- w EU Bookshop (internetowa księgarnia UE) – <http://bookshop.europa.eu>
 - w księgarniach (podając tytuł, wydawcę lub numer ISBN)
 - bezpośrednio u naszych przedstawicieli handlowych
- Dane kontaktowe przedstawicieli handlowych można uzyskać na stronie <http://bookshop.europa.eu> lub wysyłając faks na numer +352 2929-42758.

Publikacje bezpłatne:

- w EU Bookshop (internetowa księgarnia UE) – <http://bookshop.europa.eu>
 - w przedstawicielstwach lub delegaturach Komisji Europejskiej
- Dane kontaktowe przedstawicielstw i delegatur można uzyskać na stronie <http://ec.europa.eu> lub wysyłając faks na numer +352 2929-42758.



URZĄD PUBLIKACJI UNII
EUROPEJSKIEJ

*Wiele informacji o Unii Europejskiej można
znaleźć w portalu Europa*

www.edps.europa.eu



Urząd Publikacji



9 789295 073173

ISBN 978-92-95073-02-9