



SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VI kadencja

Druk nr 103

Warszawa, 20 grudnia 2007 r.

Panie i Panowie Posłowie
na Sejm
Rzeczypospolitej Polskiej

Uprzejmie przekazuję wniesiony przez Generalnego Inspektora Ochrony Danych Osobowych w dniu 17 sierpnia 2007 r. – w wykonaniu art. 20 ustawy o ochronie danych osobowych - dokument:

-Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2006.

Marszałek Sejmu

(-) Bronisław Komorowski

**Generalny Inspektor
Ochrony Danych Osobowych**

**SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH
W ROKU 2006**

Sprawozdanie stanowi wykonanie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002 r., Nr 101, poz. 926 ze zm.), zgodnie z którym Generalny Inspektor Ochrony Danych Osobowych składa Sejmowi, raz w roku, sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych.¹

¹ Niniejsze *Sprawozdanie* obejmuje okres działalności Generalnego Inspektora Ochrony Danych Osobowych od dnia 1 stycznia 2006 roku do dnia 31 grudnia 2006 roku.

SPIS TREŚCI

WPROWADZENIE.....	4
A. PRAWNE PODSTAWY DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH	4
B. BIURO GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH.....	5
1. STRUKTURA ORGANIZACYJNA	5
2. PRACOWNICY BIURA GODO.....	6
3. WYKONANIE BUDŻETU GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH ZA 2006 ROK.....	6
CZĘŚĆ I. STAN WIEDZY I PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH	8
1. INFORMACJE OGÓLNE	8
2. KONTROLA ZGODNOŚCI PRZETWARZANIA DANYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH.....	9
3. WYDAWANIE DECYZJI ADMINISTRACYJNYCH I ROZPATRYWANIE SKARG W SPRAWACH WYKONANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH.....	19
1) Administracja publiczna.....	22
2) Bezpieczeństwo publiczne	23
3) Sądy, organy prokuratury, komornicy.....	25
4) Organizacje społeczne	28
5) Banki i inne instytucje finansowe	31
6) Internet	35
7) Marketing	37
8) Sektor mieszkalnictwa.....	40
9) Oświata	42
10) Służba zdrowia	43
11) Ubezpieczenia społeczne, majątkowe i osobowe.....	46
12) Telekomunikacja	48
13) Sektor zatrudnienia.....	50
14) Windykacja	52
15) Inne.....	54
4. PROWADZENIE REJESTRU ZBIORÓW DANYCH ORAZ UDZIELANIE INFORMACJI O ZAREJESTROWANYCH ZBIORACH.....	57
5. OPINIOWANIE PROJEKTÓW USTAW I ROZPORZĄDZEŃ DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH..	67
6. INICJOWANIE I PODEJMOWANIE PRZEDSIĘWZIĘĆ W ZAKRESIE DOSKONALENIA OCHRONY DANYCH OSOBOWYCH	79
7. UCZESTNICTWO W PRACACH MIĘDZYNARODOWYCH ORGANIZACJI I INSTYTUCJI ZAJMUJĄCYCH SIĘ PROBLEMATYKĄ OCHRONY DANYCH OSOBOWYCH	86
CZĘŚĆ II. CHARAKTERYSTYKA DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W 2006 ROKU	93

CZĘŚĆ III. WNIOSKI I PLANOWANE KIERUNKI DZIAŁAŃ GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH.....	111
Załącznik nr 1 Wykaz wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2006 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego.	120
Załącznik nr 2 Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2006 do podmiotów prywatnych.....	121
Załącznik nr 3 Wykaz kontroli przeprowadzonych w 2006 roku.....	123
Załącznik nr 4 Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2006 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych.....	131
Załącznik nr 5 Informacje przekazane przez organy ścigania w sprawach skierowanych w 2006 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa.	137
Załącznik nr 6 Dokumenty Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych przyjęte w 2006 r.	138

SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2006

Wprowadzenie

Rok 2006 był dziewiątym rokiem obowiązywania ustawy o ochronie danych osobowych. Był to rok szczególnie, z uwagi na zmianę na stanowisku Generalnego Inspektora Ochrony Danych Osobowych. Został nim Michał Serzycki, wybrany przez Sejm Rzeczypospolitej Polskiej za zgodą Senatu. Po złożeniu ślubowania, z dniem 13 lipca 2006 r. objął obowiązki Generalnego Inspektora.

A. Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych

Podstawę prawną działania Generalnego Inspektora Ochrony Danych Osobowych [dalej: GIODO] stanowi ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz wydane na jej podstawie akty wykonawcze:

- a) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),**
- b) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 100, poz. 1025),**
- c) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 94, poz. 923).**

W 2006 r. dokonano nowelizacji ustawy o ochronie danych osobowych poprzez zmianę jej art. 43 ust. 2². Według obecnego brzmienia tego przepisu, Generalnemu Inspektorowi nie przysługują

² Zmiana ta została wprowadzona przepisami ustawy z dnia 9 czerwca 2006 r. Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz ustawę o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz. U. Nr 104, poz. 711 ze zm.) oraz ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 ze zm.).

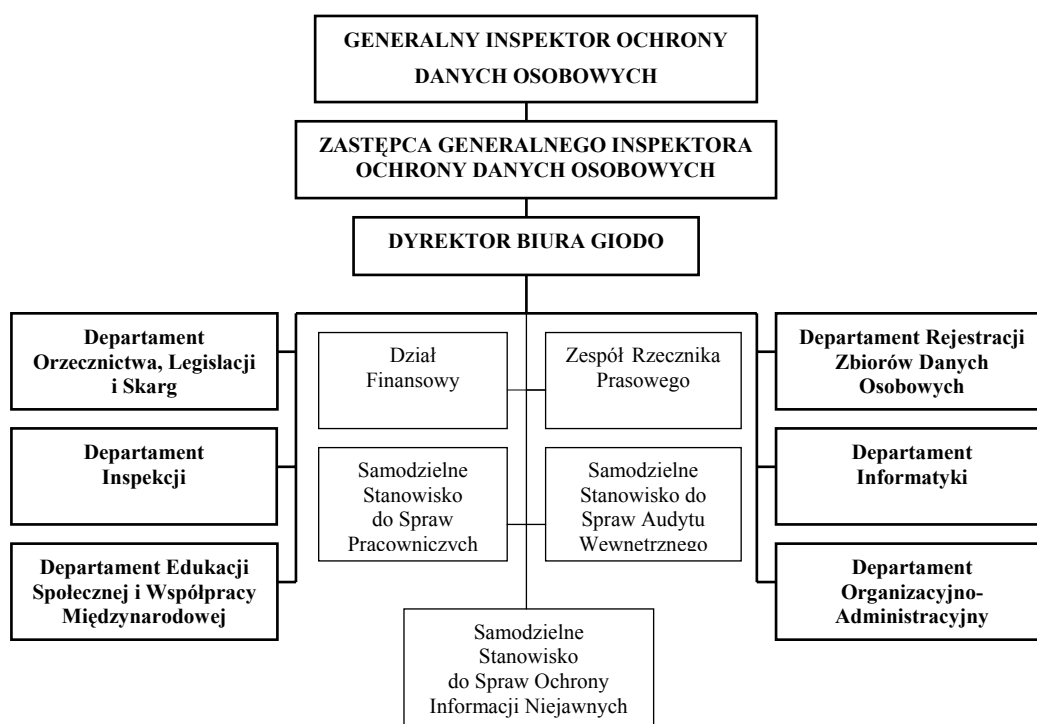
uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1,3-5 oraz w art. 15-18 w odniesieniu do zbiorów, o których mowa w ust. 1 pkt 1 i 3 oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne.

B. Biuro Generalnego Inspektora Ochrony Danych Osobowych

1. Struktura organizacyjna

Zgodnie z art. 13 ustawy o ochronie danych osobowych, Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. Organizacja oraz zasady działania Biura określone zostały w statucie stanowiącym załącznik do rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biura Generalnego Inspektora Ochrony Danych Osobowych.

Poniżej przedstawiona została w formie graficznej obecna struktura organizacyjna Biura Generalnego Inspektora Ochrony Danych Osobowych.



2. Pracownicy Biura GIODO

Stan zatrudnienia w Biurze GIODO na dzień 31 grudnia 2006 r. wyniósł 116,7 etatu. Na stanowiskach merytorycznych zatrudnionych było 98 osób, a na stanowiskach pomocniczych 23 osoby. Wyższe wykształcenie posiadało 96 pracowników, w tym 66 legitymowało się wykształceniem wyższym prawniczym. Zlikwidowany został Pion Ochrony, ale z uwagi na bieżące okresy wypowiedzenia, pracownicy ochrony w liczbie 8 osób, zostali jeszcze uwzględnieni w stanie osobowym Biura na dzień 31 grudnia 2006 r. Z Pionu Ochrony wydzielone zostało Samodzielne Stanowisko do Spraw Ochrony Informacji Niejawnych.

Zatrudnienie w poszczególnych jednostkach organizacyjnych Biura GIODO w przeliczeniu **na pełny etat** na koniec 2006 r. przedstawiał się następująco:

- GIODO – 1 osoba,
- Zastępca GIODO – 1 osoba,
- Asystent GIODO – 1 osoba,
- Dyrektor Biura – 1 osoba,
- Zespół Rzecznika Prasowego – 3 osoby,
- Departament Edukacji Społecznej i Współpracy Międzynarodowej [dalej: DESiWM] – 10 osób,
- Departament Informatyki [dalej: DIF] – 15 osób,
- Departament Inspekcji [dalej: DIS] – 13 osób,
- Departament Orzecznictwa Legislacji i Skarg [dalej: DOLiS] – 28 osób,
- Departament Rejestracji Zbiorów Danych Osobowych [dalej: DRZDO] – 14 osób,
- Departament Organizacyjno-Administracyjny [dalej: DOA] – 15 osób,
- Dział Finansowy – 3 osoby,
- Samodzielne Stanowisko ds. Pracowniczych – 1 osoba,
- Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 1 osoba,
- Samodzielne Stanowisko ds. Audytu Wewnętrznego – 1 osoba,
- Radcy Prawni – 2 osoby.
- Pion Ochrony – 8 osób,

3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2006 rok

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2006 r. wynosił:
12 020 tys. zł, w tym:

wynagrodzenia	7 827 tys. zł
pochodne od wynagrodzeń	1 417 tys. zł
wydatki majątkowe	200 tys. zł

pozostałe wydatki	2 576 tys. zł
-------------------	---------------

Wydatki zrealizowane przez GIODO wynosiły 11 547 tys. zł, w tym:

wynagrodzenia	7 528 tys. zł
---------------	---------------

poходne od wynagrodzeń	1 282 tys. zł
------------------------	---------------

wydatki majątkowe	180 tys. zł
-------------------	-------------

pozostałe wydatki	2 557 tys. zł
-------------------	---------------

Część I. Stan wiedzy i przestrzegania przepisów o ochronie danych osobowych

1. Informacje ogólne

Ustawa o ochronie danych osobowych wprowadza szczegółowe normy służące realizacji prawa do ochrony danych osobowych. Reguluje postępowanie przy przetwarzaniu danych osobowych, czyli operacjach takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zdefiniowanych jako wszelka informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby.

Jako obywatele mamy możliwość skorzystania z przysługującego nam prawa do formalnej kontroli przestrzegania przetwarzania dotyczących nas danych, które to prawo zapisane jest w rozdziale 4 ustawy. Możemy domagać się również uzyskania informacji, czy zbiór danych istnieje, ustalenia administratora danych, adresu jego siedziby, uzyskania informacji o celu, zakresie i sposobie przetwarzania danych oraz informacji o źródle, z którego pochodzą, żądania uzupełnienia, uaktualnienia, sprostowania, a nawet żądania czasowego lub stałego wstrzymania przetwarzania danych, jeżeli są one nieaktualne, niekompletne, nieprawdziwe lub zostały zebrane z naruszeniem prawa, albo są już zbędne do realizacji celu, dla którego były zebrane. Mamy także prawo do sprzeciwu, gdy administrator przetwarza je w celach marketingowych lub przekazuje je innemu administratorowi danych. Służy nam więc prawo żądania od administratora danych odpowiedniego zachowania się w przypadku nieprzestrzegania ustawy, a także prawo do występowania do Generalnego Inspektora Ochrony Danych Osobowych, organów ścigania oraz wymiaru sprawiedliwości w sprawach naruszenia przepisów o ochronie danych osobowych.

Reasumując, ustawa o ochronie danych osobowych konkretyzuje prawa osoby, której dane dotyczą w taki sposób, aby zagwarantować maksymalne bezpieczeństwo informacjom jej dotyczącym, a ponadto wyposażyła ją w instrumenty służące realizacji tego prawa.

Od chwili wejścia w życie ustawy o ochronie danych osobowych w kwietniu 1998 r., poziom świadomości prawnej społeczeństwa na temat danych osobowych z roku na rok ulega nieznacznemu, ale zauważalnemu zwiększeniu. Dynamikę tego procesu prześledzić można w oparciu o zakres zadań stojących przed Generalnym Inspektorem Ochrony Danych Osobowych, określonych w art. 12 ww. ustawy, który stwierdza, że do zadań Generalnego Inspektora należy w szczególności:

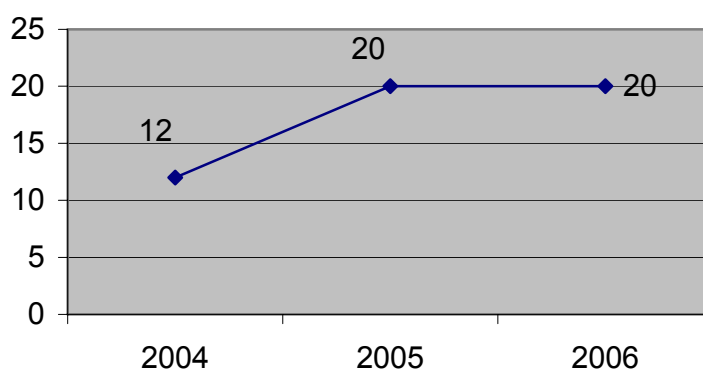
- 1) kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- 2) wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- 3) prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach,
- 4) opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,

- 5) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- 6) uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

2. Kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych

Czynności kontrolne, których celem jest ustalenie, czy jednostka kontrolowana przetwarza dane zgodnie z przepisami o ochronie danych osobowych, należą do podstawowych zadań Generalnego Inspektora Ochrony Danych Osobowych, jego Zastępcy oraz upoważnionych inspektorów.

W 2006 roku, na ogólną liczbę 132 kontroli, w **podmiotach wykonujących zadania publiczne** przeprowadzono 20 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.³



Wykres 1: Porównanie liczby przeprowadzonych kontroli w podmiotach należących do sfery publicznej w latach 2004 – 2006.

W ramach tej kategorii podmiotów kontrole przeprowadzono m.in. w placówkach Straży Granicznej, izbach celnych, a także w stacji sanitarno – epidemiologicznej.

Na podstawie wyników kontroli należy stwierdzić, że ww. podmioty miały problemy z właściwym zabezpieczeniem danych osobowych. Stosowane w tym zakresie rozwiązania techniczne i organizacyjne nie zapewniały bowiem ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, w szczególności przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Uchybienia polegały w szczególności na nie zastosowaniu protokołu kryptograficznej ochrony danych przesyłanych w sieci publicznej dla systemu rejestracji internetowej, w którym przetwarzane są dane osobowe, a także na zainstalowaniu

³ Np. GI-DIS-K-411/34/06, GI-DIS-K-411/65/06, GI-DIS-K-411/77/06.

nieaktualnej bazy antywirusowej na komputerze przenośnym służącym do przetwarzania danych osobowych.

Kontrole wykazały również inne uchybienia w procesie przetwarzania danych osobowych. W szczególności dotyczyły one dokumentacji opisującej sposób ich przetwarzania, a zwłaszcza przetwarzania danych osobowych przy użyciu systemów informatycznych. Stwierdzone w tym zakresie nieprawidłowości polegały m.in. na nie opracowaniu polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a także na nie prowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych. Natomiast uchybienia w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych dotyczyły przede wszystkim nie spełniania przez te systemy wszystkich wymogów o charakterze technicznym (m.in. nie zapewnianie przez te systemy dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy,⁴ którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, zmienianie haseł dostępu rzadziej niż co 30 dni). W pojedynczych przypadkach stwierdzono także nieprawidłowości polegające na nie wyznaczeniu administratora bezpieczeństwa informacji, na dopuszczeniu do przetwarzania danych osobowych osób nie posiadających upoważnień nadanych przez administratora danych.

Spośród organów administracji publicznej najwięcej kontroli Generalny Inspektor przeprowadził w jednostkach **Straży Granicznej**.⁵ Zakresem wskazanych kontroli objęto ustalenie stanu zaawansowania prac i ich zgodności z przepisami o ochronie danych osobowych w zakresie wdrożenia dorobku prawnego Schengen w związku z realizacją przepisów Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen [dalej: KWS] z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. UE L z 2000 r. Nr 239, poz. 19 ze zm.). Przeprowadzone kontrole wykazały, iż placówki Straży Granicznej są przygotowane do wdrożenia dorobku prawnego Schengen, jednakże termin oraz sposób zakończenia prac wdrożeniowych uzależniony jest od zakończenia procesu opracowywania systemu informatycznego o nazwie „SIS II”, który ma służyć do wymiany informacji wynikających z Konwencji Wykonawczej do Układu z Schengen pomiędzy państwami członkowskimi należącymi do tego Układu. Jednocześnie w toku przedmiotowych kontroli nie stwierdzono uchybień w zakresie nieodpowiedniego zabezpieczenia danych osobowych.

⁴ Zgodnie z art. 7 pkt 6 ustawy o ochronie danych osobowych, przez odbiorcę danych rozumie się każdego, komu udostępnia się dane osobowe, z wyłączeniem: a) osoby, której dane dotyczą, b) osoby upoważnionej do przetwarzania danych, c) przedstawiciela, o którym mowa w art. 31a, d) podmiotu, o którym mowa w art. 31, e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

⁵ Np. GI-DIS-K-411/63/06, GI-DIS-K-411/64/06 i GI-DIS-K-411/67/06.

W 2006 r. Generalny Inspektor przeprowadził kontrolę w **stowarzyszeniu** zajmującym się m.in. ochroną zdrowia, leczeniem i rehabilitacją dzieci i osób niewidomych i słabowidzących, w szczególności ze sprzężonymi niepełnosprawnościami oraz dzieci zagrożonych utratą widzenia lub zaburzeniami widzenia.⁶ W ramach swej działalności stowarzyszenie prowadzi niepubliczne zakłady opieki zdrowotnej, poradnie specjalistyczne, poradnie diagnostyczne dla dzieci i osób niewidomych i słabowidzących oraz organizuje i prowadzi niepubliczne placówki edukacyjne,⁷ jak również opracowuje raporty o sytuacji społecznej dzieci i osób niewidomych i słabowidzących i ich rodzin.⁸ W toku kontroli rozstrzygnięto, iż mimo, że środki finansowe dla ww. placówek są pozyskiwane przez stowarzyszenie, to ze względu na odrębność wynikającą z działania każdego z podmiotów na podstawie własnych statutów oraz przepisów prawa, tj. ustawy o systemie oświaty i ustawy o zakładach opieki zdrowotnej, a także charakteru działalności (świadczenie usług medycznych, działalność oświatowa), uznano, że każdy ośrodek jest administratorem przetwarzanych przez niego danych osobowych. Stowarzyszeniu przypisano natomiast przymiot administratora danych w stosunku do osób będących członkami stowarzyszenia, osób zatrudnionych przez stowarzyszenie, a także osób, którym stowarzyszenie udziela pomocy socjalnej. Stowarzyszenie uznano również za administratora danych przekazywanych do Narodowego Funduszu Zdrowia w związku z zawartymi z NFZ umowami o udzielanie świadczeń opieki zdrowotnej – „Rehabilitacja lecznicza” oraz „Programy profilaktyczne i promocja zdrowia.”⁹ W toku kontroli ustalono, iż stowarzyszenie wnioskuje o udzielenie świadczeń z pomocy społecznej swoim podopiecznym w oparciu o art. 102 ustawy z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. Nr 64, poz. 593 ze zm.).¹⁰ Stwierdzono, że pracownicy stowarzyszenia przeprowadzają w tym celu tzw. wywiady środowiskowe na podstawie ustnej zgody. Jeżeli zgoda taka nie zostanie udzielona, stowarzyszenie nie prowadzi postępowania w sprawie przyznania pomocy. Przetwarzanie danych szczególnie chronionych (o stanie zdrowia), które pozyskiwane są w toku

⁶ GI-DIS-K-411/75/06.

⁷ Stowarzyszenie prowadzi m.in. niepubliczne szkoły, przedszkola, ośrodki szkoleniowo – rehabilitacyjne i szkolno – wychowawcze, placówki wczesnego wspomagania rozwoju, poradnie psychologiczno – pedagogiczne i inne poradnie specjalistyczne.

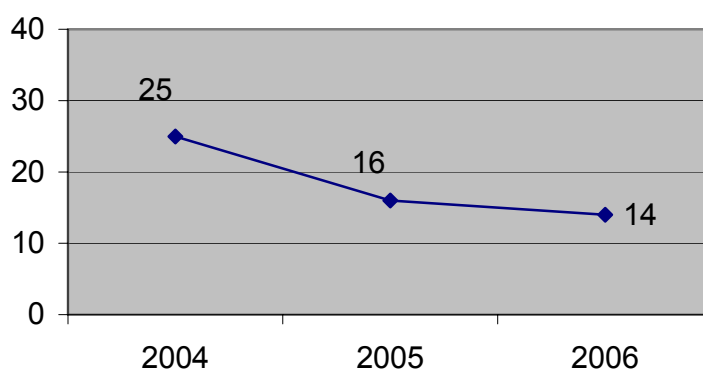
⁸ Stowarzyszenie jest organem założycielskim m.in.: Niepublicznego Specjalnego Ośrodka Szkolno-Rehabilitacyjnego dla Dzieci i Młodzieży Niewidomej i Słabowidzącej ze Sprzężonymi Niepełnosprawnościami przy Zespole Ośrodków dla Dzieci i Młodzieży Niewidomej i Słabowidzącej ze Sprzężonymi Niepełnosprawnościami, Niepublicznego Przedszkola Specjalnego dla Dzieci Niewidomych i Słabowidzących przy Zespole Ośrodków dla Dzieci i Młodzieży Niewidomej i Słabowidzącej ze Sprzężonymi Niepełnosprawnościami i Niepublicznego Zakładu Opieki Zdrowotnej przy Zespole Ośrodków dla Dzieci i Młodzieży Niewidomej i Słabowidzącej ze Sprzężonymi Niepełnosprawnościami.

⁹ W toku kontroli ustalono, że w związku z zawarciem przez stowarzyszenie ww. umów do NFZ przekazywane są dane o wykonanych świadczeniach opieki zdrowotnej. Rejestry świadczeń medycznych są prowadzone przez Niepubliczny Zakład Opieki Zdrowotnej przy Zespole Ośrodków dla Dzieci i Młodzieży Niewidomej i Słabowidzącej ze Sprzężonymi Niepełnosprawnościami i co dziesięć dni przekazywane stowarzyszeniu w celu wystawienia faktury. Świadczenia są wykonywane w gabinetach ww. zakładu opieki zdrowotnej znajdujących się w ośrodkach, dla których kontrolowane stowarzyszenie jest organem założycielskim. Z zakładu opieki zdrowotnej do stowarzyszenia przekazywane są dane dzieci obejmujące imię, nazwisko oraz informację o wykonanym świadczeniu. Ww. dane są przekazywane w formie papierowych rejestrów świadczeń medycznych.

¹⁰ Zgodnie z tym przepisem, świadczenia z pomocy społecznej są udzielane na wniosek osoby zainteresowanej, jej przedstawiciela ustawowego albo innej osoby, za zgodą osoby zainteresowanej lub jej przedstawiciela ustawowego.

przeprowadzanych wywiadów środowiskowych, odbywa się zatem bez podstawy prawnej. Zgoda na przetwarzanie tego typu danych nie jest bowiem wyrażana w formie pisemnej, czego wymaga art. 27 ust. 2 pkt 1 ustawy o ochronie danych osobowych.¹¹

W 2006 r. w **bankach oraz innych instytucjach finansowych** przeprowadzono 14 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.¹² Zauważyć należy, że w porównaniu z latami ubiegłymi mniejsza liczba przeprowadzonych kontroli w wymienionych podmiotach wynikała w szczególności ze spadku liczby skarg na te instytucje.



Wykres 2: Porównanie liczby przeprowadzonych kontroli w bankach i innych instytucjach finansowych w latach 2004 – 2006.

Na podstawie wyników kontroli należy stwierdzić, że jednostki kontrolowane najczęściej problemów miały z prawidłowym wykonaniem obowiązków związanych z opracowaniem dokumentacji opisującej sposób przetwarzania danych. Stwierdzone w tym zakresie nieprawidłowości polegały m.in. na nie opracowaniu polityki bezpieczeństwa lub nie zawarciu w opracowanych dokumentach wszystkich informacji określonych w przepisach o ochronie danych osobowych, a w szczególności: wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

W pojedynczych przypadkach stwierdzano również inne uchybienia w procesie przetwarzania danych osobowych, np. dopuszczenie do przetwarzania danych osobowych osób nie posiadających upoważnień nadanych przez administratora danych, brak ewidencji osób upoważnionych do przetwarzania danych osobowych lub nie zawarcie w niej wszystkich wymaganych informacji (np.

¹¹ Stosownie do treści tego przepisu, przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych.

¹² Np. GI-DIS-K-411/10/06, GI-DIS-K-411/30/06 i GI-DIS-K-411/109/06.

informacji o dacie nadania i ustania oraz zakresie upoważnienia do przetwarzania danych osobowych), a także nie spełnianie przez systemy informatyczne służące do przetwarzania danych osobowych wszystkich wymogów o charakterze technicznym określonych w przepisach rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (m.in. nie zapewnianie przez te systemy odnotowania dla każdej osoby, której dane osobowe przetwarzane były w systemie informatycznym, identyfikatora użytkownika wprowadzającego dane osobowe do systemu).

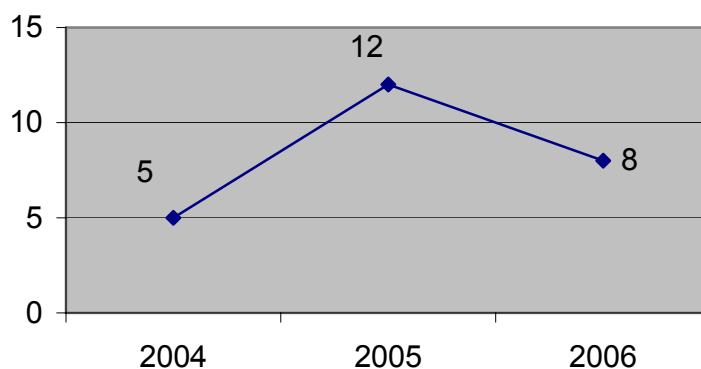
Jedną z przeprowadzonych kontroli wykazała, iż klienci banku mają możliwość korzystania z automatycznego systemu informacyjnego, służącego do udzielania informacji m.in. o rachunkach kredytowych bez udziału pracowników banku.¹³ Jak ustalono, ww. system jest uruchamiany w momencie dodzwonienia się na infolinię banku. Część oferowanych przez ten system opcji, np. dotyczących oferty banku, nie wymaga identyfikacji osoby dzwoniącej, inne natomiast wymagają takiej identyfikacji, np. dotyczące rachunków kredytowych. Identyfikacja osoby dzwoniącej jest dokonywana poprzez numer PESEL oraz, jeżeli został przydzielony, czterocyfrowy telekod. Informacje te wraz z numerem telefonu zapisywane są w logach systemu. Po sprawdzeniu podanych danych udzielane są dzwoniącemu informacje o rachunku, np. wielkość zadłużenia, wysokość raty. W logach omawianego systemu zapisywane są jednak nie tylko numer PESEL i numery telefonów klientów banku, którzy za pośrednictwem tego systemu chcieli uzyskać informacje dotyczące ich rachunków kredytowych, ale również PESEL i numery telefonów osób, które nie są klientami banku, a opcję systemu informacyjnego wymagającą identyfikacji osoby dzwoniącej wybrały przez pomyłkę. Jak ustalono, dane osób nie będących klientami banku zapisane w logach systemu nie są wykorzystywane przez bank w żadnych celach oraz nie są udostępniane innym komórkom organizacyjnym banku. Nie wskazano jednak podstawy prawnej przetwarzania danych ww. osób. Wobec powyższego wszczęte zostało postępowanie administracyjne, które zakończyło się wydaniem decyzji nakazującej zaprzestanie zbierania danych osobowych osób nie będących klientami banku, które przez pomyłkę wybrały opcję systemu informatycznego, wymagającą identyfikacji osoby telefonującej oraz usunięcie z logów tego systemu informatycznego danych ww. osób.¹⁴

W okresie sprawozdawczym 2006 roku, w **podmiotach udzielających świadczeń zdrowotnych oraz jednostkach organizacyjnych samorządu lekarzy** przeprowadzono 8 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.¹⁵

¹³ GI-DIS-K-411/13/06.

¹⁴ Decyzja z dnia 26 lipca 2006 r. o sygn. GI-DEC-DIS-277/06.

¹⁵ Np. GI-DIS-K-411/19/06, GI-DIS-K-411/39/06, GI-DIS-K-411/48/06 i GI-DIS-K-411/49/06.



Wykres 3: Porównanie liczby kontroli przeprowadzonych w służbie zdrowia w latach 2004 – 2006.

Na podstawie ustaleń kontrolnych należy negatywnie ocenić poziom spełnienia przez ww. podmioty wymogów określonych w przepisach o ochronie danych osobowych – uchybień w procesie przetwarzania danych osobowych nie stwierdzono tylko w toku jednej kontroli. W szczególności dotyczy to stosowanych przez podmioty udzielające świadczeń zdrowotnych środków technicznych i organizacyjnych w celu ochrony przetwarzanych danych, które w kontrolowanych jednostkach zostały zastosowane w ograniczonym zakresie. W przypadku podmiotów udzielających świadczeń zdrowotnych podjęcie działań mających na celu właściwe zabezpieczenie danych jest o tyle istotne, że podmioty te przetwarzają dane o stanie zdrowia, które na gruncie przepisów o ochronie danych osobowych korzystają ze wzmożonej ochrony. Tymczasem, w poddanych kontroli podmiotach udzielających świadczeń zdrowotnych, sposób zabezpieczenia dokumentacji medycznej nie zapewniał odpowiedniego poziomu bezpieczeństwa przetwarzanych danych. Uchybienia w tym zakresie polegały m.in. na przechowywaniu dokumentacji zawierającej dane osobowe, w tym dane o stanie zdrowia, na odkrytych regałach oraz w szafach nie wyposażonych w zamki, a także w pomieszczeniach, w których przyjmowane były osoby postronne. Przeprowadzone kontrole wykazały ponadto, że podmioty udzielające świadczeń zdrowotnych miały również dużo problemów z prawidłowym wypełnieniem innych obowiązków dotyczących zabezpieczenia danych osobowych, tj. opracowaniem ewidencji osób upoważnionych do przetwarzania danych osobowych oraz opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

W toku kontroli podmiotów udzielających świadczeń zdrowotnych stwierdzono także liczne uchybienia w procesie przetwarzania danych osobowych w systemach informatycznych. Uchybienia te polegały m.in. na nie zapewnianiu przez systemy informatyczne służące do przetwarzania danych osobowych dla każdej osoby, której dane osobowe były przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika

wprowadzającego dane osobowe do systemu, nie zabezpieczeniu systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz zmienianiu haseł dostępu rzadziej niż co 30 dni.

W pojedynczych przypadkach przeprowadzone kontrole wykazały także inne naruszenia przepisów o ochronie danych osobowych. Wskazane nieprawidłowości dotyczyły dopuszczenia do przetwarzania danych osób nie posiadających upoważnienia nadanego przez administratora danych, nie wyznaczenia administratora bezpieczeństwa informacji oraz zbierania danych osobowych pracowników w zakresie szerszym (m.in. o nazwisko rodowe matki), niż wynikało to z przepisów art. 22¹ § 1, § 2 i § 4 Kodeksu pracy.¹⁶

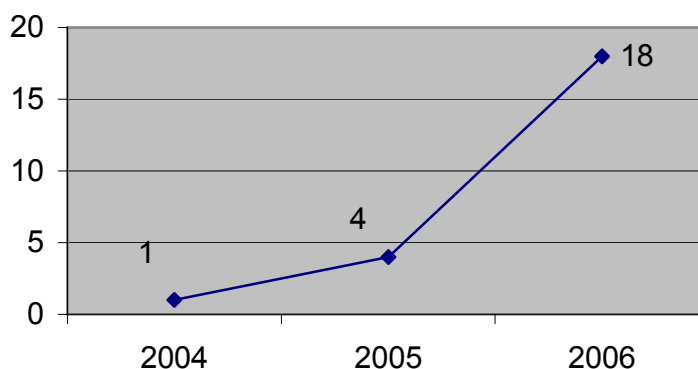
W związku ze stwierdzonymi w toku kontroli uchybieniami wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych przez jednostki kontrolowane w toku postępowania.¹⁷ W wydanych decyzjach Generalny Inspektor nakazał m.in. opracowanie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zmodyfikowanie systemów informatycznych służących do przetwarzania danych osobowych tak, aby zapewniały odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz zmienianie haseł dostępu nie rzadziej niż co 30 dni.

W 2006 r. w jednostkach organizacyjnych **Zakładu Ubezpieczeń Społecznych** zostało przeprowadzonych 14 kontroli¹⁸, a w podmiotach prowadzących działalność w zakresie ubezpieczeń majątkowych i osobowych 4 kontrole zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

¹⁶ Art. 22¹ § 1 Kodeksu pracy stanowi, iż pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: 1) imię (imiona) i nazwisko, 2) imiona rodziców, 3) datę urodzenia, 4) miejsce zamieszkania (adres do korespondencji), 5) wykształcenie, 6) przebieg dotychczasowego zatrudnienia. Pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, także: 1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, 2) numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL) (§ 2). Zgodnie z § 4, pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

¹⁷ Np. decyzja z dnia 12 lipca 2006 r. o sygn. GI-DEC-DIS-254/06 i decyzja z dnia 8 listopada 2006 r. o sygn. GI-DEC-DIS-418/06.

¹⁸ Np. kontrole GI-DIS-K-411/57/06, GI-DIS-K-411/78/06 i GI-DIS-K-411/79/06.



Wykres 4: Porównanie liczby przeprowadzonych kontroli w podmiotach prowadzących działalność w zakresie ubezpieczeń w latach 2004 – 2006.

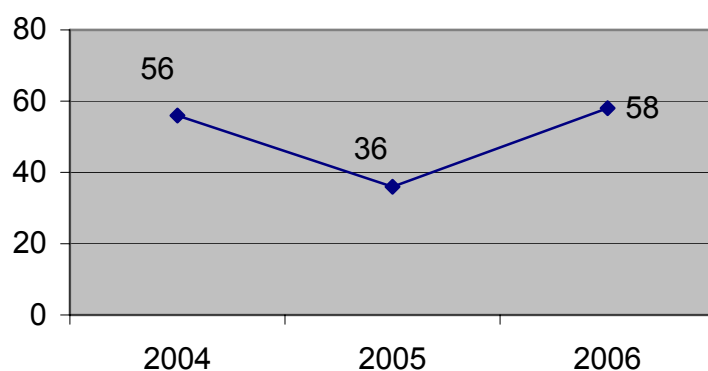
Kontrole w jednostkach organizacyjnych ZUS przeprowadzone zostały w celu ustalenia sposobu zabezpieczenia danych osobowych. Oceniając wyniki kontroli należy stwierdzić, że w poddanych kontroli jednostkach zastosowane zostały środki organizacyjne i techniczne zapewniające ochronę danych osobowych przetwarzanych w formie tradycyjnej przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Uchybienia w tym zakresie stwierdzono tylko w toku dwóch kontroli – dokumenty zawierające dane osobowe zostały umieszczone na odkrytych regałach oraz w szafach, które nie zostały wyposażone w zamki. Więcej problemów kontrolowane jednostki miały z prawidłowym wypełnieniem obowiązków dotyczących przetwarzania danych osobowych przy użyciu systemów informatycznych. Stwierdzone nieprawidłowości polegały m.in. na nie zapewnianiu przez systemy informatyczne służące do przetwarzania danych osobowych dla każdej osoby, której dane osobowe były przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W pojedynczych przypadkach przeprowadzone kontrole wykazały także inne naruszenia przepisów o ochronie danych osobowych. Wskazane nieprawidłowości dotyczyły w szczególności nie uwzględnienia w prowadzonej ewidencji osób upoważnionych do przetwarzania danych osobowych wszystkich osób posiadających upoważnienie do ich przetwarzania, nie zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, nie zawarcia w polityce bezpieczeństwa informacji w zakresie

opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami.

Kontrole w podmiotach prowadzących działalność w zakresie **ubezpieczeń majątkowych i osobowych** przeprowadzono w związku z badaniami Enforcement Task Force Grupy Roboczej Artykułu 29 dotyczącymi wspólnych działań organów ochrony danych osobowych na terenie Unii Europejskiej w prywatnym sektorze ubezpieczeń zdrowotnych. Zakresem kontroli objęto przetwarzane przez te podmioty dane osobowe osób korzystających z prywatnego ubezpieczenia zdrowotnego, w szczególności w zakresie wskazanym w opracowanym przez Enforcement Task Force Grupy Roboczej Artykułu 29 „Kwestionariuszu dla firm prywatnych oferujących prywatne ubezpieczenia zdrowotne”, dotyczącym m.in. rodzaju gromadzonych danych osobowych, podstawy prawnej i rodzaju informacji wymienianych z innymi podmiotami oraz okresu przechowywania danych. Na podstawie ustaleń kontroli opracowano sprawozdanie, które zostało przekazane Grupie Roboczej Artykułu 29 w celu przygotowania zbiorczego raportu na temat ochrony danych osobowych w prywatnym sektorze ubezpieczeń zdrowotnych w Unii Europejskiej.

W roku sprawozdawczym 2006, największą grupę jednostek kontrolowanych stanowiły podmioty zaliczone do sektora „**Inne**”, które ze względu na charakter prowadzonej działalności nie zostały zakwalifikowane gdzie indziej. W podmiotach tych przeprowadzono 58 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.¹⁹ Grupa skontrolowanych podmiotów była bardzo zróżnicowana i obejmowała m.in. podmioty wykonujące działalność gospodarczą w zakresie transportu drogowego, wydawców prasy i książek oraz podmioty zajmujące się produkcją i handlem.



Wykres 5: Porównanie liczby przeprowadzonych kontroli w podmiotach należących do sektora Inne w latach 2004 – 2006.

¹⁹ Np. GI-DIS-K-411/7/06, GI-DIS-K-411/31/06 i GI-DIS-K-411/59/06.

Analizując wyniki przeprowadzonych kontroli należy stwierdzić, że jednostki kontrolowane najczęściej problemów miały z prawidłowym wykonaniem podstawowych obowiązków wynikających z przepisów o ochronie danych osobowych. Uchybienia w tym zakresie dotyczyły w szczególności nie dopełnienia wobec osób, których dane dotyczą, obowiązku informacyjnego wynikającego z art. 24 ust. 1 ustawy o ochronie danych osobowych, nie zgłoszenia do rejestracji Generalnemu Inspektorowi prowadzonych zbiorów danych (np. zbioru danych klientów) oraz zbierania w szerszym zakresie danych osobowych pracowników (m.in. o nazwisko rodowe matki) i kandydatów do pracy (m.in. o stan cywilny) niż wynika to z przepisów art. 22¹ § 1, § 2 i § 4 Kodeksu pracy. Kontrole wykazały również inne nieprawidłowości w procesie przetwarzania danych osobowych, takie jak: dopuszczenie do przetwarzania danych osób nie posiadających upoważnień nadanych przez administratora danych, brak ewidencji osób upoważnionych do przetwarzania danych osobowych oraz polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych lub nie zawarcie w ww. dokumentach wszystkich wymaganych informacji, określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych²⁰ oraz § 4 i § 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.²¹

Negatywnie należy ocenić także sposób wykonania obowiązków związanych z przetwarzaniem danych przy użyciu systemów informatycznych. Nieprawidłowości dotyczyły przede wszystkim nie spełniania przez te systemy wszystkich wymogów o charakterze technicznym (m.in. nie zapewnianie dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu; zmienianie haseł dostępu rzadziej niż co 30 dni; nie stosowanie mechanizmów uwierzytelnienia użytkownika).

²⁰ Art. 39. 1. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej, 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

²¹ § 4. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; 4) sposób przepływu danych pomiędzy poszczególnymi systemami; 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. § 5. Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności: 1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; 2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; 3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; 5) sposób, miejsce i okres przechowywania: a) elektronicznych nośników informacji zawierających dane osobowe, b) kopii zapasowych, o których mowa w pkt 4, 6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia; 7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4; 8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

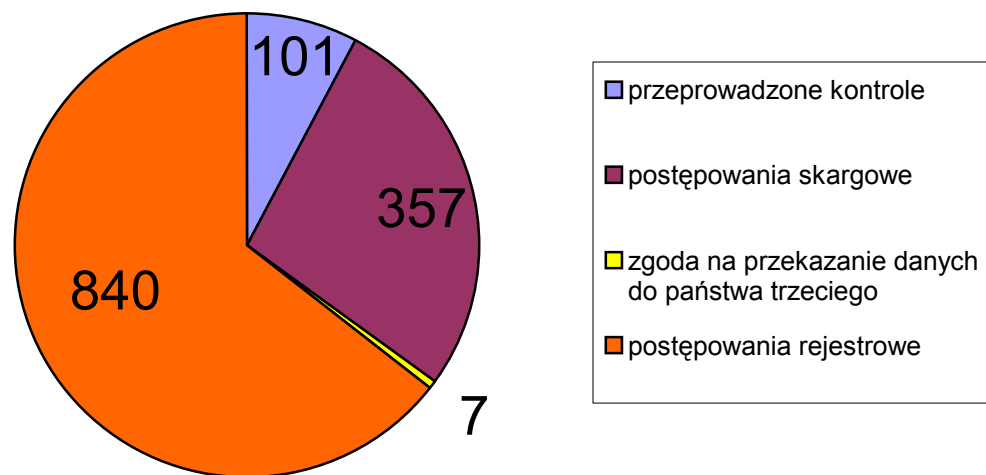
W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych przez jednostki kontrolowane, wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych w toku postępowania.²² Generalny Inspektor w decyzjach nakazywał w szczególności dopełnianie wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, zaprzestanie zbierania danych osobowych pracowników w zakresie nazwiska rodzowego matki, uzupełnienie polityki bezpieczeństwa o informację dotyczącą zakresu danych osobowych przetwarzanych w poszczególnych systemach informatycznych służących do przetwarzania danych osobowych i informację dotyczącą zakresu danych osobowych przepływających pomiędzy ww. systemami informatycznymi oraz opracowanie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych

Postępowanie wszczęte przez Generalnego Inspektora z urzędu lub na wniosek osoby zainteresowanej dotyczące naruszenia ustawy o ochronie danych osobowych, toczy się według przepisów Kodeksu postępowania administracyjnego. Postępowanie to może zakończyć się wydaniem decyzji administracyjnej nakazującej administratorowi danych przywrócenie stanu zgodnego z prawem.

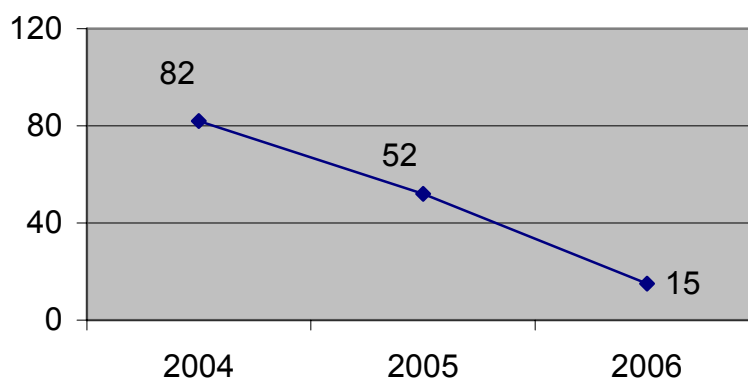
W 2006 roku Generalny Inspektor wydał 1305 decyzji administracyjnych, w tym 840 dotyczyło postępowań rejestrowych, 101 zostało wydanych w związku z przeprowadzonymi kontrolami, 357 wydano na skutek postępowania zainicjowanego skargą, zaś 7 dotyczyło zgody na przekazanie danych do państwa trzeciego.

²² Np. decyzja z dnia 8 czerwca 2006 r. o sygn. GI-DEC-DIS-186/06, decyzja z dnia 26 lipca 2006 r. o sygn. GI-DEC-DIS-279/06 i decyzja z dnia 15 września 2006 r. o sygn. GI-DEC-DIS-359/06.



Wykres 6: Zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2006 roku.

Liczba **zawiadomień o popełnieniu przestępstwa** składanych przez Generalnego Inspektora od 2004 r. sukcesywnie maleje. Tendencję tę obrazuje poniższy Wykres 7:

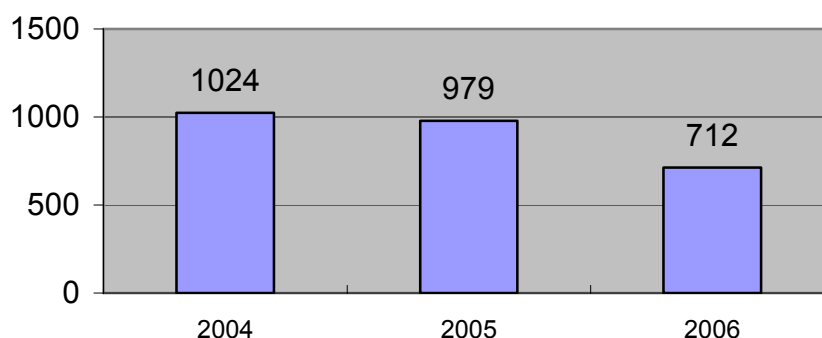


Niewielka liczba zawiadomień złożonych do organów ścigania w 2006 r. wskazuje, iż wśród podmiotów przetwarzających dane osobowe wzrasta świadomość prawna w zakresie zasad przetwarzania danych osobowych.

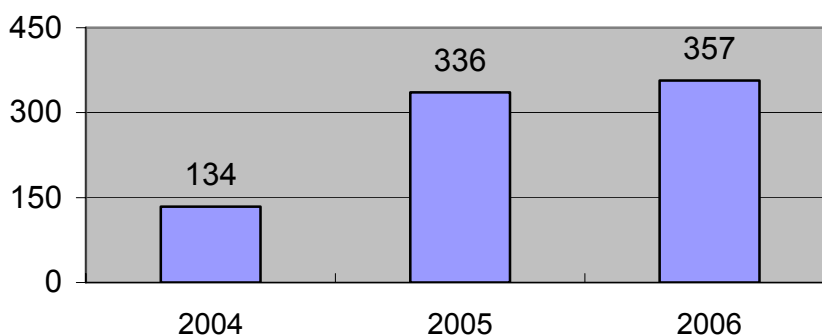
Jak co roku najwięcej zawiadomień o popełnieniu przestępstwa złożonych zostało w związku z postępowaniami prowadzonymi na skutek skarg wniesionych do Generalnego Inspektora (12). Najczęściej są to zawiadomienia o popełnieniu przestępstwa z art. 54 ustawy o ochronie danych osobowych (niedopełnienie obowiązku informacyjnego, o którym mowa w art. 24 lub art. 25 ustawy) przez podmioty zajmujące się sprzedażą swoich produktów i usług w tzw. „systemie wysyłkowym” posiadające siedzibę poza terytorium Polski. Podmioty te unikały przekazywania informacji o dokładnym adresie siedziby, czy źródle pozyskania danych, co uniemożliwiało skarżącym realizację

zagwarantowanych im ustawą uprawnień, np. skuteczne sprzeciwianie się dalszemu wykorzystywaniu ich danych. Nie dysponując innymi środkami, które skłoniłyby takie podmioty do podjęcia czynności zmierzających do usunięcia występujących w ich działaniach nieprawidłowości, Generalny Inspektor składał zawiadomienie o popełnieniu przestępstwa do właściwych organów ścigania.

W 2006 r. do Generalnego Inspektora wpłynęło 712 **skarg** dotyczących naruszenia przepisów o ochronie danych osobowych. Liczba ta zatem zmniejsza się od 2004 r., co obrazuje *Wykres 8*. Zwiększeniu zaś uległa liczba decyzji wydanych w latach 2004–2006 w związku z rozpatrywanymi skargami (zob. *Wykres 9*).



Wykres 8: Liczbowe zestawienie skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004–2006.



Wykres 9: Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2004–2006 w związku z rozpatrywanymi skargami.

Zakres przedmiotowy skarg zgłoszonych Generalnemu Inspektorowi najczęściej dotyczył: dopuszczalności przetwarzania danych osobowych przy braku wyrażenia zgody na powyższe,

kwestionowania zgodności z prawem pozyskania i dalszego przetwarzania danych osobowych skarżącego ze względu na brak zgody, nie zapewnienia przez administratorów danych osobowych opcjonalności wyrażania zgody na przetwarzanie danych, niewłaściwe wypełnianie przez administratorów danych obowiązku informacyjnego, powstającego z chwilą pozyskania danych, udostępnianie danych osobowych osobom nieupoważnionym.

Zakres podmiotowy skarg najczęściej kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w 2006 roku obejmował w kolejności następujące obszary:

1) Administracja publiczna, 2) Bezpieczeństwo publiczne, 3) Sądy, organy prokuratury, komornicy, 4) Organizacje społeczne, 5) Banki i inne instytucje finansowe, 6) Internet, 7) Marketing, 8) Sektor mieszkalnictwa, 9) Oświata, 10) Służba zdrowia, 11) Ubezpieczenia społeczne, majątkowe, osobiste, 12) Telekomunikacja, 13) Sektor zatrudnienia, 14) Windykacja, 15) Inne.

1) Administracja publiczna

Jednym z częściej odnotowywanych naruszeń przepisów ustawy jakich dopuszczają się organy administracji publicznej jest nieprawidłowe wykorzystywanie danych pozyskanych w związku z postępowaniem administracyjnym, udostępnianie danych osobom nieupoważnionym²³ oraz błędna interpretacja przepisów ustawy o ochronie danych osobowych. Wskazywano na ujawnienie danych osobowych w toku postępowania administracyjnego, czy skargowego przez urzędników gminnych, starostów i prezydentów miast.²⁴ Kwestionowano różne formy udostępniania danych stronom postępowania toczącego się z udziałem skarżących, podważano legalność pozyskania danych dla potrzeb postępowań prowadzonych przez organy administracji, a także legalność umieszczania danych osobowych w treści,²⁵ czy w rozdzielniku decyzji administracyjnej.²⁶

Organy administracji publicznej w sposób niewłaściwy interpretowały też przesłankę zgody na przetwarzanie danych. Uznawały bowiem tę przesłankę za konieczną w sytuacjach, gdy pozyskanie, gromadzenie i udostępnianie danych wprost wynika z istniejących odrębnych przepisów prawa. Jednym z wielu przykładów tego rodzaju spraw jest skarga na Miejski Ośrodek Pomocy Społecznej, który pozyskiwał zgody na przetwarzanie danych dla potrzeb rodzinnego wywiadu środowiskowego

²³ GI-DS-430/265/06, GI-DS-430/382/06, GI-DS-430/418/06, GI-DS-430/462/06, GI-DS-430/452/06, GI-DS-430/473/06, GI-DS-430/493/06, GI-DS-430/517/06, GI-DS-430/521/06, GI-DS-430/527/06, GI-DS-430/558/06, GI-DS-430/559/06, GI-DS-430/580/06, GI-DOLiS-430/21/06, GI-DOLiS-430/22/06, GI-DOLiS-430/32/06, GI-DOLiS-430/36/06, GI-DOLiS-430/54/06, GI-DOLiS-430/80/06, GI-DOLiS-430/83/06, GI-DOLiS-430/84/06, GI-DOLiS-430/85/06, GI-DOLiS-430/86/06, GI-DOLiS-430/87/06, GI-DOLiS-430/96/06, GI-DOLiS-430/114/06, GI-DOLiS-430/115/06.

²⁴ Przykładem sprawy, w której przetwarzanie danych osobowych wynikało z przepisów prawa była skarga dotycząca przetwarzania danych osobowych spadkobiercy członka gminnej spółki wodnej celem odzyskania składek i należności na rzecz spółki (GI-DS-430/50/06), które to przetwarzanie jest dopuszczalne na podstawie art. 23 ust. 1 pkt 2 w zw. z art. 165 ust. 7 ustawy z dnia 18 lipca 2001 r. Prawa wodne (tekst jednolity Dz. U. z 2005 r. Nr 239, poz. 2019 ze zm.), zgodnie z którym następca prawny członka spółki wodnej wstępuje w jego prawa i obowiązki.

²⁵ GI-DS-430/344/06.

²⁶ GI-DS-430/371/06.

w postępowaniu o przyznanie świadczeń z tytułu pomocy społecznej. GIODO uznał,²⁷ iż działania takie są zbędne z punktu widzenia ustawy o ochronie danych osobowych, a także wprowadzają osoby zainteresowane uzyskaniem pomocy w błąd, co do skuteczności ich oświadczeń woli. Z tych względów GIODO zwrócił się do Ośrodka o zaprzestanie pozyskiwania zgód na przetwarzanie danych osobowych w celu przeprowadzenia wywiadu środowiskowego, ponieważ wystarczającą podstawę przetwarzania danych dla potrzeb jego przeprowadzenia stanowią przepisy prawa.²⁸

W innej sprawie Generalny Inspektor zakwestionował dopuszczalność udostępnienia przez Urząd Pracy danych osobowych bezrobotnych o znacznym i umiarkowanym stopniu niepełnosprawności, w zakresie obejmującym imię, nazwisko i adres zamieszkania. Dane te miały być wykorzystane przez podmiot prywatny do badań w celu rozpoznania potrzeb osób niepełnosprawnych. Generalny Inspektor uznał, że prowadzone przez podmiot prywatny badania nie mają znamion badania naukowego, które by uzasadniały możliwość i legalność udostępnienia ww. danych osobowych w oparciu o art. 26 ust. 2 pkt 1 ustawy o ochronie danych osobowych.

2) Bezpieczeństwo publiczne

W analizowanym 2006 roku, organ ds. ochrony danych osobowych rozpatrywał zagadnienie odnoszące się do przetwarzania danych przez organy ścigania w postaci odmowy usunięcia przez Policję danych osobowych skarżącego z prowadzonego przez nią zbioru pod nazwą „Ewidencja kierowców naruszających przepisy ruchu drogowego”.²⁹ Dane w zakresie imienia, nazwiska, imion rodziców, nazwiska panińskiego matki, daty urodzenia i numeru PESEL osoby skarżącej, w wyniku spowodowanego przez nią wykroczenia zostały wstępnie umieszczone w ewidencji w postaci wpisu tymczasowego. Zaś po uprawomocnieniu się wyroku wydanego przez sąd w związku z zaistnieniem przedmiotowego zdarzenia status wpisu został zmieniony stając się wpisem ostatecznym. Żądanie skarżącego dotyczące usunięcia ww. danych osobowych było nieuzasadnione, albowiem zebranie i dalsze przetwarzanie przedmiotowych danych osobowych przez Policję znajdowało umocowanie w obowiązujących przepisach prawa,³⁰ określających w sposób szczegółowy zasady prowadzenia „Ewidencji kierowców naruszających przepisy ruchu drogowego” oraz umieszczania w niej wpisów tymczasowych i ostatecznych.³¹ W świetle tych regulacji brak było podstaw do stwierdzenia, że Policja

²⁷ Pismo z dnia 13 września 2006 r., znak: GI-DS-430/262/06/3992.

²⁸ Por. art. 107 ustawy o pomocy społecznej.

²⁹ GI-DS-430/151/06.

³⁰ W szczególności w ustawie z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. z 2005 r. Nr 108, poz. 908 ze zm.) oraz w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 20 grudnia 2002 r. w sprawie postępowania z kierowcami naruszającymi przepisy ruchu drogowego (Dz. U. Nr 236, poz. 1998 ze zm.).

³¹ Stosownie do § 2 ust. 1 rozporządzenia w sprawie postępowania z kierowcami naruszającymi przepisy ruchu drogowego, do ewidencji kierowców naruszających przepisy ruchu drogowego, zwanej dalej „ewidencją”, wpisuje się kierowcę, który kierując pojazdem dopuścił się naruszenia przepisów ruchu drogowego, zwanego dalej „naruszeniem”. Wpisu ostatecznego do ewidencji dokonuje się, z zastrzeżeniem ust. 2 i 3, jeżeli naruszenia zostaną stwierdzone prawomocnymi wyrokami sądów, postanowieniami sądu o warunkowym umorzeniu postępowania albo nakazami lub mandatami karnymi (§ 4 ust. 1

postępowała w sposób sprzeczny z wyznaczonymi zasadami, umieszczając w ewidencji kwestionowane wpisy. Mając natomiast na uwadze fakt, że wpis tymczasowy stał się wpisem ostatecznym, a w tym przypadku obowiązuje określony termin do usunięcia danych o tego rodzaju statusie,³² uzasadniona była w momencie wydawania decyzji odmowa nakazania usunięcia danych skarżącego z prowadzonej ewidencji.³³

W innej sprawie z zakresu bezpieczeństwa publicznego³⁴ skarżący zakwestionował legalność pozyskania przez Policję odcisków jego linii papilarnych oraz zdjęć sygnalitycznych, a następnie wykorzystania tych danych w innych sprawach. Zarzucił również, iż Policja działała niezgodnie z prawem odmawiając udzielenia mu pełnych informacji o okolicznościach przetwarzania jego danych osobowych, o które skarżący zwrócił się na podstawie art. 33 ustawy. Z dokonanych w sprawie ustaleń wynikało, że dane osobowe skarżącego, w tym odciski linii papilarnych oraz zdjęcia sygnalityczne zostały pobrane przez organy ścigania od skarżącego, jako osoby podejrzanej. W odpowiedzi na wniosek skarżącego o udzielenie mu informacji odnośnie przetwarzania jego danych w zakresie odcisków linii papilarnych oraz zdjęć został on jedynie poinformowany o zarejestrowaniu jego danych przez organy ścigania w postaci karty daktyloskopijnej oraz zdjęć sygnalitycznych. Jednocześnie odmówiono przekazania skarżącemu szczegółowych informacji na ten temat. W wydanej w tej sprawie decyzji administracyjnej³⁵ nie uwzględniono wniosku skarżącego wskazując, że działania organu Policji znajdowały umocowanie w przepisach prawa.³⁶ Jednocześnie, ze względu na ograniczenia w udostępnianiu danych osobowych przewidziane w art. 30 ust. 2 ustawy, tj. zagrożenie dla bezpieczeństwa i porządku publicznego oraz okoliczność, że organy ścigania miały prawo do przetwarzania kwestionowanych danych bez zgody skarżącego,³⁷ odmowa udzielenia mu żądanych informacji była uzasadniona.

rozporządzenia). Zgodnie z ust. 2 wymienionego przepisu, dopuszcza się dokonanie wpisu tymczasowego do ewidencji przed wydaniem rozstrzygnięcia, o którym mowa w ust. 1, jeżeli po ujawnieniu naruszenia wszczęto postępowanie przygotowawcze lub skierowano wniosek o ukaranie do sądu albo skierowano sprawę do organu właściwego do uchylenia immunitetu parlamentarnego, sędziowskiego lub prokuratorskiego. Wpis tymczasowy zawiera informację o liczbie punktów, które zostaną przypisane w przypadku potwierdzenia naruszenia prawomocnym orzeczeniem. Z kolei ust. 4 omawianego przepisu stanowi, że wpis tymczasowy staje się wpisem ostatecznym po stwierdzeniu naruszenia odpowiednim rozstrzygnięciem, o którym mowa w ust. 1.

³² Zgodnie z § 5 ust. 2 przytoczonego rozporządzenia, organ prowadzący ewidencję usuwa z ewidencji wpis ostateczny dotyczący naruszeń, jeżeli nastąpiło zatarcie ukarania (skazania). Z kolei, zgodnie z art. 46 § 1 ustawy z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz. U. Nr 12, poz. 114 ze zm.), ukaranie uważa się za niebyłe po upływie 2 lat od wykonania, darowania lub przedawnienia wykonania kary.

³³ Decyzja z dnia 20 czerwca 2006 r. o sygn. GI-DEC-DS-232/06.

³⁴ GI-DS-430/181/06.

³⁵ Decyzja z dnia 4 września 2006 r. o sygn. GI-DEC-DS-341/06.

³⁶ W tym przypadku zastosowanie miały bowiem przepisy ustawy o Policji, na podstawie których organy Policji mogą pobierać, przetwarzać i wykorzystywać w celach wykrywczych i identyfikacyjnych informacje, w tym dane osobowe m.in. o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, takie jak odciski linii papilarnych czy zdjęcia i opisy wizerunku.

³⁷ Art. 20 ustawy o Policji.

Pośród spraw dotyczących **Straży Miejskich** odnotowano skargę na odmowę udostępnienia temu podmiotowi przez ZUS danych osobowych w zakresie miejsca zatrudnienia osoby fizycznej.³⁸ Tego typu zdarzenia nie były we wcześniejszych latach sygnalizowane GIODO. Celem pozyskania danych przez Straż Miejską było skuteczne zainicjowanie przeciwko osobie, której dane dotyczyły postępowania sądowego w sprawie o wykroczenie. Wniosek o ukaranie skierowany przez Straż do sądu grodzkiego nie spełniał wymogów formalnych ponieważ nie zawierał wskazania miejsca zatrudnienia obwinionego.³⁹ Wniosek ten został zwrócony przez sąd, celem uzupełnienia pisma, dlatego też Straż wystąpiła do ZUS o udostępnienie ww. zakresu danych. Zakład odmówił udostępnienia danych powołując się na ograniczenia wynikające z wiążących go przepisów prawa, w szczególności ze względu na tzw. tajemnicę ubezpieczeniową.⁴⁰ Przepis prawa, regulujący kwestię udostępniania przez ZUS danych zgromadzonych na koncie ubezpieczonego oraz na koncie płatnika wprowadza zamknięty katalog podmiotów, którym dane mogą być udostępnione. Pośród podmiotów tych nie są wymienione straże gminne (miejskie), ani ich organy. Ze skargą na odmowę udostępnienia danych Straż Miejska zwróciła się więc do GIODO wnosząc o nakazanie ZUS udostępnienia danych. GIODO rozstrzygając sprawę przychylił się do stanowiska ZUS i przyjął, iż odmowa była uzasadniona i świadczyła o właściwej dbałości administratora danych o ochronę tajemnicy ubezpieczeniowej.⁴¹

3) Sądy, organy prokuratury, komornicy

Podobnie jak miało to miejsce w latach ubiegłych, najczęstszym przedmiotem zarzutów było udostępnianie danych osobowych z akt prowadzonych postępowań osobom nieupoważnionym,⁴² odmowę ich udostępnienia,⁴³ gromadzenie w aktach postępowań danych osobowych, w tym danych szczególnie chronionych⁴⁴ mimo, że powyższe działania były konsekwencją stosowania przez Policję, sądy i prokuraturę odrębnych procedur. Nie odnotowano natomiast skarg na niewłaściwe zabezpieczanie danych osobowych przez ww. podmioty, co może być rezultatem prowadzonych przez GIODO szkoleń i kontroli w tym sektorze w poprzednich latach.

Na poprawę przestrzegania przepisów ustawy należy wskazać w przypadku komorników sądowych. Wiele z wcześniej stwierdzanych naruszeń, np. udostępnianie w toku prowadzonych

³⁸ GI-DS-430/310/06.

³⁹ Art. 57 § 3 pkt 2 Kodeksu postępowania w sprawach o wykroczenia.

⁴⁰ Art. 50 ust. 3 ustawy o systemie ubezpieczeń społecznych stanowi, że dane zgromadzone na koncie ubezpieczonego, o których mowa w art. 40, i na koncie płatnika składek, o których mowa w art. 45, mogą być udostępniane sądom, prokuratorom, organom kontroli skarbowej, organom podatkowym, komornikom sądowym, ośrodkom pomocy społecznej, powiatowym centrom pomocy rodzinie oraz Komisji Nadzoru Finansowego, z uwzględnieniem przepisów dotyczących ochrony danych osobowych.

⁴¹ Decyzja z dnia 29 grudnia 2006 r. o sygn. GI-DEC-DOLiS-459/06.

⁴² GI-DS-430/375/06.

⁴³ GI-DS-430/99/06.

⁴⁴ GI-DS-430/215/06.

postępowań egzekucyjnych danych osobowych osobom nieupoważnionym, w szczególności poprzez podawanie ich do publicznej wiadomości w różnego rodzaju obwieszczeniach, czy zbieranie przez komorników danych osobowych w szerszym zakresie, niż to wynika z przepisów prawa uległo całkowitemu wyeliminowaniu.

Jako przykład sprawy z opisywanego sektora, odnoszącej się do przetwarzania danych przez sądy, można wskazać skargę na odmowę udostępnienia PZU S.A. przez sąd rejonowy danych osobowych nieletniego sprawcy czynu karalnego.⁴⁵ PZU S.A. zwróciła się do sądu o przesłanie prawomocnego wyroku w prowadzonej przez ten sąd sprawie oraz podanie adresu zamieszkania skazanego, uzasadniając swoje żądanie koniecznością wystąpienia na drogę sądową z roszczeniem regresowym wobec tej osoby. Sąd odmówił, co stało się przyczyną złożenia przez PZU S.A. skargi do GODO z wnioskiem o nakazanie udostępnienia całych akt prowadzonej wobec ww. osoby sprawy i zawartych tam danych. Zdaniem Generalnego Inspektora,⁴⁶ o ile podstawę do uzyskania przez PZU S.A. od sądu danych sprawcy przestępstwa w zakresie: imię, nazwisko i adres zamieszkania w celu zainicjowania wobec niego postępowania sądowego stanowił art. 23 ust. 1 pkt 2 i art. 5 ustawy⁴⁷, to udostępnienie PZU S.A. całych akt przedmiotowej sprawy nie znajdowało uzasadnienia w obowiązujących przepisach prawa, gdyż spółka ta nie posiadała statusu strony postępowania toczącego się z udziałem sprawcy.⁴⁸

Inna z rozpatrywanych spraw wiązała się z kolei z zakwestionowaniem przez osobę skarżącą wypełnienia wobec niej przez sąd obowiązku informacyjnego⁴⁹. Skarżący zwrócił się do sądu o przekazanie mu informacji dotyczących przetwarzania jego danych osobowych, w tym również o podanie dat rozpraw oraz sygnatur spraw, w których orzekał jako ławnik. Sąd udzielił zainteresowanemu informacji odnoszących się do jego osoby, z wyjątkiem informacji o datach rozpraw i sygnaturach akt - co stało się powodem złożenia skargi do GODO. Przeprowadzone postępowanie, potwierdziło, że sąd prawidłowo wypełnił względem skarżącego obowiązek informacyjny wskazując na piśmie, stosownie do przepisów art. 32 i art. 33 ustawy i zgodnie z żądaniem, jakie dane go dotyczące zawiera prowadzony zbiór, w jaki sposób dane te zostały zebrane, od kiedy, w jakim celu i zakresie są one przetwarzane. Natomiast na sądzie nie spoczywał obowiązek udzielenia skarżącemu informacji w zakresie dat rozpraw, w których orzekał oraz sygnatur tych spraw, bowiem tego typu

⁴⁵ GI-DS-430/99/06.

⁴⁶ Sprawa zakończyła się wydaniem decyzji administracyjnej z dnia 12 lipca 2006 r. o sygn. GI-DEC-DS-258/06.

⁴⁷ W szczególności przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 ze zm.) oraz przepisy ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. Nr 124, poz. 1151 ze zm.).

⁴⁸ W szczególności w ustawie z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (tekst jednolity: Dz. U. z 2002 r. Nr 11, poz. 109 ze zm.), enumeratywnie wyliczającej krąg osób, mających dostęp do akt sprawy oraz określającej warunki tego dostępu.

⁴⁹ GI-DS-430/895/05.

informacji nie można zaliczyć do kategorii danych osobowych w rozumieniu ustawy.⁵⁰ Wojewódzki Sąd Administracyjny w Warszawie potwierdził stanowisko GODO w przedmiotowej sprawie.⁵¹

W 2006 r. rozpatrywana była również skarga, w której zarzucono, że sędzia sądu rejonowego włączyła część akt sprawy karnej, zawierających dane osobowe skarżącego, w tym dane o stanie zdrowia do akt innej sprawy, a tym samym doszło do udostępnienia danych osobowych osobom nieupoważnionym.⁵² Generalny Inspektor uznając, że przetwarzanie danych skarżącego odbywało się w oparciu o przesłankę wynikającą z art. 23 ust. 1 pkt 2 oraz art. 27 ust. 2 pkt 2 ustawy – w zakresie danych sensytywnych, wskazał jednocześnie, że nie jest w żaden sposób organem upoważnionym do badania zasadności postanowień dowodowych wydawanych przez sądy.⁵³ Rola organu administracji publicznej, jakim jest GODO, kończy się bowiem na stwierdzeniu istnienia podstawy prawnej do przetwarzania danych osobowych, natomiast sama celowość takiego przetwarzania będącego następstwem wydanych w sprawie cywilnej postanowień dowodowych podlega wyłącznie ocenie sądu.

W roku sprawozdawczym 2006, skarżono się również na działania komorników sądowych. Przykładem sprawy z tego zakresu była skarga na bezprawne przetwarzanie przez komornika danych osobowych skarżącej w toku prowadzonej egzekucji.⁵⁴ Jak ustalono, skarżony komornik działając w oparciu o tytuł wykonawczy, czyli wyrok sądu prowadził przeciwko skarżącej postępowanie egzekucyjne z wniosku wierzyciela - spółdzielni mieszkaniowej, której skarżąca była członkiem. W ramach i na potrzeby postępowania egzekucyjnego komornik udostępnił dane skarżącej ZUS, który jest podmiotem dokonującym potrąceń z przysługującego skarżącej świadczenia emerytalno-rentowego, jak również sądom i Policji. Działaniom tym nie można było jednak przypisać cech bezprawności, bowiem były one podejmowane na podstawie powszechnie obowiązujących przepisów prawa,⁵⁵ a więc wypełniały przesłankę określoną w art. 23 ust. 1 pkt 2 ustawy. GODO nie podzielając zatem zarzutów skarżącej w zakresie związanym z przetwarzaniem przez komornika jej danych osobowych⁵⁶ podkreślił jednocześnie, że czynności komorników, w związku z wypełnianiem przez nich prawem nałożonych zadań podlegają ocenie sądu, a nie organu ds. ochrony danych osobowych.⁵⁷

⁵⁰ Decyzją z dnia 31 marca 2006 r. o sygn. GI-DEC-DS-107/06, utrzymaną w mocy decyzją z dnia 28 czerwca 2006 r. o sygn. GI-DEC-DS-220/06 odmówiono skarżącemu uwzględnienia jego wniosku.

⁵¹ Sygn. akt: II SA/Wa 1526/06.

⁵² GI-DS-430/215/06.

⁵³ Decyzją z dnia 22 czerwca 2006 r. o sygn. GI-DEC-DS-204/06 utrzymana w mocy decyzją z dnia 16 sierpnia 2006 r. o sygn. GI-DEC-DS-301/06.

⁵⁴ GI-DS-430/400/06.

⁵⁵ Przepisów Kodeksu postępowania cywilnego oraz przepisów ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (tekst jednolity: Dz. U. z 2004 r. Nr 39, poz. 353 ze zm.).

⁵⁶ Decyzją z dnia 29 grudnia 2006 r. o sygn. GI-DEC-DOLiS-458/06 odmówiono skarżącemu uwzględnienia jego wniosku.

⁵⁷ Zgodnie z art. 767 § 1 Kodeksu postępowania cywilnego, na czynności komornika przysługuje skarga do sądu rejonowego, przy którym działa komornik.

Kwestionowano także niedochowanie należytej staranności przez komornika sądowego przy doręczaniu korespondencji dłużnikowi.⁵⁸ Komornik, nie zastawszy adresata pozostawił pismo w drzwiach wejściowych, przy czym nie było ono w żaden sposób zabezpieczone, np. poprzez umieszczenie w zaklejonej kopercie. GODO uznając, że taki sposób doręczania korespondencji sprzeciwia się zasadom określonym w przepisach prawa,⁵⁹ a ponadto stwarza zagrożenie ujawnienia zawartych w niej danych osobowych osobom nieupoważnionym wystosował do prezesa sądu, przy którym działał wskazany w skardze komornik pismo sygnalizacyjne, ze wskazaniem na konieczność wyeliminowania tego rodzaju praktyk. W odpowiedzi poinformowano, że podlegli sądowi komornicy otrzymali polecenie przestrzegania przepisów prawa we wskazanym zakresie.⁶⁰

4) Organizacje społeczne

Spośród skarg na przetwarzanie danych osobowych przez **organizacje społeczne** odnotowano sprawę wykorzystania danych osobowych członka stowarzyszenia w celach niezwiązanych z działalnością statutową tego stowarzyszenia.⁶¹ Skarżący otrzymał przesyłkę zawierającą list agitacyjny i ulotkę wyborczą, powiadamiające go o kandydowaniu przez innego członka stowarzyszenia w wyborach parlamentarnych w 2006 r. Do udostępnienia danych adresowych skarżącego kandydatowi do Sejmu RP, w celu wykorzystania ich dla marketingu politycznego doszło, choć stowarzyszenie nie dysponowało zgodą skarżącego, ani inną z przesłanek określonych w art. 23 ust. 1 ustawy. W tym przypadku nie było wątpliwości, iż przedmiotowe dane zostały wykorzystane niezgodnie z celami, dla których zostały zebrane, określonymi w statucie stowarzyszenia, a zatem również z naruszeniem art. 26 ust. 1 pkt 2 ustawy. W tej sytuacji koniecznym było nakazanie stowarzyszeniu zaprzestania przetwarzania danych osobowych skarżącego w celach innych niż te, dla których zostały pierwotnie pozyskane.⁶²

W 2006 roku Wojewódzki Sąd Administracyjny w Warszawie wydał rozstrzygnięcie,⁶³ w którym przychylił się do stanowiska GODO prezentowanego w jednej z rozpatrywanych w roku poprzednim spraw,⁶⁴ iż fundacja, której statutową działalnością jest ochrona zwierząt, żądając od innej fundacji, prowadzącej schronisko dla bezdomnych zwierząt, udostępnienia jej danych osobowych osób, którym przekazano zwierzęta w tzw. trybie adopcji, w celu sprawdzenia dalszego losu bezdomnych zwierząt, nie legitymuje się żadną z przesłanek dopuszczalności przetwarzania danych osobowych. Za taką podstawę nie może być w szczególności uznany art. 23 ust. 1 pkt 2 ustawy, bowiem z przepisów

⁵⁸ GI-DS-430/65/06.

⁵⁹ Tj. ustawy o komornikach sądowych i egzekucji oraz rozporządzenia w sprawie czynności komorników.

⁶⁰ Pismo z dnia 11 lipca 2006 r. o sygn. AII 084-63/06.

⁶¹ GI-DS-430/790/05.

⁶² Decyzja administracyjna z dnia 4 maja 2006 r. o sygn. GI-DEC-DS-139/06.

⁶³ Wyrok WSA w Warszawie z dnia 28 września 2006 r. (sygn. akt: II SA/Wa 898/06), prawomocny od 16 grudnia 2006 r.

⁶⁴ GI-DS-430/315/05.

prawa nie wynika, iż fundacje posiadają jakiekolwiek uprawnienia kontrolne w ww. zakresie,⁶⁵ a w konsekwencji prawo do pozyskiwania tego rodzaju danych. W tym przypadku zastosowania nie znalazł również art. 23 ust. 1 pkt 5 ustawy, gdyż o usprawiedliwionym celu administratora danych można jedynie mówić wówczas, gdy został on uprzednio określony w akcie normatywnym, a tak się w rozpatrywanej sytuacji nie stało. Sąd uznał również, że przeszkodą pozyskania danych na podstawie ww. przepisu była możliwość naruszenia w tym przypadku praw i wolności osób, których dane dotyczyły.

Z kolei, zawiadomieniem organów ścigania o popełnieniu przestępstwa zakończyła się sprawa, gdzie doszło do udostępnienia na rzecz osób trzecich przez jedno ze stowarzyszeń danych osobowych skarżącej członkom tego stowarzyszenia i jednocześnie umożliwienia dostępu do nich szerszemu kręgowi osób nieuprawnionych.⁶⁶ Ze skargi wynikało, że stowarzyszenie przesłało mieszkańcom osiedla, na którym zamieszkuje skarżąca, protokół z zebrania jego członków, w którego treści zamieszczone zostały m.in. dane osobowe skarżącej obejmujące jej imię i nazwisko, adres oraz informację o zaleganiu przez nią z opłatami czynszowymi. Ponadto skarżąca podniosła zarzut nieprawidłowego doręczania jej przez stowarzyszenie korespondencji, wskazując, że pisma kierowane przez to stowarzyszenie zostawiane są w drzwiach wejściowych, co umożliwia dostęp do ich treści osobom trzecim. W tej sytuacji istniało uzasadnione podejrzenie wypełnienia przez osoby odpowiedzialne w stowarzyszeniu za przetwarzanie danych osobowych skarżącej znamion przestępstwa określonego w art. 51 ustawy. Prokuratura nie podzieliła jednak zarzutów GODO, umarzając przeprowadzone w niniejszej sprawie śledztwo.⁶⁷

W 2006 r. stowarzyszenia zwracały się do Generalnego Inspektora z pytaniami, czy mają obowiązek zgłosić do rejestracji zbiory wyroków zasądzających nawiązkę na rzecz stowarzyszenia w stosunku do sprawcy wykroczenia bądź przestępstwa.⁶⁸ Zbiory takie podlegają zgłoszeniu do rejestracji, nie zachodzi bowiem żadna z przesłanek zwalniających stowarzyszenia z powyższego obowiązku spośród wskazanych w art. 43 ust. 1 ustawy.

Fundacja Rozwoju Rolnictwa i Gospodarki Żywnościowej, która w zakresie swojej działalności statutowej udziela pożyczek rolnikom i grupom producenckim miała wątpliwości, czy Ministerstwo Rolnictwa i Rozwoju Wsi nadzorujące Fundację może żądać od niej przekazania imiennego wykazu wszystkich pożyczkobiorców i wielkości kwot udzielonych pożyczek.⁶⁹ Podstawę udostępnienia danych stanowią w tym przypadku przepisy ustawy o fundacjach oraz wydane na jej podstawie akty wykonawcze, w szczególności rozporządzenie Ministra Sprawiedliwości z dnia 8 maja

⁶⁵ Z ustawy z dnia 21 sierpnia 1997 r. o ochronie zwierząt (Dz. U. z 2003 r. Nr 106 poz. 1002 ze zm.) wynika bowiem, że organem uprawnionym do kontroli wykonywania przepisów ww. ustawy jest wyłącznie Inspekcja Weterynaryjna.

⁶⁶ GI-DS-430/20/06.

⁶⁷ Zawiadomienie z dnia 19 października 2006 r. o sygn. 4 Ds. 439/06/V.

⁶⁸ GI-DP-024/2/06, GI-DP-024/116/06.

2001 r. w sprawie ramowego zakresu sprawozdania z działalności fundacji (Dz. U. Nr 50, poz. 529). Na podstawie art. 12 ust. 2 ustawy o fundacjach, fundacja składa corocznie właściwemu ministrowi (jako organowi nadzorującemu) sprawozdanie ze swojej działalności. Zgodnie z § 2 rozporządzenia w sprawie ramowego zakresu sprawozdania z działalności fundacji, sprawozdanie powinno zawierać m.in. informacje o udzielonych przez fundację pożyczkach pieniężnych, z podziałem według ich wysokości, ze wskazaniem pożyczkobiorców i warunków przyznania pożyczek oraz z podaniem podstawy statutowej ich udzielania. (§ 2 pkt 7 lit. e). Są to zatem informacje jawne dla organu nadzorującego fundację, na mocy wskazanych powyżej przepisów.

W 2006 r. zaistniał także zgłaszany już w roku 2005 problem ujawnienia list współpracowników Służby Bezpieczeństwa⁷⁰ przez stowarzyszenia zrzeszające m.in. osoby poszkodowane w rozumieniu przepisów ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz. U. z 2007 r. Nr 63, poz. 1016, poz. 424). Osoby pokrzywdzone miały na mocy art. 30 ust. 1 tej ustawy prawo dostępu do danych osobowych funkcjonariuszy, pracowników, współpracowników organów bezpieczeństwa państwa, którzy zbierali lub oceniali dane o nich lub „prowadzili” tych współpracowników, jeśli można je jednoznacznie określić na podstawie dokumentów danego organu bezpieczeństwa. Przepis ten stosowany był również do innych osób, które denuncjowały pokrzywdzonego (art. 32 ust. 1). Osoby pokrzywdzone mogą swobodnie dysponować wiedzą pozyskaną z udostępnionych im przez Instytut Pamięci Narodowej dokumentów. Zaznaczenia wymaga, iż przepis art. 30 ust. 1 powołanej wyżej ustawy, został zmieniony ustawą z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990 oraz treści tych dokumentów (Dz. U. Nr 63, poz. 425), która weszła w życie 15 marca 2007 r. Przepis ten w obecnie obowiązującym brzmieniu stanowi, iż każdy ma prawo wystąpić z wnioskiem do Instytutu Pamięci o udostępnienie do wglądu kopii dotyczących go dokumentów.

Stowarzyszenie skupiające osoby represjonowane w stanie wojennym chciało pozyskać od Instytutu Pamięci Narodowej imiona i nazwiska osób internowanych w stanie wojennym i osadzonych w jednym z zakładów karnych.⁷¹ Generalny Inspektor wskazał, iż dopuszczalność udostępnienia przedmiotowych informacji powinna być rozpatrywana wyłącznie na gruncie art. 36 ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu. Zgodnie z treścią tego przepisu, dokumenty zawierające dane o pokrzywdzonych lub osobach trzecich mogą być, w niezbędnym zakresie i w sposób nie naruszający praw tych osób, wykorzystywane przez organy władzy publicznej oraz przez inne instytucje, organizacje i osoby w celach prowadzenia badań

⁶⁹ GI-DP-024/1069/06.

⁷⁰ GI-DP-024/723/06.

⁷¹ GI-DP-024/468/06.

naukowych, o ile Prezes Instytutu Pamięci wyrazi na to zgodę (pkt 5). Zatem organem właściwym do rozstrzygania o udostępnieniu danych zawartych w powyższych dokumentach jest Prezes Instytutu Pamięci Narodowej.

5) Banki i inne instytucje finansowe

Jedną z największych grup stanowiły skargi na podmioty z sektora bankowości. Sporna od wielu lat pozostaje kwestia udostępniania danych osobowych Biuru Informacji Kredytowej S.A. [zwane dalej: BIK S.A.] i Związkowi Banków Polskich [zwany dalej ZBP].

W omawianym okresie sprawozdawczym 2006 roku, wątpliwości budziła interpretacja powoływanego przez banki i BIK S.A. okresu przejściowego⁷² dla zastosowania wprowadzonych w życie nowych przepisów prawa bankowego,⁷³ nakładających na banki obowiązek spełnienia określonych ściśle przesłanek w przypadku przetwarzania danych osobowych rzetelnych i nierzetelnych klientów po wygaśnięciu łączących ich z bankami zobowiązań. Ostatecznie o zasadności stanowiska GODO przesądził WSA w Warszawie wskazując, iż przepis ten nie może być traktowany jako regulacja dająca prawo do przetwarzania danych osobowych w terminie 3 lat osób terminowo wywiązujących się z zaciągniętych wobec banków zobowiązań, bez ich zgody, w momencie gdy występują z żądaniem usunięcia danych z baz BIK. Trzyletni okres dostosowawczy potraktować należy jako czas, który ustawodawca przewidział do zweryfikowania bazy dotyczącej wszystkich klientów banku.⁷⁴

Analiza spraw z tego sektora wskazuje, iż banki nadal mają trudności z właściwym formułowaniem klauzul zgód na przetwarzanie danych osobowych, uzależniając zgodę na przetwarzanie danych w celach realizacji umów od zgody na przetwarzanie danych w celach

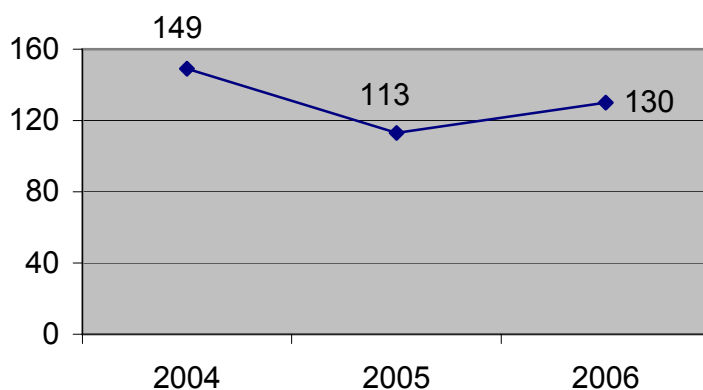
⁷² Art. 6 ustawy z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 727), z którego wynika, że banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4 ustawy Prawo bankowe obowiązane są dostosować przetwarzanie informacji zgromadzonych przed dniem wejścia w życie niniejszej ustawy do wymagań w niej określonych, w terminie nie dłuższym niż 3 lata od wejścia w życie niniejszej ustawy.

⁷³ Zgodnie z art. 105 a ust 2 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. poz. 72 ze zm.) w brzmieniu obowiązującym do 31 grudnia 2006 r. instytucje, o których mowa w ust. 1, mogą z zastrzeżeniem ust. 3, przetwarzać informacje stanowiące tajemnicę bankową w zakresie dotyczącym osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, pod warunkiem uzyskania pisemnej zgody osoby, której informacje te dotyczą. Zgoda ta może być w każdym czasie odwołana. Zgodnie natomiast z art. 105 a ust. 3 ww. ustawy instytucje, o których mowa w ust. 1, mogą przetwarzać informacje stanowiące tajemnicę bankową dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby przez bank lub inną instytucję upoważnioną do udzielania kredytów o zamiarze przetwarzania dotyczących jej informacji stanowiących tajemnicę bankową bez jej zgody.

⁷⁴ Zob. decyzja z dnia 4 maja 2006 r., znak: GI-DEC-DS-141/06 w sprawie GI-DS-430/638/05; decyzja z dnia 25 maja 2006 r., znak: GI-DEC-DS-169/06 w sprawie GI-DS-430/877/05; decyzja z dnia 30 czerwca 2006 r., znak: GI-DEC-DS-230/06 w sprawie GI-DS-430/83/06.

marketingowych oraz niewłaściwie wypełniają obowiązki informacyjne.⁷⁵ Nie stwierdzono natomiast nieprawidłowości w przypadku skarg na udostępnienie danych w celach dochodzenia wierzytelności przez banki,⁷⁶ gdyż następowało ono albo w trybie powierzenia przetwarzania danych⁷⁷ albo w ramach sprzedaży wierzytelności na podstawie przepisów prawa.⁷⁸

Efekty przeprowadzonych wobec banków postępowań administracyjnych wskazują, iż podmioty te dążą do zapewnienia większego bezpieczeństwa przetwarzanym danym osobowym w systemach informatycznych, choć nadal istniejący brak skorelowania systemów informatycznych banków oraz instytucji, takich jak BIK i ZBP powoduje, iż w systemach tych ostatnich figurują dane nieaktualne, co ma zasadniczy wpływ na ocenę sytuacji kredytowej klientów banków. Wobec wprowadzenia stosownych regulacji w przepisach Prawa bankowego odnotowywany został spadek skarg odnoszących się do zakresu danych pozyskiwanych przez banki, które w latach poprzednich stanowiły znaczny odsetek.



Wykres 10: Zestawienie porównawcze liczby skarg dotyczących sektora bankowości, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

W związku z napływającymi sygnałami wskazującymi na nie skorelowanie systemów informatycznych banków oraz systemu informatycznego Biura Informacji Kredytowej S.A. skutkujące opóźnieniami w aktualizowaniu danych przekazywanych przez banki do bazy „Kredytobiorcy”, GIODO wystąpił do Generalnego Inspektora Nadzoru Bankowego o podjęcie działań mających na celu

⁷⁵ Art. 33 ustawy o ochronie danych osobowych.

⁷⁶ GI-DS-430/35/06, GI-DS-430/67/06, GI-DS-430/116/06, GI-DS-430/227/06, GI-DS-430/324/06, GI-DS-430/366/06, GI-DS-430/377/06, GI-DS-430/419/06, GI-DS-430/508/06, GI-DS-430/560/06, GI-DOLiS-12/06, GI-DOLiS-16/06, GI-DOLiS-81/06, GI-DOLiS-107/06.

⁷⁷ Zgodnie z art. 31 ustawy o ochronie danych osobowych.

⁷⁸ Decyzja z dnia 20 czerwca 2006 r., znak: GI-DEC-DS-199/06 w sprawie GI-DS-430/912/04; decyzja z dnia 26 czerwca 2006 r., znak: GI-DEC-DS-219/06 w sprawie GI-DS-430/67/06; decyzja z dnia 10 sierpnia 2006 r., znak: GI-DEC-DS-298/06 w sprawie GI-DS-430/116/06; z dnia 29 sierpnia 2006 r., znak: GI-DEC-DS-328/06 w sprawie GI-DS-430/870/05; decyzja z dnia 28 września 2006 r., znak: GI-DEC-DS-379/06 w sprawie GI-DS-430/324/06.

zmianę takiego stanu rzeczy.⁷⁹ Wystąpienie to było konieczne dlatego, że w toku prowadzonych postępowań GODO ustalił, że banki oraz BIK S.A. przetwarzają nieprawdziwe (nieaktualne) informacje o klientach banków (kredytobiorcach). Przyczyną powstawania nieprawidłowości był brak spójności systemów informatycznych banków z systemem stosowanym przez BIK S.A. W szczególności systemy te były źle opracowane na poziomie banku, albo komunikaty przez nie generowane nie były jednoznaczne dla systemu informatycznego BIK S.A. W jednej ze spraw, która była przyczyną ww. wystąpienia, bank dokonał aktualizacji danych po 18 miesiącach. Sprawa była istotna również z tego względu, że bank ten przyznał także, iż problem aktualizacji danych dotyczył 55 tysięcy rekordów klientów tego banku w bazie BIK S.A. W innej sprawie aktualizacja danych była wielokrotnie odrzucana jako błędna, a w konsekwencji przez wiele miesięcy niemożliwe było zaktualizowanie informacji i odnotowanie w systemie BIK S.A., że nastąpiła spłata kredytu i zamknięcie rachunku kredytowego. Generalny Inspektor Nadzoru Bankowego, odpowiadając na pismo GODO,⁸⁰ poinformował, że działając w granicach swych uprawnień zwrócił się do prezesów zarządów banków wskazanych przez GODO z prośbą o podjęcie niezbędnych działań, które doprowadzą do usprawnienia funkcjonowania systemów informatycznych przekazujących dane osobowe do BIK S.A., eliminując przypadki nieuzasadnionego przetwarzania danych osobowych w zbiorze pod nazwą „Kredytobiorcy”.

W roku sprawozdawczym 2006, warte są także odnotowania sprawy dotyczące skarg na nieuzasadnione przetwarzanie danych osobowych skarżących w zbiorze prowadzonym przez BIK S.A. pod nazwą „Kredytobiorcy”, po wygaśnięciu zobowiązania łączącego skarżącego z bankiem. W sprawach tych GODO badał, czy zastosowanie znajduje przesłanka legalnego przetwarzania danych osobowych,⁸¹ tj. czy istnieją podstawy do przetwarzania przez bank danych osobowych skarżących po wygaśnięciu zobowiązania w zbiorze BIK S.A. Kwestię tę regulują przepisy art. 105a Prawa bankowego, które weszły w życie w dniu 16 czerwca 2005 r. W jednej z tych spraw GODO wydał nakaz usunięcia danych osobowych ze zbioru danych kredytobiorców prowadzonego przez BIK S.A.⁸² Po wygaśnięciu zobowiązania podstawę prawną przetwarzania danych skarżącego w BIK S.A. może stanowić bądź art. 105a ust. 2 Prawa bankowego⁸³ legalizujący przetwarzanie danych konsumenta po wygaśnięciu zobowiązania za jego zgodą, bądź ust. 3 powołanego przepisu⁸⁴

⁷⁹ Pismo z dnia 10 kwietnia 2006 r., znak: GI-DS-430/370/04/1592/06.

⁸⁰ Pismo z dnia 7 lipca 2006 r., znak: NB-BPN-I-AJCH-073-2-15/06).

⁸¹ Z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

⁸² Decyzja z dnia 4 maja 2006 r., znak: GI-DEC-DS-141/06/426,427,428 w sprawie GI-DS-430/638/05.

⁸³ W myśl tego przepisu, instytucje, o których mowa w ust. 1 [banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4], mogą, z zastrzeżeniem ust. 3, przetwarzać informacje stanowiące tajemnicę bankową w zakresie dotyczącym osób fizycznych (konsumentów) po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, pod warunkiem uzyskania pisemnej zgody osoby, której informacje te dotyczą.

⁸⁴ Zgodnie z tym przepisem, ww. instytucje mogą przetwarzać informacje stanowiące tajemnicę bankową oraz informacje, o których mowa w art. 105 ust. 4 pkt 2 w zakresie dotyczącym osób fizycznych (konsumentów) po wygaśnięciu

uprawniający do przetwarzania danych konsumenta po wygaśnięciu zobowiązania, bez jego zgody, przy zaistnieniu jednakże łącznie dwóch określonych w nim przesłanek. Materiał dowodowy pozyskany w tej sprawie nie pozwolił jednak na przyjęcie, że po wejściu w życie przepisu art. 105a ust. 2 Prawa bankowego skarżący złożył pisemne oświadczenie woli, z którego wynikałoby, że godzi się na przetwarzanie jego danych w BIK S.A. GODO przyjął także, że żądanie skarżącego usunięcia jego danych z BIK S.A. – które stanowiło przedmiot postępowania prowadzonego w tej sprawie – niewątpliwie oznacza brak zgody na dalsze przetwarzanie danych w zbiorze tej instytucji. Analiza przesłanek, o których mowa w art. 105a ust. 3 Prawa bankowego, legalizujących przetwarzanie danych osobowych konsumenta bez jego zgody po wygaśnięciu zobowiązania, doprowadziła GODO do stwierdzenia, że skarżący nie jest osobą, która „nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem.” Jednocześnie bez znaczenia w tej sprawie pozostawał fakt, czy bank dochował czy też nie 30-dniowego terminu informacyjnego, o którym mowa w art. 105a ust. 3 pkt 2 Prawa bankowego. W analizowanej sprawie dane osobowe skarżącego znajdowały się w zbiorze BIK S.A. bez stosownej podstawy prawnej i z naruszeniem art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Niezbędne było zatem wydanie nakazu usunięcia przez bank danych osobowych skarżącego ze zbioru prowadzonego przez BIK S.A. Podobne sprawy⁸⁵ zakończone zostały wydaniem przez Generalnego Inspektora nakazów usunięcia danych skarżących ze zbiorów BIK S.A.⁸⁶

Ciekawą ze względu na przetwarzanie przez bank danych nieprawdziwych w zbiorze ZBP była skarga na umieszczenie przez bank danych osobowych skarżących w tym zbiorze pomimo przyjęcia przez sąd powszechny, że umowa kredytowa została sfalszowana. GODO wydał w tej sprawie nakaz usunięcia przez bank danych osobowych skarżących ze zbioru ZBP.⁸⁷ Ważne jest to, że dane osobowe zawarte w Bankowym Rejestrze służyć mają wypełnieniu przez banki, jako instytucje zaufania publicznego, ich ustawowych obowiązków związanych z zapewnianiem bezpieczeństwa przechowywanym środkiem pieniężnym oraz należytym badaniem wiarygodności i zdolności kredytowej przyszłych kredytobiorców. Wobec braku jednoznacznego potwierdzenia, że skarżący byli poręczycielami umowy kredytowej, GODO nie miał podstaw do uznania, że ich dane są potrzebne innym bankom. Skarżący nie poręczyli kredytu, nie byli zobowiązani do jego spłaty i niesłusznie

zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczą, jeśli spełnione są łącznie następujące warunki: 1) osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, 2) po zaistnieniu okoliczności, o której mowa w pkt 1, upłynęło co najmniej 30 dni od poinformowania tej osoby przez bank lub inną instytucję ustawowo upoważnioną do udzielania kredytów o zamiarze przetwarzania dotyczących jej informacji stanowiących tajemnicę bankową, bez jej zgody.

⁸⁵ GI-DS-430/877/05, GI-DS-430/83/06.

⁸⁶ Decyzja z dnia 25 maja 2006 r., znak: GI-DEC-DS-169/06/491,492,493, decyzja z dnia 30 czerwca 2006 r., znak: GI-DEC-DS-230/06/624,625,626.

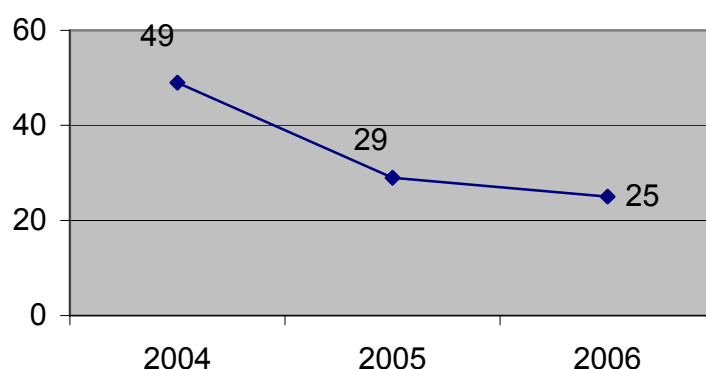
⁸⁷ Decyzja z dnia 14 kwietnia 2006 r., znak: GI-DEC-DS-132/06/391,392,393.

prowadzono wobec nich postępowanie egzekucyjne, a zatem ich dane nie były potrzebne innym bankom dla oceny ich wiarygodności i zdolności kredytowej. GODO uznał także, że umieszczenie nieprawdziwych danych o skarżących mogło wprowadzać inne banki w błąd, co do ich wiarygodności i ograniczyć ich możliwości w korzystaniu z usług bankowych.

W analizowanym roku sprawozdawczym 2006, pośród skarg rozpatrywanych przez GODO odnotowano przypadki niewypełnienia przez bank obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych, tj. uniemożliwienie realizacji przez klientów uprawnień kontrolnych. W konsekwencji konieczne było wydanie nakazów co do przekazania informacji wynikających z przepisu art. 33 ustawy.⁸⁸ Nakaz tego rodzaju GODO wydał również wobec Biura Informacji Kredytowej S.A.⁸⁹

6) Internet

Liczba skarg związanych z przetwarzaniem danych osobowych za pośrednictwem sieci Internet od kilku lat maleje.⁹⁰



Wykres 11: Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych w Internecie, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

Zmienia się również zakres przedmiotowy skarg. O ile w latach 2004-2005 zasadniczym problemem była kwestia dotycząca braku właściwych zabezpieczeń stron internetowych, jak również umieszczania danych na stronach internetowych bez spełnienia przesłanek dopuszczalności ich przetwarzania, to obecnie skala tego rodzaju naruszeń zmniejszyła się. Administratorzy danych umieszczanych w sieci publicznej poprzez wprowadzanie jednej klauzuli zgody na przetwarzanie danych w różnych celach, np. związanych z wykonywaniem zawartych umów oraz jednocześnie na

⁸⁸ Decyzja z dnia 5 lipca 2006 r., znak: GI-DEC-DS-240/06/648,649 w sprawie znak GI-DS-430/23/06 oraz decyzja z dnia 28 sierpnia 2006 r., znak: GI-DEC-DS-326/06/885,886 w sprawie znak GI-DS-430/229/06.

⁸⁹ Decyzja z dnia 5 stycznia 2006 r., znak: GI-DEC-DS-6/06/9,10 w sprawie znak: GI-DS-430/347/04.

potrzeby organizowanych akcji marketingowych czy przekazywania danych innym podmiotom wymuszają zgody w celach marketingowych.⁹¹ Nie udostępniają także danych podmiotom do tego uprawnionym, tj. takim, które występują z właściwie uzasadnionym wnioskiem i wykazują potrzebę pozyskania danych dla realizacji prawnych interesów.⁹² Uzasadnione wątpliwości budził również zbyt szeroki zakres pozyskiwanych danych osobowych.⁹³ W 2006 r. nie odnotowano natomiast skarg związanych z przesyłaniem drogą elektroniczną nie zamówionej informacji handlowej, co dowodzi, iż obecnie w powszechnej świadomości prawidłowo funkcjonuje już rozgraniczenie zakresów obowiązywania ustawy o ochronie danych osobowych i ustawy o świadczeniu usług drogą elektroniczną. Administratorzy z tego sektora zaczęli także dostrzegać konieczność rzetelnego informowania osób korzystających ze stron internetowych o swojej nazwie i siedzibie, gdyż w przeciwieństwie do lat ubiegłych, obecnie nie sygnalizowano naruszeń w tym zakresie.

Spadek liczby skarg oraz zmiana ich przedmiotu, w tym ograniczenie naruszeń może wskazywać, że w obszarze związanym z siecią Internet podmioty organizujące tą drogą usługi zyskują coraz większą wiedzę jak postępować w przypadku przetwarzania informacji, których częścią są dane osobowe. Z uwagi na ciągły rozwój tego interaktywnego środka przekazu przedwczesnym byłoby jednak twierdzenie, że obserwowana tendencja utrzyma się również w przyszłości.

Internet jest coraz częściej wykorzystywany przez podmioty sfery publicznej, które próbują wykorzystywać ten środek przekazu informacji do wykonywania swoich ustawowych zadań.

Jednym z problemów poruszonych w omawianym sektorze było zbieranie danych osobowych w zbyt szerokim zakresie. Zagadnienie to było przedmiotem postępowania prowadzonego z urzędu.⁹⁴ W jego toku ustalono, że jeden z podmiotów świadczących usługi polegające na rejestracji domen internetowych na rzecz konsumentów uzależniał wykonanie tej usługi od przesłania przez klientów kserokopii dowodu osobistego. W szczególności miało to miejsce w sytuacji tzw. transferu domen, tj. zmiany abonenta, na rzecz którego domena została rejestrowana. Podejmowanie takich działań miało zagwarantować, że osobą zlecającą przerejestrowanie domeny jest faktycznie osoba, na rzecz której domena została zarejestrowana. Jednakże, zdaniem GODO zakres zbieranych danych poprzez sporządzanie kopii z nowego typu dowodu osobistego, gdzie zawarty jest m.in. wizerunek klienta, jego nazwisko rodowe, imiona jego rodziców, a w przypadku dowodu starego typu dodatkowo dane o stanie

⁹⁰ Szczegółowe informacje na temat lat ubiegłych można odnaleźć w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, Część II, lit. R, Internet, str. 245 oraz w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności za rok 2004*, Część II, lit. K Internet, str. 209.

⁹¹ GI-DS-430/12/06, GI-DS-430/273/06.

⁹² GI-DS-430/84/06, GI-DS-430/199/06, GI-DOLiS-430/120/06.

⁹³ GI-DS-430/836/05, GI-DS-430/157/06.

⁹⁴ GI-DS-430/836/05.

cywilnym klienta, nie był adekwatny do celu, w jakim były one przetwarzane.⁹⁵ Jednocześnie z postanowień obowiązującego w tym podmiocie regulaminu, wynikało, że przedsiębiorca ten miał jedynie prawo do przetwarzania danych osobowych klienta niezbędnych do wykonania usługi, tj. imion i nazwisk klientów, ich numeru PESEL, adresu zameldowania na pobyt stały, adresu do korespondencji, jeżeli jest inny niż adres zameldowania, adresu elektronicznego, numeru telefonu oraz numeru faksu (opcjonalnie). Wskazując zatem na brak przesłanki uzasadniającej przetwarzanie dodatkowych danych zawartych w kserokopiach dowodu osobistego oraz naruszenie zasady równowagi pomiędzy uprawnieniem osoby do dysponowania swoimi danymi a interesem administratora, nakazano ww. podmiotowi zaprzestanie pozyskiwania danych w zakwestionowanym zakresie.⁹⁶

W roku sprawozdawczym 2006, pojawiło się również zagadnienie zamieszczania na stronach internetowych danych osobowych, bez uprzedniego pozyskania od zainteresowanych zgody na powyższe. Taka praktyka miała miejsce w związku z zamieszczeniem przez podmiot przetwarzający dane w sieci Internet danych osobowych laureatów zorganizowanego przez ten podmiot konkursu.⁹⁷ Chodziło o dane w zakresie: imię, nazwisko, miejsce zamieszkania (miejscowość, ulica, numer domu i lokalu). Jednocześnie osoby te nie zostały poinformowane o pełnej treści art. 24 ust. 1 ustawy. Jak podkreślił Generalny Inspektor w wydanym w sprawie rozstrzygnięciu,⁹⁸ wprowadzić uczestnicy quizu wyrazili zgodę na wykorzystanie ich danych osobowych na potrzeby konkursu, ale oświadczenie woli w tym zakresie nie jest równoznaczne z udzieleniem zgody na ich zamieszczenie w Internecie. Zgoda na przetwarzanie danych w tym celu musi być bowiem wyraźna i udzielona odrębnie.

7) Marketing

W analizowanym 2006 roku, nadal napływały skargi na przetwarzanie danych przez podmioty prowadzące marketing swoich produktów i usług w tzw. „systemie wysyłkowym”. I choć statystycznie liczba sygnałów dotyczących nieprawidłowych praktyk spada,⁹⁹ to jednak wiele z nich było przedmiotem zawiadomień kierowanych do organów ścigania.

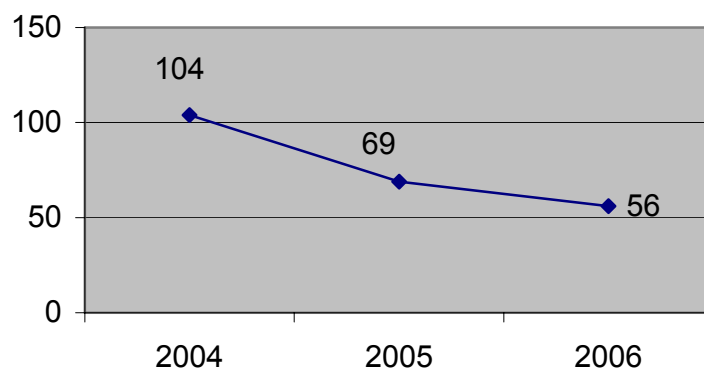
⁹⁵ Zgodnie z brzmieniem art. 26 ust. 1 pkt 3 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

⁹⁶ Decyzja z dnia 15 maja 2006 r. o sygn. GI-DEC-DS-157/06.

⁹⁷ GI-DS-430/2/05.

⁹⁸ Decyzja z dnia 6 lipca 2006 r. o sygn. GI-DEC-DS-244/06.

⁹⁹ Szczegółowe informacje na temat lat ubiegłych można odnaleźć w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, Część II, lit. E Marketing, str. 128 oraz w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności za rok 2004*, Część II, lit. I Marketing, str. 195.



Wykres 12: Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych w celach marketingowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

Na poprawę sytuacji niewątpliwie wpłynęła konsekwentna polityka GODO, polegająca nie tylko na podejmowaniu wobec administratorów danych przewidzianych ustawą działań (wydawania decyzji administracyjnych, kierowania do organów ścigania zawiadomień o naruszeniu przepisów karnych ustawy, czy pism sygnalizacyjnych), ale również na propagowaniu wśród osób zgłaszających skargi wiedzy na temat tego, jak powinny postępować w sytuacji, gdy ich dane stały się przedmiotem nieuprawnionego obrotu handlowego, a także o przysługujących im uprawnieniach wynikających z ustawy o ochronie danych osobowych.

Przeprowadzone postępowania wykazywały, iż podstawą prawną dokonywanych operacji na danych była często zgoda lub usprawiedliwiony cel administratora danych.¹⁰⁰ Wielokrotnie stwierdzano również brak właściwego wypełniania obowiązków informacyjnych, określonych w art. 24 i art. 25 ustawy. Problem ten był szczególnie widoczny w przypadkach przetwarzania danych przez podmioty prowadzące działalność poza terytorium Polski. Unikały one przekazywania informacji o dokładnym adresie siedziby, czy źródle pozyskania danych, co uniemożliwiało skarżącym realizację zagwarantowanych im ustawą uprawnień, np. skuteczne sprzeciwianie się dalszemu wykorzystywaniu ich danych. W takich sytuacjach GODO kierował do organów ścigania zawiadomienia o naruszeniu art. 54 ustawy.¹⁰¹ Problematyczna była również kwestia odbierania przez podmioty z tego sektora zgody na przetwarzanie danych osobowych w aspekcie braku zapewnienia opcjonalności wyrażania oświadczeń woli na przetwarzanie danych w różnych celach.¹⁰² W tych przypadkach wystarczającym było sygnalizowanie administratorom konieczności dokonania stosownych zmian w proponowanych formularzach w kierunku wyodrębnienia zgód na proponowane cele.

¹⁰⁰ Np.: GI-DS430/271/06, GI-DS-430/353/06.

¹⁰¹ Np.: GI-DS-430/150/06, GI-DS-430/167/06.

¹⁰² 18 skarg - m.in. GI-DS-430/224/06, GI-DS-430/250/06, GI-DS-430/451/06.

Przetwarzanie danych dla celów marketingowych może być oparte na dwóch przesłankach spośród wskazanych w art. 23 ust. 1 ustawy o ochronie danych osobowych. W przypadku marketingu własnych produktów i usług administratora danych, gdy przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, podstawą przetwarzania danych będzie art. 23 ust. 1 pkt 5 ustawy, tj. prawnie usprawiedliwiony cel administratora danych. W pozostałych przypadkach, np. gdy marketing dotyczy produktów innych podmiotów, przetwarzanie danych dopuszczalne jest tylko za zgodą osoby, której dane dotyczą.

Innego rodzaju nieprawidłowością, zaobserwowaną w toku działalności GIODO w 2006 r., było nie zapewnienie przez jeden z podmiotów z tego sektora w treści przedstawianego klientom formularza opcjonalności klauzuli zgody na przetwarzanie danych w celach marketingowych.¹⁰³ W zaproponowanej przez ten podmiot klauzuli klient wyrażał jednoczesną zgodę na przetwarzanie jego danych osobowych w celach związanych z wykonaniem zlecenia oraz dla celów marketingowych.

W związku ze zbliżającą się kampanią wyborczą do wyborów samorządowych, podmiot specjalizujący się w udostępnianiu adresowych, telefonicznych, oraz e-mailowych zbiorów danych do projektów z zakresu marketingu bezpośredniego zgłosił do rejestracji zbiór zawierający dane sympatyków Sojuszu Lewicy Demokratycznej.¹⁰⁴ Celem utworzenia takiego zbioru było zgromadzenie informacji o osobach prezentujących lewicowe poglądy polityczne, deklarujących się jako zwolennicy SLD. Dane miały służyć przeprowadzeniu samorządowej kampanii wyborczej, a po wyborach zaplanowano ich wykorzystanie do utrzymywania kontaktów z osobami, których dane dotyczą, w celu poznania ich poglądów na temat działań władz lokalnych. Wnioskodawca błędnie wskazał, że przetwarzane przez niego dane zostaną powierzone SLD. W rzeczywistości nie zamierzał tych danych powierzyć, ale je udostępnić. O udostępnieniu danych Sojuszowi Lewicy Demokratycznej osoby, których dane dotyczą informowane były przed wyrażeniem przez nie zgody na przetwarzanie danych. Ponadto, w omawianym przypadku, kierując się zasadą adekwatności przetwarzania danych Generalny Inspektor zakwestionował celowość gromadzenia informacji o numerze PESEL. Administrator danych przyznając, iż zbieranie tej informacji nie jest w tym przypadku niezbędne zrezygnował z jej przetwarzania. Po złożeniu niezbędnych wyjaśnień przez wnioskodawcę niniejszych zbiór został zarejestrowany.

W przypadku analizy zgłoszeń zbiorów zawierających dane przetwarzane w celu marketingu bezpośredniego własnych produktów i usług najwięcej wątpliwości budził zakres przetwarzanych danych. Dla przykładu, producent alkoholi zgłosił zbiór danych swoich klientów, w którym, jak wynikało ze zgłoszenia, gromadził dane ujawniające nałogi konsumentów.¹⁰⁵ Przyjął on bowiem, że

¹⁰³ GI-DS-430/224/06.

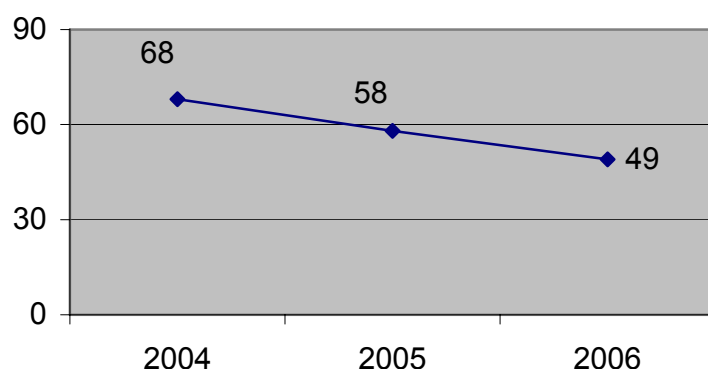
¹⁰⁴ Zgłoszenie nr R 003662/06.

¹⁰⁵ Zgłoszenie nr R 004888/05.

informacja o częstotliwości picia whisky pozyskana do zbioru za pomocą ankiety, świadczy o nałogu konkretnej osoby. Osoba wypełniająca przedmiotową ankietę informowała o częstotliwości spożycia alkoholu przez zaznaczenie jednej z możliwych odpowiedzi: „raz na tydzień”, „raz na miesiąc”, „okazjonalnie”, „nie piję” oraz wskazywała swoje preferencje na temat marki kupowanych alkoholi. Dane te w żaden sposób nie świadczą o nałogu alkoholowym osoby, której informacje te dotyczą. Zatem w przedmiotowym zbiorze nie są przetwarzane dane o nałogach. Zbiór ten został zarejestrowany.

8) Sektor mieszkalnictwa

Innym z obszarów, którego dotyczyły wpływające skargi był sektor mieszkalnictwa, związany głównie z działalnością spółdzielni, wspólnot mieszkaniowych, zarządców nieruchomości oraz gminy w zakresie przetwarzania danych osobowych w związku z gospodarowaniem przez nie zasobami mieszkaniowymi. W 2006 r. w porównaniu z latami ubiegłymi odnotowano spadek liczby skarg na przetwarzanie danych przez ww. podmioty.¹⁰⁶



Wykres 13: Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych osobowych z zakresu mieszkalnictwa, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

Częściowej zmianie uległa również tematyka podnoszonych przez skarżących zarzutów. Dużym problemem w rozpatrywanym roku sprawozdawczym okazała się kwestia dostępu do danych członków spółdzielni znajdujących się w prowadzonych przez spółdzielnie rejestrach.¹⁰⁷ Spółdzielnie, nieprawidłowo interpretując postanowienia przepisów prawa spółdzielczego¹⁰⁸ odmawiały dostępu do

¹⁰⁶ Szczegółowe informacje na temat lat ubiegłych można odnaleźć w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, Część II, lit. G Mieszkalnictwo, str. 141 oraz w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności za rok 2004*, Część II, lit. G Mieszkalnictwo, str. 176.

¹⁰⁷ Np. GI-DS-430/57/06, GI-DS-430/246/06, GI-DS-430/395/06.

¹⁰⁸ Np. GI-DS-430/106/06.

danych gromadzonych w rejestrze` spółdzielców osobom do tego uprawnionym.¹⁰⁹ W stopniu większym niż w ubiegłych latach było udostępnianie przez podmioty z opisywanego sektora danych osobowych swoich członków innym podmiotom takim jak, np. kancelarie prawne, czy podmioty świadczące usługi na rzecz spółdzielni i wspólnot. Skargi w tym zakresie okazywały się jednakże najczęściej niezasadne. Kwestionowane operacje na danych podejmowane były bowiem bądź w usprawiedliwionym celu administratora danych, bądź w celu zrealizowania konkretnych uprawnień wynikających z przepisów prawa.¹¹⁰ Zdarzały się również przypadki przekazywania danych w wyniku zawartych umów powierzenia.¹¹¹

Poruszano także kwestie nieuprawnionego upubliczniania przez podmioty z omawianego sektora danych osobowych członków spółdzielni i wspólnot.¹¹² Proceder ten, podobnie jak w latach poprzednich, polegał m.in. na wywieszaniu w miejscach powszechnie dostępnych informacji o osobach zadłużonych, informacji o zapadłych wobec członków wyrokach, czy nawet samych wyroków.¹¹³ Choć liczba skarg z tego zakresu z roku na rok maleje, to jednak niektórzy administratorzy z obszaru mieszkalnictwa wciąż traktują upowszechnianie posiadanych danych jako jedną z metod wywierania nacisku na swoich członków mimo, że zostali wyposażeni w inne środki dyscyplinujące dłużników, które nie stoją w kolizji z przepisami ustawy.¹¹⁴

Jedna ze spraw będących w 2006 r. przedmiotem rozpoznania przez Generalnego Inspektora była związana z odmową udostępnienia danych osobowych z rejestru członków spółdzielni.¹¹⁵ Z odmową spotkał się dłużnik spółdzielni, legitymujący się nakazem zapłaty wydanym wobec spółdzielni w postępowaniu upominawczym. Z uwagi na bezskuteczność prowadzonej wobec spółdzielni egzekucji, skarżący na podstawie art. 29 ustawy zwrócił się do spółdzielni o udostępnienie mu danych osobowych jej członków, w celu przeprowadzenia egzekucji z wnoszonych przez nich opłat czynszowych. Odmowa udostępnienia skarżącemu wnioskowanych danych była jednak nieuzasadniona, bowiem był on uprawniony do ich otrzymania na mocy przepisów prawa, tj. w szczególności na podstawie ustawy - Prawo spółdzielcze.¹¹⁶ Wierzyciel członka spółdzielni bądź wierzyciel spółdzielni ma bowiem prawo przeglądać rejestr, który m.in. zawiera imiona i nazwiska

¹⁰⁹ Art. 30 ustawy Prawo spółdzielcze.

¹¹⁰ Np. GI-DS-430/138/06, GI-DS-430/402/06.

¹¹¹ Np. GI-DS-430/89/06.

¹¹² GI-DS-430/176/06, GI-DS-430/196/06, GI-DS-430/373/06, GI-DS-430/390/06.

¹¹³ Niemalże całkowitemu wyeliminowaniu uległ natomiast problem udostępniania danych osobowych na domofonach czy listach mieszkańców.

¹¹⁴ Mogą, np. zgłaszać dłużników do biur informacji gospodarczej.

¹¹⁵ GI-DS-430/57/06.

¹¹⁶ Zgodnie z art. 29 ust. 1 ustawy, w przypadku udostępniania danych osobowych w celach innych niż włączanie do zbioru administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

członków spółdzielni, a więc dane, o których udostępnienie wnosili skarżący.¹¹⁷ Wobec takich ustaleń nakazano spółdzielni udostępnienie danych z rejestru członków w określonym przez skarżącego zakresie.¹¹⁸

Również wspólnoty upubliczniały dane osobowe swoich członków w sposób niezgodny z prawem. Miało to miejsce, np. w sprawie dotyczącej wywieszenia w miejscu powszechnie dostępnym kserokopii wyroków sądowych zawierających dane osobowe skarżących.¹¹⁹ W ocenie wspólnoty podjęcie takich działań nie było sprzeczne z ustawą bowiem wyroki oprócz imion i nazwisk skarżących nie zawierały żadnych innych danych. Taka interpretacja przepisów ustawy nie była jednak uprawniona. Dane zawarte w orzeczeniach wydanych w postępowaniach sądowych są bowiem nie tylko danymi osobowymi w rozumieniu art. 6 ustawy, ale również danymi szczególnie chronionymi, których udostępnienie następuje wyłącznie po spełnieniu rygorystycznych przesłanek z art. 27 ust. 2 ustawy. O ile w oparciu o przepisy prawa regulujące funkcjonowanie wspólnot¹²⁰ przekazanie tego rodzaju danych członkom wspólnoty ze względu na prawidłowe zarządzanie własnością oraz efektywne wykonywanie kontroli wydatków byłoby uprawnione, to ich udostępnieniu osobom trzecim brakowało przymiotu legalności.

W 2006 r. GODO wystąpił do Przewodniczącego Komisji Sejmowej Samorządu Terytorialnego i Polityki Regionalnej¹²¹ o podjęcie działań legislacyjnych w celu rozszerzenia¹²² katalogu sytuacji, w których właściciele lokali stanowiących mieszkaniowy zasób gminny mogą pozyskiwać dane osobowe najemców wskazanych lokali w drodze wywiadu środowiskowego o przypadek, kiedy pozyskanie takich danych służy weryfikacji faktycznego zamieszkiwania ww. osób w najmowanych lokalach. Obowiązujące przepisy dopuszczają bowiem przeprowadzenie takiego wywiadu wyłącznie w celu ustalenia sytuacji majątkowej wnioskodawcy i członków gospodarstwa domowego. Za modyfikacją przepisów przemawia interes publiczny w postaci pełniejszej realizacji uprawnień własnościowych określonych przepisami prawa.

9) Oświata

W omawianym 2006 roku, GODO interweniował także w sprawie opublikowania w jednym z przedszkoli w miejscu powszechnie dostępnym danych osobowych dzieci, których rodzice zalegali z uregulowaniem opłat za ich pobyt w przedszkolu.¹²³ Interwencja była konieczna, gdyż na skutek takiego przetwarzania danych osobowych dostęp do nich miały osoby postronne. Dyrektor przedszkola

¹¹⁷ Art. 30 ustawy Prawo spółdzielcze.

¹¹⁸ Decyzja z dnia 28 czerwca 2006 r. o sygn. GI-DEC-DS-226/06.

¹¹⁹ GI-DS-430/196/06.

¹²⁰ Ustawa o własności lokali oraz ustawa Kodeks cywilny.

¹²¹ Pismo z dnia 18 maja 2006 r., znak: GI-DS-430/69/06.

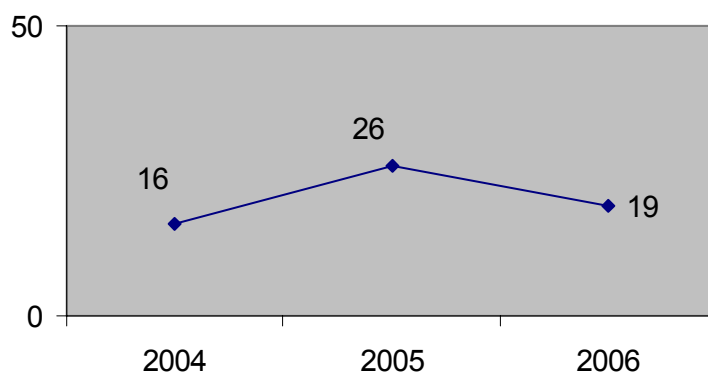
¹²² Przewidzianego w ustawie z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego (Dz. U. z 2005 r. Nr 31, poz. 266 ze zm.).

¹²³ Pismo z dnia 20 września 2006 r., znak: GI-DS-430/368/06/4130.

argumentował, że potrzeba upublicznienia danych wynikała z niemożności wyegzekwowania od rodziców opłat za pobyt ich dzieci w przedszkolu, jednak organ do spraw ochrony danych osobowych uznał, iż dla udostępnienia danych w opisany sposób nie było podstawy prawnej, a z danymi mogły się zapoznać osoby nieupoważnione. W odpowiedzi na wystosowane w tym zakresie wystąpienie dyrektor przedszkola poinformował, że zaprzestano praktyki wywieszania list osób zadłużonych, ponownie zapoznano pracowników z przepisami ustawy i zdecydowano, że w stosunku do osób zalegających z opłatami będą kierowane wnioski do sądu.

10) Służba zdrowia

Zmniejszeniu uległa liczba skarg w sektorze służby zdrowia w porównaniu z 2005 r. i ustaliła się na poziomie porównywalnym z latami wcześniejszymi. Przedmiot skarg pozostawał podobny, tj. skarżono się głównie na publiczne i niepubliczne zakłady opieki zdrowotnej, które udostępniały dane podmiotom nieupoważnionym. Wyeliminowaniu uległy natomiast skargi na organ nadzoru nad prawidłowością świadczenia usług medycznych, tj. Narodowy Fundusz Zdrowia (wcześniej Kasy Chorych), skargi na porzucenie dokumentacji medycznej, jak również skargi na udostępnianie danych pacjentów w miejscach publicznych. Jedynie incydentalnie skarżono się na zakres danych przetwarzanych przez jednostki służby zdrowia, które to zagadnienie przez wiele ubiegłych lat było przedmiotem większości zarzutów.



Wykres 14: Zestawienie porównawcze liczby skarg z sektora służby zdrowia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

W jednej ze spraw z tego sektora GIODO przeprowadził postępowanie wyjaśniające zainicjowane skargą, dotyczącą udostępnienia przez szpital danych osobowych skarżącego kancelarii prawnej.¹²⁴ Jak ustalono, kancelaria prawna zwróciła się do szpitala o udzielenie jej informacji o terminach pobytu w szpitalu skarżącego, w tym o terminach wykorzystania przez niego przepustek.

¹²⁴ GI-DS-430/886/05.

Wnioskowanych informacji udzielono, pomimo, że kancelaria nie przedstawiła stosownie umotywowanego wniosku. Nie wskazała bowiem przeznaczenia, dla którego przedmiotowe dane mają być udostępnione. Tymczasem na szpitalu, jako administratorze danych spoczywał obowiązek zachowania szczególnej staranności przy udostępnianiu podmiotom trzecim danych osobowych skarżącego.

Ciekawą sprawę z zakresu przetwarzania danych o stanie zdrowia zapoczątkowała skarga dotycząca udostępnienia przez terenową wojskową komisję lekarską danych osobowych skarżącego jednostce wojskowej.¹²⁵ Podczas badań laboratoryjnych przeprowadzanych w związku z zakwalifikowaniem skarżącego do pełnienia służby wojskowej poza granicami kraju, ww. komisja stwierdziła w jego moczu obecność opiatów (dodatni test na narkotyki). Informacja ta przesłana została do dowódcy jednostki wojskowej, gdzie skarżący pełnił służbę, przy czym zapoznali się z nią również osoby, które nie były do tego uprawnione. Udostępnienie przedmiotowych danych miało być podyktowane troską o ochronę życia i zdrowia badanego oraz osób przebywających w miejscu służby. Jednak w świetle art. 27 ust. 2 pkt 2 ustawy i przepisów szczególnych, tj. rozporządzenia Ministra Obrony Narodowej z dnia 10 maja 2004 r. w sprawie orzekania o zdolności do zawodowej służby wojskowej oraz właściwości i trybu postępowania wojskowych komisji lekarskich w tych sprawach (Dz. U. Nr 133, poz. 1422 ze zm.), takie działania nie znajdowały prawnego uzasadnienia. Wojskowe komisje lekarskie są bowiem zobowiązane do doręczenia żołnierzowi zawodowemu oraz organowi, który skierował go na badania wyłącznie orzeczenia lekarskiego, a nie jednostkowego wyniku badania żołnierza.¹²⁶

Generalny Inspektor spotkał się także z problemem zbierania danych o stanie zdrowia bez podstawy prawnej, z naruszeniem zasady adekwatności. Miało to miejsce w sprawie dotyczącej przetwarzania przez ośrodek rehabilitacyjno-edukacyjny danych opiekunów dzieci przyjmowanych do leczenia w tym ośrodku.¹²⁷ Ośrodek zbierał od opiekunów (kobiet) dane związane z badaniem ginekologicznym, uzasadniając stawianie takich wymogów prowadzeniem rehabilitacji dzieci w jednym basenie z opiekunami. W toku przeprowadzonego w tej sprawie postępowania ustalono, że ośrodek zaprzestał przetwarzania danych osobowych w zakwestionowanym zakresie. Obecnie, na skutek wszczęcia postępowania przez Generalnego Inspektora, w przypadku zbierania danych o stanie zdrowia uzyskiwana jest pisemna zgoda osoby zainteresowanej i spełniany wobec niej obowiązek informacyjny.

Generalny Inspektor odniósł się też do kwestii legalności wydania osobie, której brat cierpiący na chorobę psychiczną postanowieniem sądu umieszczony został w domu opieki społecznej,

¹²⁵ GI-DS-430/346/06.

¹²⁶ § 25 i § 30 ww. rozporządzenia.

¹²⁷ GI-DS-430/1013/04.

zaświadczenia dotyczącego jego pobytu w tym domu.¹²⁸ Zaświadczenie to było niezbędne, by móc zarządzać nieruchomością, której był on współwłaścicielem. Rozpatrując to zagadnienie GODO odwołał się do przepisów ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. Nr 111, poz. 535 ze zm.). Zgodnie z jej art. 50 ust. 1, osoby wykonujące wynikające z niej czynności zobowiązane są do zachowania w tajemnicy wszystkiego, o czym powezną wiadomość w związku z wykonywaniem tych czynności, poza wyjątkami wskazanymi w ust. 2 niniejszego przepisu. Osobom spoza kręgu podmiotów uprawnionych do posiadania informacji objętych tajemnicą, wymienionym w art. 50 ust. 2, nie ujawnia się żadnych wiadomości związanych z wykonywaniem czynności wynikających z przepisów o ochronie zdrowia psychicznego. Zatem udostępnienie członkowi rodziny informacji dotyczącej pobytu określonej osoby w domu pomocy społecznej, jak też wydanie przez osobę zarządzającą placówką ww. zaświadczenia, nie jest dopuszczalne.

Lekarz pracujący w centrum onkologii zwrócił się z pytaniem o dopuszczalność przekazania do właściwego wydziału komunikacji (pracodawcy) informacji o tym, że u pacjenta, którym był kierowca, rozpoznano guza mózgu.¹²⁹ Informacja o stanie zdrowia należy do danych szczególnie chronionych. Brak jest jednak przepisu, z którego wprost wynikałoby uprawnienie lekarza do przekazania właściwym wydziałom komunikacji informacji o stanie zdrowia pacjenta mogących mieć wpływ na jego zdolności motoryczne, w tym kierowanie pojazdem mechanicznym. Zatem przekazanie takich danych jest niedopuszczalne.

Niekonsekwencja w proponowanych uregulowaniach pojawiła się w projekcie rozporządzenia Ministra Zdrowia w sprawie szczegółowych warunków i trybu postępowania w przedmiocie leczenia lub rehabilitacji osób uzależnionych, skazanych za przestępstwa pozostające w związku z używaniem środków odurzających lub substancji psychotropowych.¹³⁰ Z jednej strony § 3 ust. 3 pkt 7 wskazywał na gromadzenie w ewidencji prowadzonej przez zakład, w którym osoba uzależniona ma się poddać leczeniu lub rehabilitacji, sygnatury orzeczenia sądowego, a jednocześnie § 3 ust. 4 zakazywał umieszczania w takiej ewidencji danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Generalny Inspektor stwierdził, że sygnatura orzeczenia stanowi bez wątpienia daną, o której mowa w § 3 ust. 4, a co za tym idzie, wskazane regulacje są ze sobą sprzeczne i nawzajem się wykluczają. Uwagi Generalnego Inspektora zostały uwzględnione.¹³¹

¹²⁸ GI-DP-024/330/06.

¹²⁹ GI-DP-024/1614/06.

¹³⁰ Pismo z dnia 20 marca 2006 r. o sygn. MZ-ZPO-0212-3009-7/DB/06. Odpowiedź GODO z dnia 30 marca 2006 r. o sygn. GI-DP-023/66/06.

¹³¹ Wykreślono ust. 4 z § 3 projektu rozporządzenia. Rozporządzenie Ministra Zdrowia z dnia 1 grudnia 2006 r. w sprawie szczegółowych warunków i trybu postępowania w przedmiocie leczenia lub rehabilitacji osób uzależnionych, skazanych za przestępstwa pozostające w związku z używaniem środków odurzających lub substancji psychotropowych (Dz. U. Nr 239, poz. 1738) weszło w życie w dniu 6 stycznia 2007 r.

W związku z pracami nad projektem ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz niektórych innych ustaw,¹³² Generalny Inspektor uznał za wkraczający bezpodstawnie w zagwarantowaną konstytucyjną sferę prywatności (art. 31 ust. 3, art. 47 i art. 51 Konstytucji RP) zapis wprowadzający obowiązek składania przez posiadaczy pojazdów mechanicznych oświadczeń o prawomocnym skazaniu za prowadzenie pojazdu mechanicznego w stanie po użyciu alkoholu lub podobnie działającego środka przed zawarciem umowy ubezpieczenia OC. Wprowadzenie powszechnego obowiązku składania oświadczeń o karalności mogłoby – zdaniem Generalnego Inspektora – narażać obywateli na ingerencję w ich prywatność oraz naruszać zasadę proporcjonalności, które to działanie nie wydaje się konieczne i niezbędne, a także współmierne do ewentualnych korzyści płynących z wprowadzenia tej instytucji. W związku z tym organ ochrony danych osobowych zakwestionował także przepis uprawniający zakłady ubezpieczeń do weryfikowania prawdziwości tych oświadczeń w oparciu o dane zgromadzone przez szeroko określone organy władzy państwowej (sądy, organy prokuratury, Policji oraz inne organy władzy państwowej), jak również zwrócił uwagę na brak określenia trybu weryfikacji informacji zawartych w tych oświadczeniach.¹³³ Zgłosił także uwagę w kwestii doprecyzowania momentu, od którego biegnie 5 – letni okres opłacania składki OC.¹³⁴ W omawianym okresie prace nad ostatecznym kształtem ustawy nie zostały zakończone.

11) Ubezpieczenia społeczne, majątkowe i osobowe

Skargi z zakresu ubezpieczeń społecznych rozpatrzone w analizowanym 2006 r., głównie dotyczyły kwestii udostępnienia danych przez Zakład Ubezpieczeń Społecznych (ZUS). Przy czym większość była skargami nieuzasadnionymi, gdyż działania ww. podmiotu znajdowały uzasadnienie w przepisach prawa.¹³⁵ Ze względu na ograniczenia wynikające z przepisów prawa wskazujące zamknięty katalog podmiotów, którym ZUS może udostępniać dane zgromadzone na kontach

¹³² Pismo z dnia 27 lipca 2006 r. o sygn. MZ-UZ-RP-0212-5923-6/JC/06. Odpowiedź GIODO z dnia 7 września 2006 r. o sygn. DI-DP-023/23/05/06.

¹³³ Zgodnie z projektowanym art. 29a ust. 6 ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, „Na wniosek zakładu ubezpieczeń sądy, organy prokuratury, Policji oraz inne organy władzy państwowej mają obowiązek nieodpłatnie udzielić informacji w zakresie oświadczenia, o którym mowa w ust. 1.”

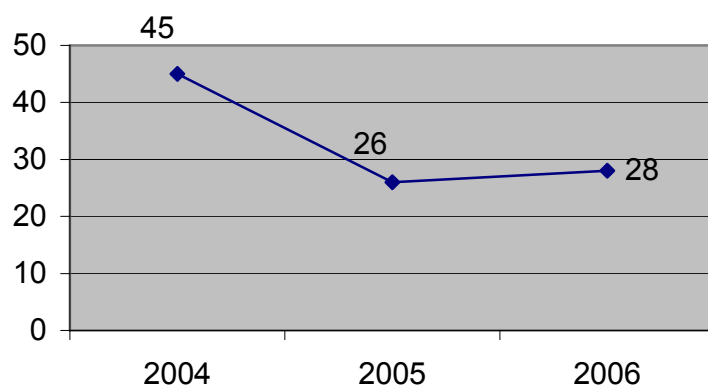
¹³⁴ Zgodnie z projektowanym art. 29a ust. 4 ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, „Jeżeli w oświadczeniu (...) znajdzie się informacja o prawomocnym skazaniu lub ukaraniu za prowadzenie pojazdu mechanicznego w stanie nietrzeźwości lub ukaraniu za prowadzenie pojazdu mechanicznego znajdując się w stanie po użyciu alkoholu lub podobnie działającego środka, w tym pod wpływem środków odurzających, substancji psychotropowych lub środków zastępczych w rozumieniu przepisów o przeciwdziałaniu narkomanii, składkę z tytułu zawarcia obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych ustala się w wysokości potrójnej w stosunku do wysokości składki ustalonej bez uwzględnienia okoliczności wskazanych w oświadczeniu”. W toku prac legislacyjnych nad projektem tej ustawy wycofano w całości art. 29a.

¹³⁵ Decyzja z dnia 15 grudnia 2006 r., znak: GI-DEC-DOLiS-452/06, w sprawie znak: GI-DS-430/303/06.

ubezpieczonych i kontach płatników¹³⁶ wiele podmiotów nie było uprawnionych do pozyskania danych z tych kont.¹³⁷

Reasumując omówione powyżej zagadnienia stwierdzić należy, że zakres przedmiotowy skarg z sektora ubezpieczeń społecznych, a także majątkowych i osobowych, jakie wpłynęły do GODO w roku 2006 r. był podobny do zagadnień poruszanych przez skarżących w skargach z tego zakresu wnoszonych w latach poprzednich.

W skargach z 2006 r. utrwaliła się tendencja z lat 2004-2005 polegająca na sygnalizowaniu przypadków przetwarzania danych osobowych, które znajdowało uzasadnienie w obowiązujących przepisach prawa, a zatem nie mogło być uznane przez GODO za nielegalne. Nie wpłynęły natomiast skargi odnoszące się do nieprawidłowości w przetwarzaniu danych będących skutkiem błędnych działań ich pracowników lub osób, którym zlecono przetwarzanie danych. Nie odnotowano także skarg na przetwarzanie danych w celach marketingowych, ani też na niewłaściwe wykonywanie obowiązków informacyjnych, co może świadczyć o stałym podnoszeniu wiedzy z zakresu ochrony danych osobowych wśród instytucji ubezpieczeniowych.



Wykres 15: Zestawienie porównawcze liczby skarg dotyczących sektora ubezpieczeń, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

Najciekawszymi sprawami z zakresu ubezpieczeń społecznych, majątkowych i osobowych, jakie w analizowanym roku sprawozdawczym rozpatrywał GODO były te, których zakres przedmiotowy dotyczył sprostowania pisowni nazwiska skarżącego. Skargi wskazywały na lekceważenie przez administratorów obowiązku zapewnienia merytorycznej poprawności danych i sprostowania danych na żądanie skarżącego korzystającego z jednego z elementów prawa do kontroli procesu przetwarzania danych osobowych. W sprawach tych GODO zaakcentował konieczność dochowania

¹³⁶ Art. 50 ust. 3 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. Nr 137, poz. 887 ze zm.).

¹³⁷ Decyzja z dnia 29 grudnia 2006 r., znak: GI-DEC-DOLiS-464/06, w sprawie znak: GI-DS-430/531/06.

obowiązku merytorycznej poprawności danych.¹³⁸ Organ do spraw ochrony danych osobowych wskazał, że informacje wynikające z przetwarzanych danych powinny być zgodne z prawdą, kompletne i aktualne, jako że administrator jest odpowiedzialny nie tylko za prawidłowe przetwarzanie danych, ale także za ich jakość.

12) Telekomunikacja

W analizowanym 2006 roku, skargi z zakresu telekomunikacji, podobnie jak w latach poprzednich (2003-2005), w większości odnosiły się do problemu przetwarzania danych osobowych w ramach odzyskiwania wierzytelności z tytułu opłat za świadczenie usług telekomunikacyjnych.¹³⁹ Wśród skarg przeważały takie, w których po dokonaniu oceny stanów faktycznych spraw¹⁴⁰ okazywało się, że udostępnienie danych następowało wskutek zbycia (cesji) wierzytelności, tj. administrator danych zmieniał się, co jest dopuszczalne z punktu widzenia art. 23 ust. 1 pkt 5 ustawy lub przekazywano dane innym podmiotom na podstawie umowy powierzenia, a tym samym dokonywano działań na danych osobowych w imieniu i na rzecz administratora.¹⁴¹

Problemem pozostaje odnotowywana także w poprzednich okresach sprawozdawczych kwestia udostępniania danych osobom nieupoważnionym, np. publikowania w książce telefonicznej danych zastrzeżonych.¹⁴² Sytuacje, gdy publikacja następowała, np. na skutek błędu pracownika¹⁴³ należało traktować jako niewłaściwe wykonanie umowy o świadczenie usług telekomunikacyjnych, jednak GODO uznawał takie zdarzenia także za przejaw niestaranności operatora w procesie przetwarzania danych i albo nakazywał usunięcie danych ze spisów publicznych¹⁴⁴ albo sygnalizował możliwość ukarania dyscyplinarnego pracownika odpowiedzialnego za powyższe. W 2006 r. został ponadto ostatecznie rozstrzygnięty spór co do statusu danych transmisyjnych jako danych osobowych,¹⁴⁵ a operator dostosował się do wydanych nakazów¹⁴⁶ w zakresie konieczności dopełnienia obowiązku informacyjnego wobec osób, których przedmiotowe dane dotyczyły, wynikającego wprost z przepisów Prawa telekomunikacyjnego.

¹³⁸ Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

¹³⁹ Por. *Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, str. 178.

¹⁴⁰ Np. decyzja z dnia 12 lipca 2006 r., znak: GI-DEC-DS-262/06 i decyzja z dnia 21 września 2006 r., znak: GI-DEC-DS-366/06 w sprawie GI-DS-430/191/06; decyzja z dnia 31 lipca 2006 r., znak: GI-DEC-DS-286/06 w sprawie GI-DS-430/40/06; decyzja z dnia 1 sierpnia 2006 r., znak: GI-DEC-DS-288/06 w sprawie GI-DS-430/63/06; decyzja z dnia 20 października 2006 r., znak: GI-DEC-DS-402/06 w sprawie GI-DS-430/223/06.

¹⁴¹ Na podstawie art. 31 ustawy - np. decyzja z dnia 22 czerwca 2006 r., znak: GI-DEC-DS-203/06 i decyzja z dnia 21 sierpnia 2006 r., znak: GI-DEC-DS-309/06 w sprawie GI-DS-430/47/06 i GI-DS-430/48/06; decyzja z dnia 30 czerwca 2006 r., znak: GI-DEC-DS-229/06 w sprawie GI-DS-430/17/06; decyzja z dnia 30 sierpnia 2006 r., znak: GI-DEC-DS-336/06 w sprawie GI-DS-430/213/06; decyzja z dnia 26 września 2006 r., znak: GI-DEC-DS-369/06 w sprawie GI-DS-430/342/06; decyzja z dnia 5 października 2006 r., znak: GI-DEC-DS-384/06 w sprawie GI-DS-430/171/06.

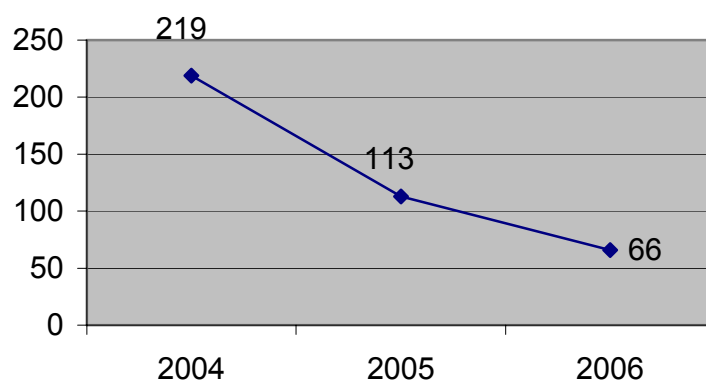
¹⁴² GI-DS-430/318/06.

¹⁴³ GI-DS-430/115/06, GI-DS-430/149/06, GI-DS-430/298/06.

¹⁴⁴ Decyzja z dnia 14 września 2006 r., znak: GI-DEC-DS-356/06/984,985.

¹⁴⁵ Decyzja z dnia 21 sierpnia 2006 r., znak: GI-DS-DS-312/06.

W 2006 r. liczba spraw z zakresu telekomunikacji znacząco spadła w stosunku do skarg z roku poprzedniego. Incydentalne były skargi na przetwarzania danych dla celów marketingowych,¹⁴⁷ a całkowitemu wyeliminowaniu uległy skargi na niewykonywanie przez operatorów obowiązku informacyjnego, czy formułowanie klauzuli zgody na przetwarzanie danych. Proces przetwarzania danych w tym sektorze nadal jednak budzi zastrzeżenia z uwagi na udostępnianie danych zastrzeżonych, będących rezultatem błędów pracowników operatorów czy wadliwości funkcjonowania stosowanych systemów informatycznych.



Wykres 16: Zestawienie porównawcze liczby skarg dotyczących sektora telekomunikacji, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

W analizowanym 2006 roku, GODO uzyskał także z urzędu informacje o działającym na rynku usług telekomunikacyjnym podmiocie, który przetwarza dane osobowe m.in. poprzez wysyłanie faktur na zapłatę wskazanych w nich kwot. Faktury przypominały rachunki wysyłane przez inny podmiot świadczący usługi telekomunikacyjne i załączano do nich umowy, na podstawie których świadczone miały być usługi umieszczenia danych osobowych na stronie internetowej dotyczącej książki telefonicznej. Ponieważ podmiot ten uchylał się od składania wyjaśnień w sprawie,¹⁴⁸ skierowano do właściwej prokuratury zawiadomienie o podejrzeniu popełnienia kilku czynów zabronionych, spenalizowanych w ustawie o ochronie danych osobowych,¹⁴⁹ polegających na: przetwarzaniu danych osobowych bez podstawy prawnej, nie zgłoszeniu do rejestracji zbioru danych osobowych i niedopełnieniu obowiązku informacyjnego określonego w art. 24 lub art. 25 ustawy.

Generalny Inspektor jeszcze w 2005 r. podjął interwencję odnośnie gromadzenia przez jednego z przedsiębiorców telekomunikacyjnych numeru PESEL oraz oznaczenia typu i numeru

¹⁴⁶ GI-DS-430/258/05.

¹⁴⁷ GI-DS-430/447/06, GI-DOLiS-430/41/06.

¹⁴⁸ GI-DS-430/481/06.

¹⁴⁹ Zawiadomienie z dnia 22 grudnia 2006 r. o sygn. GI-DS-430/481/06/677/DOLiS.

dokumentu tożsamości w postępowaniu reklamacyjnym.¹⁵⁰ Dane te były gromadzone poprzez formularz reklamacyjny dostępny na stronie internetowej przedsiębiorcy. Generalny Inspektor stanął na stanowisku, iż jakkolwiek przedsiębiorca telekomunikacyjny ma prawo przetwarzać niniejsze dane na mocy art. 161 ust. 2 Prawa telekomunikacyjnego, to ich gromadzenie w postępowaniu reklamacyjnym nie jest uprawnione. Zgodnie bowiem z § 2 ust. 1 rozporządzenia Ministra Infrastruktury z dnia 1 października 2004 r. w sprawie trybu postępowania reklamacyjnego oraz warunków, jakim powinna odpowiadać reklamacja usługi telekomunikacyjnej (Dz. U. Nr 226, poz. 2291), reklamacja powinna zawierać m.in. imię i nazwisko, przydzielony reklamującemu numer reklamacji, numer ewidencyjny nadany reklamującemu przez dostawcę usług lub adres miejsca zakończenia sieci oraz podpis reklamującego – w przypadku reklamacji złożonej w formie pisemnej. Wśród danych tych nie został wymieniony numer PESEL, ani typ i numer dokumentu tożsamości. Z uwagi na fakt, iż zakres danych wymaganych w związku ze zgłoszeniem reklamacji przedsiębiorcy telekomunikacyjnemu został określony w szczególnych przepisach prawa nie może on samodzielnie zakresu tego zmieniać dowolnie go rozszerzając.

13) Sektor zatrudnienia

Liczba skarg z sektora dotyczącego zatrudnienia wzrosła w stosunku do liczby tych, które wpłynęły do GIODO w latach 2004-2005. W przeciwieństwie do roku 2005, w 2006 r. nie wpłynęły do GIODO skargi na działania pracodawców polegające na nie wypełnianiu przez nich obowiązku informacyjnego, jaki wynika z art. 33 ustawy. Znacząco przeważały - podobnie jak w roku 2004 i 2005 - skargi związane z problemem udostępniania danych osobowych pracowników osobom trzecim. Nie odnotowano jednak sytuacji, które miały miejsce w latach poprzednich, tj. dysponowania aktami osobowymi pracowników przez podmioty nieupoważnione, nie będące administratorami danych, do którego dochodziło, np. wskutek porzucenia akt.

Najczęściej jako nieuzasadnione kwalifikowano skargi, które poruszały zagadnienia udostępnienia danych uregulowane w odrębnych przepisach prawa,¹⁵¹ np. w toku postępowania toczącego się w odrębnym trybie,¹⁵² jak procedury administracyjnej (gdy pracodawca zapoznawał się z danymi w toku postępowania administracyjnego), czy cywilnej.¹⁵³ Jako nie występujące dotychczas należy zakwalifikować skargi na udostępnianie danych osobowych pracowników, z którymi pracodawca pozostaje w sporze na skutek upublicznianie ich w szerokim zakresie na stronach

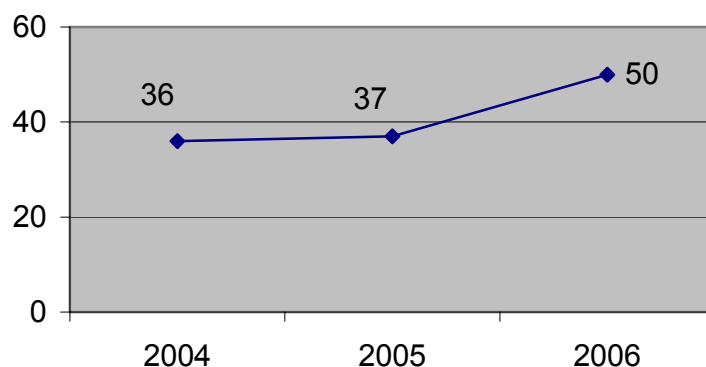
¹⁵⁰ GI-DP-024/126/05 i następnie GI-DP-024/1411/06.

¹⁵¹ Np. GI-DS-430/25/06, GI-DS-430/28/06, GI-DS-430/38/06, GI-DS-430/166/06, GI-DS-430/194/06, GI-DS-430/230/06, GI-DS-430/263/06, GI-DS-430/264/06, GI-DS-430/281/06, GI-DS-430/472/06, GI-DS-430/503/06, GI-DS-430/504/06, GI-DS-430/539/06, GI-DS-430/573/06, GI-DS-430/579/06, GI-DOLiS-430/10/06, GI-DOLiS-430/15/06.

¹⁵² A więc są dopuszczalne na podstawie art. 23 ust. 1 pkt 2 ustawy.

¹⁵³ Było to dopuszczalne na podstawie – obowiązującego w momencie wszczęcia postępowania upadłościowego - art. 97 Rozporządzenia Prezydenta Rzeczypospolitej z dnia 24 października 1934 r. Prawo upadłościowe (Dz. U. z 1991 r. Nr 118, poz. 512 ze zm.).

internetowych i intranetowych.¹⁵⁴ Rozpowszechnianie tego typu informacji spotykało się także z zarzutami skarżących co do naruszenia ich dóbr osobistych, których ocenę GODO pozostawiał sądowi powszechnemu jako organowi kompetentnemu.



Wykres 17: Zestawienie porównawcze liczby skarg dotyczących sektora zatrudnienia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

Wartych odnotowania jest także kilka stwierdzonych przez GODO przypadków błędnych zachowań pracodawców polegających na udostępnieniu przez nich danych osobowych pracowników osobom nieupoważnionym. We wszystkich tych przypadkach udostępnienie danych osobowych miało związek z konfliktem powstałym pomiędzy pracodawcą i pracownikiem.

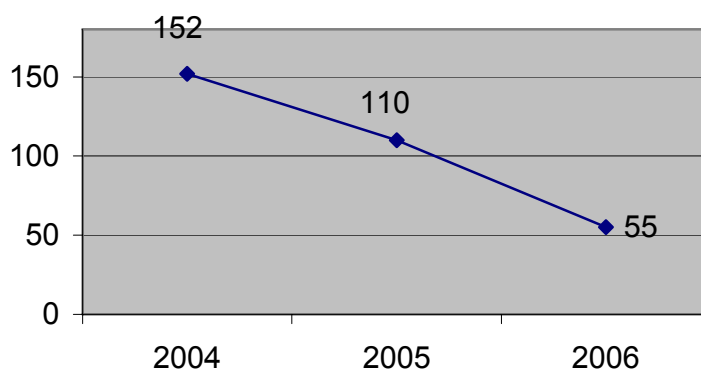
Przypadek nieprawidłowego udostępnienia przez pracodawcę danych osobowych byłego pracownika odnotowano w postępowaniu ze skargi na podanie danych osobowych do publicznej wiadomości poprzez zamieszczenie ich na witrynie intranetowej pracodawcy,¹⁵⁵ w zakresie obejmującym imię, nazwisko, stopień naukowy skarżącego oraz informacje o: zwolnieniu z pracy, o treści postanowienia sądu pracy w przedmiocie zabezpieczenia powództwa i o aktualnym miejscu zatrudnienia skarżącego. Wbrew opinii pracodawcy, w sprawie tej upublicznienie danych stanowiło przetwarzanie danych osobowych, które nie znajdowało podstawy prawnej w żadnej z przesłanek przetwarzania danych. Takie działanie nie mogło być uznane w szczególności za niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez pracodawcę. GODO uznał, że cel w postaci ochrony interesów spółki, na który powołał się w tej sprawie pracodawca mógł być osiągnięty bez publikowania danych osobowych skarżącego, byłego pracownika spółki. Wskazywana przez pracodawcę konieczność zapewnienia aktualnym bądź potencjalnym klientom rzetelnych informacji o spółce nie wymaga podawania danych osób, które szerzą na temat spółki informacje nieprawdziwe.

¹⁵⁴ GI-DS-430/357/06.

¹⁵⁵ GI-DS-430/357/06.

14) Windykacja

Część rozpatrywanych skarg dotyczyła także przetwarzania danych osobowych przez podmioty głównie z sektora prywatnego w celach windykacyjnych. Egzekwowanie należności od dłużników związane jest nierozłącznie z przetwarzaniem danych osobowych, a czynności podmiotów specjalizujących się w odzyskiwaniu wierzytelności należało oceniać albo jako wykonywanie działań windykacyjnych w charakterze samoistnego administratora danych wskutek ich pozyskania na podstawie umowy cesji wierzytelności, albo jako działanie w imieniu i na rzecz administratorów danych-wierzycieli.¹⁵⁶ Na przestrzeni ubiegłych lat liczba skarg w tym zakresie ulegała sukcesywnemu spadkowi, na co wpływ miało niewątpliwie orzecznictwo sądów administracyjnych.



Wykres 18: Zestawienie porównawcze liczby skarg dotyczących sektora windykacji, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

Rozpatrując w latach poprzednich i do połowy 2005 r. skargi, z których wynikało, że u podstaw udostępnienia danych znajdowała się cesja wierzytelności - a więc, gdy następowała zmiana administratora danych, bez pozyskania zgody osoby, której dane dotyczyły – GODO stał na stanowisku, iż działania takie nie były dopuszczalne w świetle przepisów Kodeksu cywilnego.¹⁵⁷ Argumentacja uzasadniająca to stanowisko została szeroko zaprezentowana w sprawozdaniu z działalności organu zarówno za rok 2004, jak i 2005. Początkowo sądy podzielały tę opinię,¹⁵⁸ ale została ona zmieniona wskutek kolejnych wyroków.¹⁵⁹ Naczelny Sąd Administracyjny w poszerzonym

¹⁵⁶ Tj. na podstawie art. 31 ustawy lub pełnomocnictwa.

¹⁵⁷ Art. 385³ pkt 5 i art. 385¹ § 1 K.c.

¹⁵⁸ Sygn. akt: II SA 1549/03, II SA 1563/03, II SA 1603/03, II SA 1631/03, II SA 1630/03, II SA 1974/03.

¹⁵⁹ GI-DEC-DS-90/05 z dnia 29 kwietnia 2005 r. w sprawie GI-DS-430/36/04, GI-DEC-DS-82/05 z dnia 25 kwietnia 2005 r. w sprawie GI-DS-430/443/04, GI-DEC-DS-92/05 z dnia 29 kwietnia 2005 r. w sprawie GI-DS-430/529/04, GI-DEC-DS-79/05 z dnia 25 kwietnia 2005 r. w sprawie GI-DS-430/608/04, GI-DEC-DS-76/05 z dnia 22 kwietnia 2005 r. w sprawie GI-DS-430/618/04, GI-DEC-DS-91/05 z dnia 29 kwietnia 2005 r. w sprawie GI-DS-430/781/04, GI-DEC-DS-81/05 z dnia 25 kwietnia 2005 r. w sprawie GI-DS-430/821/04, GI-DEC-DS-78/05 z dnia 22 kwietnia 2005 r. w sprawie GI-DS-430/751/04, GI-DEC-DS-94/05 z dnia 29 kwietnia 2005 r. w sprawie GI-DS-430/924/04.

składzie rozstrzygnął, iż w kwestii udostępnienia danych w związku ze sprzedażą wierzytelności¹⁶⁰ działanie to jest dopuszczalne dla wypełnienia prawnie usprawiedliwionych celów administratora danych, a przetwarzanie to nie narusza praw i wolności osoby, której dane dotyczą, z uwagi na konieczność dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej.¹⁶¹

W rozstrzygnięciach wydawanych w sprawach dotyczących przetwarzania danych osobowych w związku z dochodzeniem wierzytelności – których najwięcej wydano w sektorze telekomunikacji - za w pełni uzasadnione uznawane było prowadzenie postępowania windykacyjnego przez pracowników administratora w jego imieniu i na jego rzecz, jak również korzystanie przez administratorów z instytucji powierzenia przetwarzania¹⁶² danych podmiotom trzecim.¹⁶³ Choć liczbę skarg dotyczących omawianej problematyki maleje, co należy przypisać m.in. utrwalonej już w tym zakresie linii orzeczniczej, to jednak nadal błędnie interpretowana jest przesłanka zgody, jako jedyna uprawniająca wierzyciela do przekazania danych osobowych dłużnika w celu odzyskania należności.

W roku sprawozdawczym 2006, po analizie spraw z zakresu windykacji, warto wskazać na nowy rodzaj administratorów, którzy dochodzą wierzytelności, ewentualnie udostępniają dane osobowe dłużników w związku z dochodzeniem wierzytelności. Mianowicie są to agencje nieruchomości, podmioty zajmujące się dostawą energii, lub pobierający opłaty eksploatacyjne z tytułu użytkowania mieszkania.

Przykładem może być skarga wierzyciela na odmowę udostępnienia danych osobowych klientów spółki zajmującej się budową i sprzedażą domów oraz mieszkań, celem przekazania tych danych komornikowi sądowemu.¹⁶⁴ Wierzyciel powołał się na nakaz zapłaty wydany przez sąd okręgowy wobec dłużników wskazując, że jest zobowiązany do podania komornikowi we wniosku o wszczęcie egzekucji danych osobowych oraz przedmiotów, z których ma zostać wszczęta egzekucja. GODO odmówił w tej sprawie uwzględnienia wniosku¹⁶⁵ stwierdzając, że wskazana przez wierzyciela

¹⁶⁰ W sprawie sprzedaży wierzytelności w 2005 r., a następnie w 2006 r. GODO przyjął i stosował interpretację przepisów prawa wskazaną przez NSA, która nie zmieniła się w kolejnych wydawanych w tych sprawach wyrokach WSA w Warszawie. Zob. np. wyrok WSA z dnia 21 września 2005 r. sygn. akt II SA/Wa 1443/05, wyrok WSA z dnia 21 września 2005 r. sygn. akt II SA/Wa 1444/05. W 2006 r. sądy administracyjne uchylały decyzje GODO wydane w tych sprawach w poprzednich latach. Zob. np. wyrok WSA z dnia 27 stycznia 2006 r., sygn. akt II SA/Wa 2077/05, wyrok NSA z dnia 30 marca 2006 r., sygn. akt I OSK 628/05, wyroki WSA z dnia 31 marca 2006 r., sygn. akt II SA/Wa 2396/04, sygn. akt SA/Wa 2395/04, wyrok NSA z dnia 27 kwietnia 2006 r., sygn. akt I OSK 711/05.

¹⁶¹ Art. 23 ust. 1 pkt 5 w związku z art. 23 ust. 4 pkt 2 ustawy o ochronie danych osobowych.

¹⁶² Przewidzianej przez ustawodawcę w art. 31 ustawy.

¹⁶³ Np. decyzja z dnia 22 czerwca 2006 r., znak: GI-DEC-DS-203/06 i decyzja z dnia 21 sierpnia 2006 r., znak: GI-DEC-DS-309/06 w sprawie GI-DS-430/47/06 i GI-DS-430/48/06; decyzja z dnia 30 czerwca 2006 r., znak: GI-DEC-DS-229/06 w sprawie GI-DS-430/17/06; decyzja z dnia 30 sierpnia 2006 r., znak: GI-DEC-DS-336/06 w sprawie GI-DS-430/213/06; decyzja z dnia 26 września 2006 r., znak: GI-DEC-DS-369/06 w sprawie GI-DS-430/342/06; decyzja z dnia 5 października 2006 r., znak: GI-DEC-DS-384/06 w sprawie GI-DS-430/171/06.

¹⁶⁴ GI-DS-430/312/06.

¹⁶⁵ Decyzja z dnia 10 listopada 2006 r., znak: GI-DEC-DS-420/06.

przesłanka udostępnienia danych¹⁶⁶ nie może znaleźć zastosowania w tej sprawie, gdyż udostępnienie danych – w zakresie numerów działek i lokali należący do dłużników oraz numerów ich ksiąg wieczystych, stanu prawnego lokali, praw dłużników do lokali, numerów i serii dowodów osobistych oraz numerów PESEL dłużników – nie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów, które miały by być realizowane przez wierzyciela. W szczególności pozyskanie takich danych nie jest niezbędne do dochodzenia roszczeń z tytułu prowadzonej przez wierzyciela działalności gospodarczej. Pozyskanie danych będących przedmiotem wniosku nie było również niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.¹⁶⁷ Jak wynika ze stosownych przepisów,¹⁶⁸ jedynym podmiotem uprawnionym na mocy przepisów prawa do otrzymania żądanych danych jest komornik, co odnosi się także do sytuacji, gdy wierzyciel nie może uzyskać informacji niezbędnych do wszczęcia lub prowadzenia postępowania egzekucyjnego. Ponadto, jak ustalił GODO, posiadanie przez wierzyciela danych objętych wnioskiem nie jest warunkiem wszczęcia postępowania egzekucyjnego. Z tych względów GODO przyjął, że w sprawie tej nie można było mówić o niezbędności posiadania przez wierzyciela, żądanych przez niego danych, do realizacji uprawnienia wynikającego z przepisu prawa, czy do wypełnienia prawnie usprawiedliwionego celu odbiorcy danych.

Dodać ponadto należy, że podobnie jak w latach ubiegłych, w dalszym ciągu w wielu przypadkach mylona jest cesja wierzytelności dokonana na podstawie przepisów art. 509 Kodeksu cywilnego i zlecenie przez administratora wykonywania czynności windykacyjnych na podstawie pełnomocnictwa, (art. 96 K.c.) i dokonywania czynności prawnych przez przedstawiciela (art. 95 K.c.), z instytucją powierzenia przetwarzania danych, przewidzianą przez ustawodawcę w art. 31 ustawy o ochronie danych osobowych.

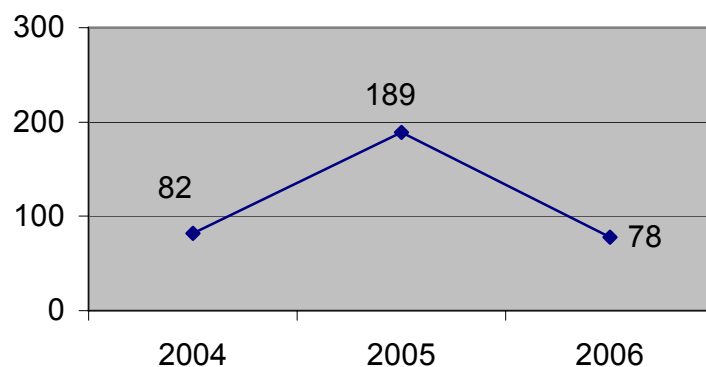
15) Inne

Tematyka skarg zakwalifikowanych do tego sektora jest niezmienna od kilku lat i dotyczy najczęściej takich naruszeń, jak legalność przetwarzania i udostępniania danych osobowych.

¹⁶⁶ Art. 23 ust. 1 pkt 5 w związku z art. 23 ust. 4 pkt 2 ustawy o ochronie danych osobowych.

¹⁶⁷ Art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

¹⁶⁸ Ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 ze zm.), rozporządzenia Ministra Sprawiedliwości z dnia 9 marca 1968 r. w sprawie czynności komorników (Dz. U. Nr 10, poz. 52 ze zm.) i ustawy z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (Dz. U. z 2001 r., Nr 124, poz. 1361 ze zm.).



Wykres 19: Zestawienie porównawcze liczby skarg z sektora Inne, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2006.

Zarzuty tego rodzaju stawiane były przede wszystkim kancelariom prawnym, choć w większości przypadków były one nieuzasadnione. Wykonywanie czynności na danych odbywało się zazwyczaj na podstawie przepisów prawa bądź w prawnie usprawiedliwionym celu administratora danych, lub ich odbiorców.¹⁶⁹ W dalszym ciągu, choć w mniejszym stopniu niż w latach ubiegłych, sygnalizowano o zbieraniu (udostępnianiu) przez podmioty z tego sektora danych osobowych w zbyt szerokim zakresie, wykraczającym poza przepisy prawa i zasady wyznaczone ustawą.¹⁷⁰ Inny z poruszanych problemów odnosił się do wypełniania obowiązków informacyjnych z art. 24, art. 25 i art. 33 ustawy.¹⁷¹ Nie stwierdzono jednak w analizowanych przypadkach wielu uchybień. Zmniejszyła się też liczba skarg na nie zapewnienie opcjonalności przy formułowaniu klauzul zgody na przetwarzanie danych osobowych w różnych celach. Jednocześnie mniej nieprawidłowości odnotowano w aspekcie związanym z zabezpieczaniem danych.¹⁷² W tym zakresie sytuacja na przestrzeni kilku lat uległa znacznej poprawie, co wskazuje, że administratorzy danych z sektora prywatnego przywiązują obecnie większą wagę do nałożonych na nich ustawą obowiązków techniczno-organizacyjnych w związku z koniecznością ochrony danych.

Nowym zagadnieniem w tym sektorze było natomiast przetwarzanie merytorycznie niepoprawnych danych, jak miało to miejsce w przypadku dwóch spraw, gdzie w jednej - zakład energetyczny, w drugiej – przedsiębiorca świadczący usługi dostawy gazu i dokonującego rozliczeń

¹⁶⁹ Decyzja z dnia 17 stycznia 2006 r. o sygn. GI-DEC-DS-166/06 i decyzja ją utrzymująca z dnia 9 maja 2006 r. o sygn. GI-DEC-DS-148/06 w sprawie GI-DS-430/590/05; decyzja z dnia 17 stycznia 2006 r. o sygn. GI-DEC-DS-17/06 i decyzja ją utrzymująca z dnia 9 maja 2006 r. o sygn. GI-DEC-DS-146/06 w sprawie GI-DS-430/648/05.

¹⁷⁰ GI-DS-430/218/06, GI-DS-430/121/06, GI-DS-430/518/06.

¹⁷¹ Decyzja z dnia 24 sierpnia 2006 r. o sygn. GI-DEC-DS-316/06 i decyzja ją utrzymująca z dnia 24 listopada 2006 r. o sygn. GI-DEC-DS-433/06 w sprawie GI-DS-430/258/06; GI-DS-430/17/06.

¹⁷² GI-DS-430/9/06, GI-DS-430/460/06.

płatności¹⁷³ odmówił osobie skarżącej sprostowania nazwiska, uzasadniając powyższe względami natury technicznej. Tymczasem administrator danych na mocy przepisów ustawy zobowiązany jest do przetwarzania merytorycznie poprawnych danych. W praktyce oznacza to, że informacje wynikające z przetwarzanych danych powinny być zgodne z prawdą, kompletne, poprawnie utrwalone oraz powinny odpowiadać aktualnemu stanowi rzeczy. W tym przypadku odmowa sprostowania danych we wnioskowanym zakresie, uzasadniania wyłącznie względami natury technicznej, była zatem całkowicie nieuzasadniona.¹⁷⁴

Zupełnie inny problem wystąpił w sprawie, w której poskarżono się na odmowę udostępnienia przez spółdzielnię, prowadzącą szeroko pojętą działalność gastronomiczną, jej członkowi danych osobowych innych członków spółdzielni zawartych w rejestrze.¹⁷⁵ Spółdzielnia udostępniła skarżącemu jedynie część znajdujących się tam informacji, odmawiając prawa do zapoznania się z całością rejestru z uwagi na konieczność ochrony danych osobowych jej członków. Tak wybiórcze podejście do udostępniania informacji, w tym danych osobowych zawartych w rejestrze członków spółdzielni, uzasadniane ponadto obowiązkami wynikającymi z ustawy, było jednak całkowicie nieuprawnione. Członkowi spółdzielni przysługuje bowiem prawo dostępu do wszystkich danych zgromadzonych w rejestrze w zakresie przewidzianym w przepisach Prawa spółdzielczego oraz w statucie spółdzielni. Nakazując zatem uzupełnienie przekazanych skarżącemu informacji o pozostałe dane zawarte w rejestrze, GODO jednocześnie podkreślił, że dbałość o przestrzeganie zasad związanych z ochroną danych osobowych nie może prowadzić do niezgodnego z prawem ograniczania dostępu do danych osobowych.¹⁷⁶

Z kolei inna ze spraw, prowadzona z urzędu, poruszała tematykę nieprawidłowego wywiązywania się przez podmiot z opisywanego sektora z obowiązku informacyjnego, określonego w art. 24 ustawy.¹⁷⁷ W formularzu zgłoszeniowym, za pomocą którego były pozyskiwane dane osobowe klientów, zabrakło bowiem informacji o prawie dostępu do treści danych oraz ich poprawiania, jak też o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, oraz o jego podstawie prawnej.

W 2006 r. pojawiło się również zagadnienie związane z legalnością przetwarzania danych osobowych przez notariuszy, w tym wypełniania przez nich obowiązku informacyjnego, o którym mowa w art. 25 ustawy. W skardze inicjującej postępowanie w tym zakresie wskazano na przetwarzanie przez notariusza danych skarżącego bez jego zgody oraz wiedzy.¹⁷⁸ Jak ustalono, dane

¹⁷³ GI-DS-430/323/06.

¹⁷⁴ Decyzją z dnia 26 września 2006 r. o sygn. GI-DEC-DS-368/06 nakazano administratorowi danych osobowych skarżącej sprostowanie jej nazwiska. Obecnie sprawę rozpoznaje WSA w Warszawie.

¹⁷⁵ GI-DS-430/278/06.

¹⁷⁶ Decyzja z dnia 30 sierpnia 2006 r. o sygn. GI-DEC-DS-337/06.

¹⁷⁷ GI-DS-430/170/06.

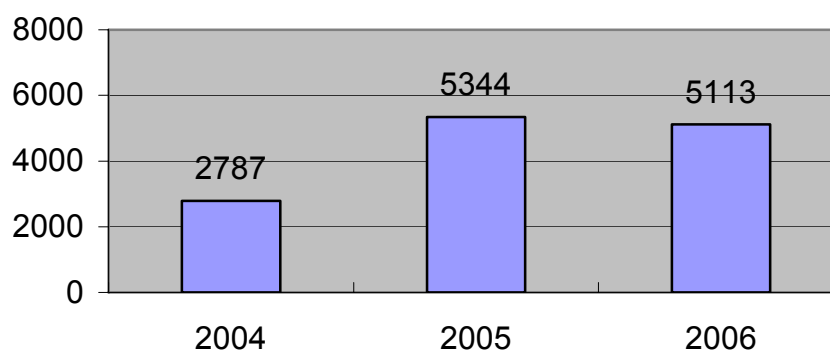
¹⁷⁸ GI-DS-430/398/06.

osobowe skarżącego - jako współwłaściciela nieruchomości - zostały ujawnione w akcie notarialnym, dotyczącym nabycia przez osobę trzecią udziału w tej nieruchomości po zmarłym bracie. Przetwarzanie danych osobowych skarżącego w tym kontekście nie było jednak czynnością nieuprawnioną, znajdowało bowiem oparcie w przepisach prawa, w szczególności w ustawie z dnia 14 lutego 1991 r. Prawo o notariacie (Dz. U. z 2002 r. Nr 42, poz. 369 ze zm.) oraz w przepisach Kodeksu postępowania cywilnego. Jednocześnie na notariuszu – wbrew twierdzeniom skarżącego - nie spoczywał obowiązek informacyjny, bowiem w tym przypadku znalazł zastosowanie art. 25 ust. 2 pkt 5 ustawy, zwalniający z jego wypełnienia podmioty niepubliczne realizujące zadania publiczne. Do takich podmiotów należy zaś zaliczyć m.in. notariuszy.¹⁷⁹ Zatem i w tym przypadku brak było powodów, aby uwzględnić wniosek skarżącego.¹⁸⁰

4. Prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach

Jednym z ustawowych zadań Generalnego Inspektora Ochrony Danych Osobowych jest prowadzenie rejestru zbiorów danych osobowych oraz udzielanie informacji o zarejestrowanych zbiorach. Głównym celem rejestracji jest zapewnienie przejrzystości w sferze przetwarzania danych osobowych oraz stworzenie warunków do sprawowania indywidualnej oraz urzędowej kontroli nad przestrzeganiem zasad przyjętych w ustawie o ochronie danych osobowych.

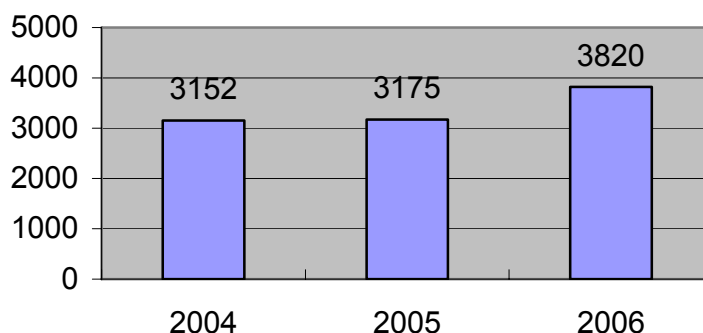
Realizując obowiązek zgłoszenia zbioru danych do rejestracji, administratorzy danych w 2006 r. zgłosili 5113 zbiorów. Najwięcej zbiorów danych zgłosiły podmioty z sektora administracji publicznej (3351).



Wykres 20: Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2004–2006

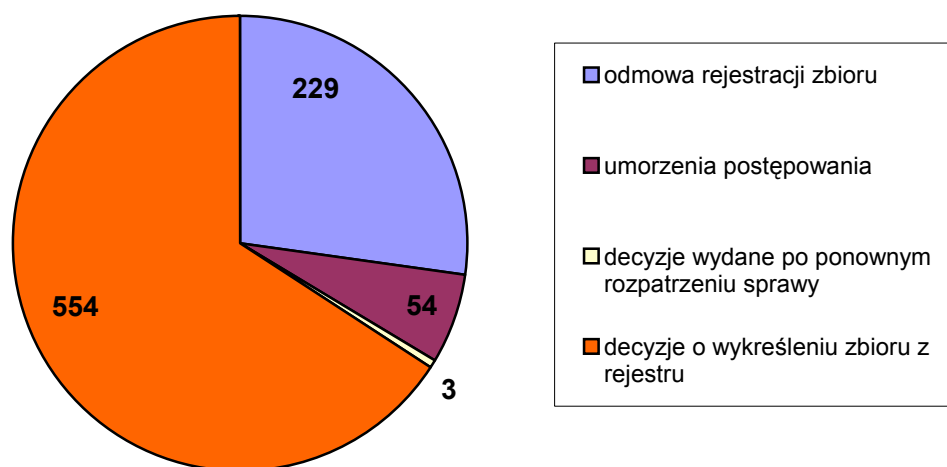
¹⁷⁹ Takie stanowisko przyjął także Wojewódzki Sąd Administracyjny w wyroku z dnia 2 listopada 2004 r. (III SA 2861/2003).

¹⁸⁰ Decyzja z dnia 20 października 2006 r. o sygn. GI-DEC-DS-398/06.



Wykres 21: Liczbowe zestawienie zbiorów danych zarejestrowanych w latach 2004–2006.

Ponadto, Generalny Inspektor wydawał decyzje administracyjne w sprawach związanych ze zgłoszeniami do rejestracji zbiorów danych osobowych. W 2006 roku GODO wydał łącznie 840 decyzji administracyjnych przygotowanych w Departamencie Rejestracji Zbiorów Danych Osobowych, z czego 229 stanowiły decyzje o odmowie rejestracji zbioru danych, 54 – decyzje o umorzeniu postępowania, 3 – decyzje wydane po ponownym rozpatrzeniu sprawy oraz 554 – decyzje o wykreśleniu zbioru danych z rejestru.



Wykres 22: Zestawienie decyzji administracyjnych dotyczących postępowań rejestrowych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2006 roku.

W roku sprawozdawczym 2006, Generalny Inspektor wydał ponadto 43 postanowienia w związku ze zgłoszeniami zbiorów danych do rejestracji. W porównaniu z rokiem 2005, odnotować należy ponad dwukrotny wzrost liczby decyzji o wykreśleniu zbioru danych z rejestru.

Biorąc pod uwagę ogół spraw związanych z rejestracją zbiorów danych osobowych należy zauważyć, iż dominującymi pod względem ilościowym, a zarazem wymagającymi z reguły przeprowadzenia postępowania wyjaśniającego, były zgłoszenia z obszarów związanych ze szkolnictwem wyższym, systemem oświaty, sądownictwem, szeroko rozumianą pomocą społeczną oraz marketingiem.

W roku ubiegłym 2005, zanotowano istotny wzrost liczby dokonywanych przez publiczne i niepubliczne szkoły wyższe, zgłoszeń do rejestracji zbiorów danych dotyczących osób ubiegających się o przyjęcie na studia. Należy podkreślić, iż zgłaszanie przez uczelnie wyższe zbiorów danych kandydatów na studia nie było procesem samoistnym, lecz reakcją na działania podjęte przez Ministra Nauki i Szkolnictwa Wyższego, w odpowiedzi na sygnalizację GIODO.¹⁸¹ Wskutek nie wywiązywania się szkół wyższych z ustawowego obowiązku zgłaszania do rejestracji posiadanych zbiorów danych, Generalny Inspektor - ramach swoich uprawnień nadzorczych – zwrócił się do Ministra Nauki i Szkolnictwa Wyższego o spowodowanie, aby reprezentujący uczelnie rektorzy dopełnili obowiązku rejestracyjnego dotyczącego zbiorów danych kandydatów na studia. Przeprowadzana przez uczelnie wyższe procedura rekrutacji wymaga przetwarzania wielu danych osobowych. Każdy kandydat na studenta składa bowiem szereg dokumentów zawierających informacje o charakterze osobowym (np. świadectwo dojrzałości, odpis dyplomu), nie tylko identyfikujących kandydata, ale także świadczących m.in. o przebiegu wykształcenia, nabytych umiejętnościach, zdobytych nagrodach, czy też innych osiągnięciach.¹⁸² Należy przy tym negatywnie odnieść się do stanowiska prezentowanego przez niektórych administratorów danych, iż powołane zbiory zwolnione są, na podstawie art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych, z obowiązku rejestracji, bądź mu nie podlegają, z uwagi na spełnienie przesłanki doraźności, o której mowa w art. 2 ust. 3 tej ustawy. O ile bowiem zbiory danych osób uczących się u administratora danych, w tym przypadku studentów, są faktycznie zwolnione z obowiązku rejestracji, o tyle przesłanka zwalniająca z tego obowiązku nie odnosi się do zbiorów danych osób ubiegających się o przyjęcie na studia. Nie można również podzielić opinii, iż niniejsze zbiory danych, należałoby traktować jako sporządzane doraźnie, wyłącznie w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, do których to zbiorów mają zastosowanie jedynie przepisy rozdziału 5 ustawy o ochronie danych osobowych. Biorąc bowiem pod uwagę prawny obowiązek uczelni przechowywania przez 12 miesięcy

¹⁸¹ Pismo Generalnego Inspektora z dnia 17 sierpnia 2006 r. o sygn. GI-DRZDO-400/19/06.

¹⁸² Do odbywania studiów w uczelni może być, na podstawie art. 169 ust. 1 ustawy z dnia 27 lipca 2005 r. - Prawo o szkolnictwie wyższym (Dz. U. Nr 164, poz. 1365 ze zm.), dopuszczona osoba, która ma: - świadectwo dojrzałości – w przypadku ubiegania się o przyjęcia na studia pierwszego stopnia lub jednolite studia magisterskie, - tytuł magistra, licencjata, inżyniera lub równorzędny – w przypadku ubiegania się o przyjęcia na studia drugiego stopnia, oraz spełnia warunki rekrutacji ustalone przez uczelnię. Warunki i tryb rekrutacji oraz formy studiów na poszczególnych kierunkach ustala senat uczelni. Uchwałę podaje się do wiadomości publicznej nie później niż do dnia 31 maja roku poprzedzającego rok akademicki, którego uchwała dotyczy i przesyła ministrowi właściwemu do spraw szkolnictwa wyższego (art. 169 ust. 2 wymienionej ustawy).

kopii dokumentów kandydatów nieprzyjętych na I rok studiów¹⁸³ oraz mając na względzie fakt, iż procedura rekrutacji osób ubiegających się o przyjęcie na studia wyższe odbywa się cyklicznie i następuje w związku z wykonywaniem podstawowych zadań uczelni, nie można uznać zbioru tworzego na potrzeby przeprowadzenia postępowania kwalifikacyjnego za zbiór danych sporządzany doraźnie. Warto odnotować, iż do chwili wystosowania sygnalizacji dotyczącej obowiązku rejestracji zbiorów danych, tylko jeden rektor dokonał w imieniu uczelni zgłoszenia do rejestracji zbioru zawierającego dane osób ubiegających się o przyjęcie na studia. Interwencja Generalnego Inspektora przyniosła efekt w postaci zgłoszenia przez uczelnie do końca 2006 r. w sumie 70 zbiorów danych kandydatów na studia wyższe.

W omawianym roku sprawozdawczym 2006, utrzymała się tendencja zgłaszania do rejestracji zbiorów danych prowadzonych w ramach systemu informacji oświatowej.¹⁸⁴ Służący uzyskiwaniu danych niezbędnych do prowadzenia polityki edukacyjnej państwa system informacji oświatowej obejmuje prowadzone przez różne podmioty bazy danych, w skład których wchodzi zbiory danych o szkole lub placówce oświatowej; uczniach, słuchaczach, wychowankach oraz absolwentach; nauczycielach, wychowawcach i innych pracownikach, a także spełnianiu obowiązku nauki. W świetle określonej w ustawie o ochronie danych osobowych definicji danych osobowych, jedynymi zbiorami, spośród prowadzonych w ramach systemu informacji oświatowej, zawierającymi dane osobowe, są zbiory dotyczące nauczycieli, wychowawców i innych pracowników pedagogicznych, o których mowa w art. 3 ust. 4 pkt 1 ustawy o systemie informacji oświatowej. Tylko te zbiory podlegają przepisom ustawy o ochronie danych osobowych. Pozostałe zbiory, w szczególności dotyczące uczniów, zawierają jedynie informacje zbiorcze, na podstawie których nie jest możliwe ustalenie, jakich konkretnie osób informacje te dotyczą.

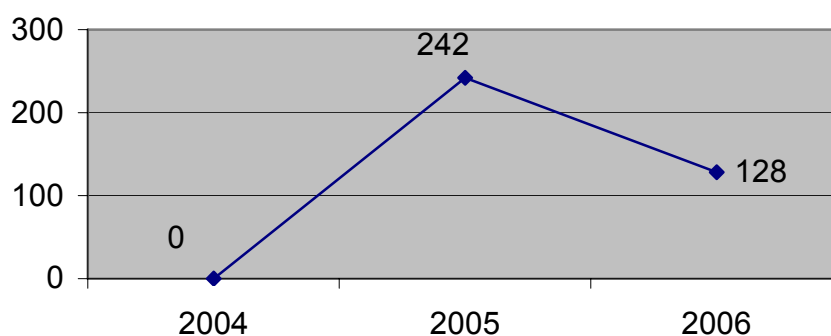
W świetle prawa, jednostki samorządu terytorialnego prowadzące bazy danych oświatowych obejmujące m.in. zbiory danych z baz oświatowych szkół i placówek oświatowych prowadzonych przez te jednostki, są administratorami danych osobowych zgromadzonych w tych zbiorach. Często jednak zgłoszeń do rejestracji dokonywały nie jednostki samorządu terytorialnego, lecz podmioty prowadzące obsługę ekonomiczno-administracyjną szkół i placówek.¹⁸⁵ Nadmienić przy tym należy, iż wspomniane podmioty zgłaszały nie tylko zbiory prowadzone na podstawie ustawy o systemie informacji oświatowej, ale także zbiory związane ze świadczeniem pomocy materialnej o charakterze

¹⁸³ Zgodnie z § 21 ust. 2 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 2 listopada 2006 r. w sprawie dokumentacji przebiegu studiów (Dz. U. Nr 224, poz. 1634).

¹⁸⁴ Na podstawie ustawy z dnia 19 lutego 2004 r. o systemie informacji oświatowej (Dz. U. Nr 49, poz. 463 ze zm.).

¹⁸⁵ Zgodnie z art. 5 ust. 7 ustawy z dnia 7 września 1991 r. o systemie oświaty (tekst jednolity: Dz. U. z 2004 r. Nr 256, poz. 2572 ze zm.), organ prowadzący szkołę lub placówkę odpowiada za jej działalność. Do zadań organu prowadzącego szkołę lub placówkę należy m.in. zapewnienie obsługi administracyjnej, finansowej i organizacyjnej tej szkoły lub placówki. W celu wykonywania wymienionych zadań dopuszcza się możliwość tworzenia jednostek obsługi ekonomiczno-administracyjnej szkół i placówek lub organizowania wspólnej obsługi administracyjnej, finansowej i organizacyjnej prowadzonych szkół i placówek (art. 5 ust. 9 ustawy o systemie oświaty).

socjalnym dla uczniów, prowadzone w oparciu o ustawę o systemie oświaty.¹⁸⁶ Z analizy przepisów, w obu tych przypadkach, wynikał jednoznaczny wniosek, iż jednostki obsługi ekonomiczno-administracyjnej nie decydują o celach i środkach przetwarzania danych osobowych, a tym samym nie ma podstaw do uznania ich za administratorów danych przetwarzanych w ww. zbiorach danych. Stąd też celem postępowań wyjaśniających było spowodowanie, aby faktyczni administratorzy danych dokonali zgłoszeń zbiorów danych. Problemy, jakie pojawiły się w związku z rejestracją zbiorów dotyczących systemu informacji oświatowej dotyczyły przetwarzania przez administratorów danych zbyt szerokiego, wykraczającego poza katalog ustawowy, zakresu danych. Każde zgłoszenie, z którego wynikało, iż w zbiorze gromadzone są imiona i nazwiska osób, których dane dotyczą, wymagało wezwania administratora danych do złożenia wyjaśnień, gdyż ustawa o systemie informacji oświatowej nie przewiduje możliwości przetwarzania takich informacji. Procedurę rejestracji utrudniało dodatkowo zgłaszanie przez jednostki samorządu terytorialnego na jednym formularzu zgłoszenia, kilku zbiorów danych osobowych, np. zbioru związanego z funkcjonowaniem systemu informacji oświatowej oraz zbioru służącego realizacji świadczeń pomocy materialnej o charakterze socjalnym.



Wykres 23: Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji z zakresu systemu informacji oświatowej w latach 2004–2006.

Spośród zbiorów zgłoszonych do rejestracji przez organizacje społeczne wyróżnić można nadesłane przez Fundację Ośrodka KARTA zgłoszenie zbioru danych dokumentującego straty osobowe i ofiary represji pod okupacją niemiecką.¹⁸⁷ Dane zbierane w ramach przedmiotowego zbioru służą wypełnieniu statutowych celów Fundacji¹⁸⁸ i są niezbędne do wykonania przez nią zadania

¹⁸⁶ Zgodnie z art. 90m ust. 1 ustawy o systemie oświaty, świadczenie pomocy materialnej o charakterze socjalnym przyznaje wójt, burmistrz lub prezydent miasta.

¹⁸⁷ Zgłoszenie nr R 004286/06.

¹⁸⁸ Statutowa działalność Fundacji polega m.in. na wywoływaniu, gromadzeniu, przechowywaniu, opracowywaniu i upowszechnianiu źródeł, danych, świadectw historycznych i literackich związanych z historią XX wieku, dotyczących

publicznego na zlecenie Instytutu Pamięci Narodowej oraz Ministra Kultury i Dziedzictwa Narodowego w ramach programu naukowo-badawczego. Celem przetwarzania danych w niniejszym zbiorze było zebranie i możliwie pełna analiza oraz weryfikacja danych obywateli polskich represjonowanych przez okupanta niemieckiego w latach 1939-1945. Dane te będą pomocne osobom poszukującym dokumentów potwierdzających fakt represji oraz rodzinom osób zaginionych w czasie okupacji niemieckiej. Zwłaszcza, że zostaną one w ograniczonym zakresie udostępnione w Internecie. Pozostałe dane, w tym szczególnie chronione, będą niedostępne dla osób niezwiązanych z realizacją programu. Administrator danych rozważa też możliwość udostępnienia pełnej treści danych historykom, badaczom, którym dane mogą być przydatne do prac naukowo-badawczych. Nadanie dostępu do pełnej wersji programu byłoby uzależnione od złożenia pisemnego wniosku wraz z uzasadnieniem zawierającym m.in. opis celów badawczych, kwalifikacje i miejsce pracy wnioskodawcy. Zbiór ten został zarejestrowany.

Jedno ze stowarzyszeń nadesłało do Generalnego Inspektora zgłoszenie do rejestracji zbioru danych podopiecznych „Domu dla dzieci i młodzieży”, prowadzonego na podstawie rozporządzenia Ministra Polityki Społecznej z dnia 14 lutego 2005 r. w sprawie placówek opiekuńczo - wychowawczych (Dz. U. Nr 37, poz. 331).¹⁸⁹ Wnioskodawca wskazał, iż w przedmiotowym zbiorze gromadzone będą dane ujawniające kod genetyczny. Ze złożonych przez stowarzyszenie wyjaśnień wynikało, iż przetwarza ono informacje o ogólnym, końcowym wyniku badania mającego na celu ustalenie lub zaprzeczenie ojcostwa mężczyzn, w odniesieniu do których przeprowadzane są takie badania. Zgłoszenie przez wnioskodawcę, iż przetwarza on dane ujawniające kod genetyczny wynikało zatem z błędnej interpretacji stanu faktycznego, gdyż tego rodzaju dane nie były przez niego przetwarzane. Niniejszy zbiór został wpisany do rejestru prowadzonego przez GODO.

W 2006 r. utrzymała się, zapoczątkowana dwa lata wcześniej, tendencja zgłaszania do rejestracji prowadzonych w sądach zbiorów danych zawierających dane osobowe m.in. ławników, kuratorów społecznych, mediatorów i kandydatów na syndyków.¹⁹⁰ Z analizy zgłoszeń nadesłanych do rejestracji z tego zakresu wynika, iż w dalszym ciągu problem stanowiła kwestia ujawniania przynależności partyjnej w zbiorach danych ławników. Praktyka taka nie znajdowała i nie znajduje żadnego uzasadnienia w obowiązujących przepisach prawa.¹⁹¹ Generalny Inspektor, jeszcze przed

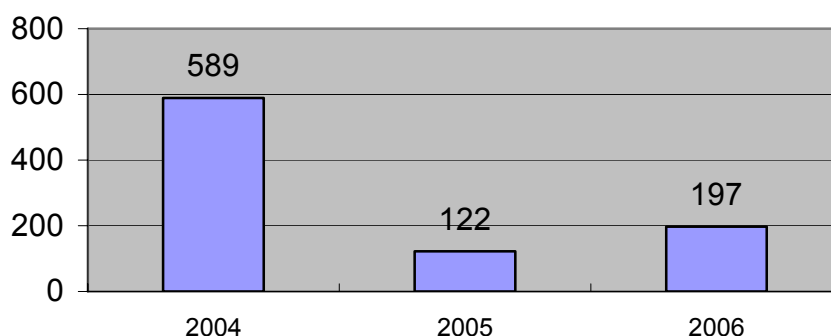
losów jednostek, środowisk i społeczeństw, szczególnie w systemach totalitarnych, służących ochronie pamięci i dziedzictwa kulturowego.

¹⁸⁹ Zgłoszenie nr R 003408/05.

¹⁹⁰ Zagadnienie to omówione zostało w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, Część II, lit. O, pkt 2, Sądy.

¹⁹¹ Zgodnie z art. 162 § 1 ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070 ze zm.) kandydatów na ławników zgłaszają radom gmin prezesi sądów, stowarzyszenia, organizacje pracodawców oraz inne organizacje zarejestrowane na podstawie przepisów prawa, z wyłączeniem partii politycznych, oraz co najmniej dwudziestu pięciu obywateli mających czynne prawo wyborcze, zamieszkujących stale na danym terenie, w terminie do dnia 30 czerwca ostatniego roku kadencji.

wprowadzeniem ustawowego zapisu *expressis verbis* zakazującego zgłaszania kandydatów na ławników przez partie polityczne, konsekwentnie prezentował stanowisko negujące dopuszczalność przetwarzania tego rodzaju informacji w odniesieniu do ławników. Działania podejmowane w toku rejestracji miały na celu przywrócenie stanu zgodnego z prawem poprzez usunięcie z posiadanej przez administratorów danych dokumentacji, informacji mogących ujawniać przynależność partyjną ławników. Interwencje te odniosły pozytywny skutek również dzięki stanowisku resortu sprawiedliwości, podzielającego w niniejszej kwestii pogląd Generalnego Inspektora.

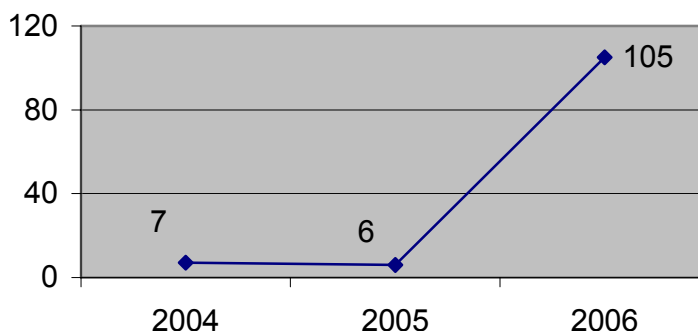


Wykres 24: Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji przez sądy w latach 2004–2006.

W roku sprawozdawczym 2006, Generalny Inspektor otrzymał 104 zgłoszenia zbiorów danych osób, w odniesieniu do których wydawane są orzeczenia o niepełnosprawności, orzeczenia o stopniu niepełnosprawności oraz orzeczenia o wskazaniach do ulg i uprawnień osób posiadających orzeczenia o inwalidztwie lub niezdolności do pracy. Powyższe zbiory zgłaszane były do rejestracji przez Powiatowe Centra Pomocy Rodzinie, Powiatowe Zespoły do Spraw Orzekania o Niepełnosprawności oraz powiaty. Zgodnie z przepisami aktów normatywnych stanowiących podstawę prowadzenia przedmiotowych zbiorów, Powiatowy Zespół do Spraw Orzekania o Niepełnosprawności będący organem właściwym w sprawie orzekania o niepełnosprawności osób stale przebywających na terenie powiatu, na zasadach określonych w ustawie o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, wydaje orzeczenia w przedmiocie ustalenia niepełnosprawności, stopnia niepełnosprawności lub wskazań do ulg i uprawnień.¹⁹² Analiza powyższych przepisów pozwala na stwierdzenie, że to Powiatowe Zespoły do Spraw Orzekania o Niepełnosprawności decydują o celach i środkach przetwarzania danych osobowych, a tym samym są administratorami danych przetwarzanych we ww. zbiorach danych. Stąd też celem postępowań

¹⁹² Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. Nr 123, poz. 776 ze zm.) oraz rozporządzenie Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 15 lipca 2003 r. w sprawie orzekania o niepełnosprawności i stopniu niepełnosprawności (Dz. U. Nr 139, poz. 1328 ze zm.).

wyjaśniających było spowodowanie, aby faktyczni administratorzy danych dokonali zgłoszeń zbiorów danych, dopełniając obowiązek rejestracyjny, przewidziany w ustawie o ochronie danych osobowych.



Wykres 25: Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w związku z wydawaniem orzeczeń osobom niepełnosprawnym w latach 2004–2006.

Administratorzy dokonujący zgłoszeń zbiorów danych prowadzonych w celu marketingowym niejednokrotnie wskazywali, że pozyskują dane osobowe w bardzo szerokim zakresie. Generalny Inspektor zwracał się w tych sprawach o złożenie wyjaśnień. Konieczne było bowiem ustalenie w jakim celu podmioty te gromadzą tak szeroki katalog danych oraz czy spełniony został wymóg adekwatności określony przepisami ustawy o ochronie danych osobowych.¹⁹³ Administratorzy prowadzący powyższe zbiory wyjaśniali najczęściej, że pozyskują dane także w celu identyfikacji osób biorących udział w organizowanych konkursach i akcjach promocyjnych oraz dokonywania rozliczeń podatkowych (w odniesieniu do osób, które otrzymują nagrody). Nie zawsze jednak argumentacja przytaczana przez te podmioty stanowiła wystarczające uzasadnienie pozyskiwania danych do zbiorów związanych z prowadzonymi działaniami marketingowymi, a w konsekwencji przetwarzanie przez nie danych osobowych sprzeczne było z zasadą adekwatności wyrażoną w przepisach ustawy o ochronie danych osobowych. Naruszenie zasady adekwatności, stanowi zaś przesłankę wydania decyzji o odmowie rejestracji zbioru danych.¹⁹⁴ W związku z powyższym Generalny Inspektor odmówił rejestracji takich zbiorów danych.

¹⁹³ Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych administrator przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były adekwatne w stosunku do celów, w jakich są przetwarzane.

¹⁹⁴ Zgodnie z przepisem art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych, Generalny Inspektor wydaje decyzję o odmowie rejestracji zbioru danych, jeżeli przetwarzanie naruszałoby zasady określone w art. 23-30 tej ustawy.

W związku ze zmianą przepisów dotyczących świadczenia pomocy prawnej¹⁹⁵ należało ustalić, czy osoby świadczące pomoc prawną lecz nie wpisane na listę radców prawnych lub listę adwokatów są zobowiązane do zgłoszenia zbiorów danych klientów do rejestracji Generalnemu Inspektorowi. Na mocy art. 43 ust. 1 pkt 5 ustawy o ochronie danych osobowych, z obowiązku rejestracji zwolnieni są administratorzy danych dotyczących osób korzystających z obsługi adwokackiej oraz obsługi radcy prawnego. Użycie przez ustawodawcę w treści powyższego przepisu sformułowań „obsługa adwokacka” oraz „obsługa radcy prawnego” oznacza, iż zwolnienie z obowiązku zgłoszenia zbioru do rejestracji skonstruowane zostało w ujęciu podmiotowym. Z obowiązku rejestracji zwolnieni są zatem administratorzy danych osób, które korzystają z ich usług, a administratorzy ci legitymują się ponadto wpisem na listę radców prawnych lub listę adwokatów. W związku z powyższym, zwolnienie z obowiązku rejestracji nie odnosi się do osób, które są uprawnione do świadczenia pomocy prawnej lecz nie wpisanych na listę adwokatów lub radców prawnych, a tym samym nie legitymujących się tytułem zawodowym adwokata lub radcy prawnego. Mając na uwadze powyższe, zbiory danych prowadzone w związku ze świadczeniem obsługi prawnej przez osoby posiadające wyższe wykształcenie prawnicze lecz nie legitymujące się tytułem zawodowym adwokata lub radcy prawnego zostały wpisane do rejestru prowadzonego przez Generalnego Inspektora.

W 2006 r., podobnie jak miało to miejsce w 2005 r., Generalny Inspektor przy postępowaniach rejestrowych zetknął się z praktyką zlecania podmiotowi prywatnemu wykonywania czynności w zakresie kontroli ruchu drogowego oraz prowadzenia postępowania mandatowego (obsługa tzw. fotoradarów, sporządzanie dokumentacji stanowiącej podstawę wystawienia mandatu karnego bądź występowanie do sądu z wnioskiem o ukaranie kierowcy).¹⁹⁶ Organ do spraw ochrony danych podtrzymał swoje wcześniejsze stanowisko, iż wykonywanie czynności w wyżej wskazanym zakresie przez pracowników podmiotu prywatnego, stanowi naruszenie przepisów będących podstawą wykonywania tych czynności. Zatem postępowania w sprawie zgłoszenia zbioru do rejestracji zostały zakończone wydaniem decyzji o odmowie rejestracji.¹⁹⁷ W toku prowadzonych postępowań w sprawie rejestracji powyższych zbiorów danych, wnioskodawcy oświadczali również, iż przywrócili stan zgodny z prawem, tj. zaprzestali przekazywania danych gromadzonych w tych zbiorach

¹⁹⁵ Na mocy przepisów ustawy z dnia 30 czerwca 2005 r. o zmianie ustawy – Prawo o adwokaturze i niektórych innych ustaw (Dz. U. Nr 75, poz. 471 ze zm.), osoby posiadające wyższe wykształcenie prawnicze uzyskały uprawnienie do świadczenia pomocy prawnej, z wyjątkiem zastępstwa procesowego, chyba że osoby te działają na podstawie art. 87 § 1 Kodeksu postępowania cywilnego w charakterze pełnomocnika pozostającego w stałym stosunku zlecenia, jeżeli przedmiot sprawy wchodzi w zakres tego zlecenia, bądź też sprawującego zarząd majątkiem lub interesami strony. Przepisy te przestały obowiązywać w dniu 1.01.2007 r.

¹⁹⁶ Stanowisko Generalnego Inspektora w tej materii zostało przedstawione w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, Część II, lit. B, pkt 2 Straże Miejskie.

¹⁹⁷ Np. decyzja z dnia 15 grudnia 2006 r. o sygn. GI-DRZDO/401/DEC/002325/05-826/06.

przedsiębiorcom prywatnym oraz zapewnili warunki, w których wszystkie zgromadzone w nich dane przetwarzane są wyłącznie przez podmioty upoważnione na podstawie przepisów prawa. W takich przypadkach zbiory danych zostały wpisane do rejestru prowadzonego przez Generalnego Inspektora.

Ogólna ocena zgłoszonych do rejestracji zbiorów danych uprawnia do stwierdzenia, iż podobnie jak w latach ubiegłych, znaczna liczba zgłoszeń zawierała uchybienia uniemożliwiające wpisanie zbioru do rejestru bez przeprowadzania postępowania wyjaśniającego. Zaistniałe uchybienia dotyczyły zarówno wymogów formalnoprawnych, jak i merytorycznej zawartości wniosków. Administratorzy danych wskazywali zbyt szeroki zakres przetwarzanych danych osobowych, nieadekwatny w stosunku do celu ich pozyskiwania. Często zgłoszenia nie zawierały określenia przesłanki legalności przetwarzania danych, jak również brakowało wskazania sposobu zbierania i udostępniania danych osobowych. Oprócz błędów wymienionych powyżej, liczne uchybienia pojawiały się także w części zgłoszenia dotyczącej informacji o sposobie wypełnienia warunków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36 – 39 ustawy. Niejednokrotnie także deklarowany przez administratorów danych poziom bezpieczeństwa przetwarzania danych w systemie informatycznym nie spełniał warunków określonych w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Istotnym i dość często powtarzającym się błędem administratorów danych, wynikającym częściowo z niezrozumienia pojęcia „zbioru danych”, było łączne zgłaszanie do rejestracji, na jednym formularzu zgłoszenia, kilku zbiorów danych osobowych, realizujących odmienne cele, prowadzonych w oparciu o różne przesłanki legalności przetwarzania danych, w których dane osobowe przetwarzane były w różnym zakresie. Wymienić w tym miejscu można zgłoszenia dokonywane przez stowarzyszenia, które razem ze zbiorami dotyczącymi swoich podopiecznych, niejednokrotnie zresztą zawierającymi dane szczególnie chronione, zgłaszały do rejestracji zbiory danych osób przekazujących darowizny na rzecz stowarzyszenia. Podobna sytuacja występowała w zgłaszanych przez ośrodki pomocy społecznej zbiorach zawierających zarówno dane osób pobierających świadczenia rodzinne, jak i uprawnionych z tytułu świadczeń alimentacyjnych.¹⁹⁸ W każdym ze wspomnianych przypadków celem prowadzonego w sprawie postępowania wyjaśniającego było spowodowanie zgłoszenia przez administratora danych każdego zbioru oddzielnie, tj. na odrębnym formularzu zgłoszenia zbioru danych do rejestracji. Szczególnie istotne jest bowiem zapewnienie, aby prowadzony przez

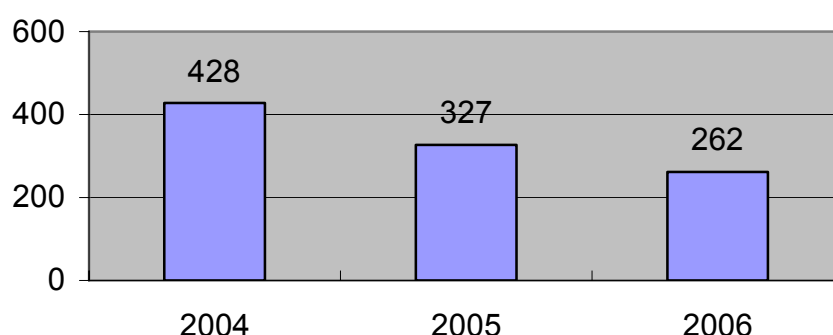
¹⁹⁸ Zbiory danych prowadzone na podstawie ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (tekst jednolity Dz. U. z 2006 Nr 139, poz. 992 ze zm.) oraz ustawy z dnia 22 kwietnia 2005 r. o postępowaniu wobec dłużników alimentacyjnych oraz zaliczce alimentacyjnej (Dz. U. Nr 86, poz. 732 ze zm.).

Generalnego Inspektora rejestr zbiorów danych osobowych odzwierciedlał faktyczny stan przetwarzania danych przez poszczególnych administratorów wraz z informacjami właściwymi dla konkretnych zbiorów danych.

5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych

Istotną rolę w działalności Generalnego Inspektora odgrywa opiniowanie projektów aktów normatywnych w ramach procesu legislacyjnego, co pozwala na wyeliminowanie nieprawidłowości już na etapie tworzenia prawa.

W 2006 roku Generalnemu Inspektorowi Ochrony Danych Osobowych przedłożone zostały do zaopiniowania 262 projekty.



Wykres 26: Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania Generalnemu Inspektorowi Ochrony Danych Osobowych w latach 2004-2006.

Podobnie jak w latach ubiegłych, przedkładane do zaopiniowania projekty wprowadzały sformułowania umożliwiające przechowywanie przez administratorów danych wszelkiego rodzaju dokumentów zawierających dane osobowe przez nieograniczony czas. Generalny Inspektor Ochrony Danych Osobowych informował wówczas, że z punktu widzenia ustawy o ochronie danych osobowych istotne jest, aby dane były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania.¹⁹⁹ W sytuacji, gdy cel przetwarzania jest bliżej niesprecyzowany, a jego realizacja odległa w czasie, nie można mówić o zgodności takiego rozwiązania z przepisami ustawy o ochronie danych osobowych.²⁰⁰

¹⁹⁹ Art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych wprowadza zasadę ograniczenia czasowego przetwarzania danych. Czasowym wyznacznikiem dopuszczalności gromadzenia i przechowywania danych jest osiągnięcie zamierzonego celu przetwarzania.

²⁰⁰ Wskazane uwagi zostały zgłoszone m.in. do projektu rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie pobierania danych z tachografu cyfrowego, ich przechowywania i przekazywania ich właścicielom (GI-DP-023/301/05/06); projektu ustawy o Centralnym Biurze Antykorupcyjnym (GI-DP-023/320/05/06, GI-DP-023/64/06) i projektu ustawy o zmianie ustawy – Prawo farmaceutyczne oraz niektórych innych ustaw (GI-DP-023/163/06).

Istotnym błędem w procesie tworzenia prawa było naruszanie regulacji art. 27 ustawy o ochronie danych osobowych, dotyczącej przetwarzania danych szczególnie chronionych. Zgodnie z ust. 2 pkt 2 wskazanego przepisu, przetwarzanie danych szczególnie chronionych (np. danych o stanie zdrowia) jest dopuszczalne jedynie na podstawie przepisu rangi ustawowej, stwarzającego przy tym pełne gwarancje ich ochrony. Tymczasem w nadsyłanych projektach przewidziano określenie zakresu i przesłanek dopuszczalności przetwarzania danych szczególnie chronionych w aktach wykonawczych (rozporządzeniach). Generalny Inspektor kwestionował powyższe rozwiązanie wskazując na – wynikający wprost z ustawy o ochronie danych osobowych – różny poziom ochrony danych tzw. zwykłych (jak np. imię i nazwisko, adres, PESEL, NIP) i danych szczególnie chronionych. W przypadku danych tzw. zwykłych określenie katalogu przetwarzanych danych może być zawarte w powszechnie obowiązujących aktach prawnych o randze niższej niż ustawa, natomiast gdy chodzi o dane szczególnie chronione istnieje konieczność określenia tego katalogu w ustawie (umowie międzynarodowej ratyfikowanej za uprzednią zgodą wyrażoną w ustawie w trybie art. 89 ust. 1 Konstytucji RP).²⁰¹

Powtarzającym się uchybieniem było wprowadzanie do projektów aktów prawnych ogólnych sformułowań mogących powodować trudności interpretacyjne, np. „inne informacje”, „diagnoza sytuacji rodzinnej”, „dane osobowe”, „dane umożliwiające identyfikację pacjenta”, „wykaz osób”. Generalny Inspektor podkreślał, że następstwem użycia w przepisach niezdefiniowanych pojęć może być pozyskiwanie danych w zbyt szerokim zakresie, nieadekwatnym do realizowanego celu.²⁰² Organ ochrony danych osobowych proponował zatem takie sformułowanie treści przepisów, które nie będzie budziło wątpliwości co do zakresu przetwarzanych danych osobowych.²⁰³

W okresie objętym sprawozdaniem przedmiotem szczególnej troski Generalnego Inspektora było zapewnienie zgodności projektowanych przepisów z regulacjami konstytucyjnymi w zakresie

²⁰¹ Wskazane uwagi zostały zgłoszone m.in. do projektu rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wniosków i dokumentów w sprawach pobytu na terytorium Rzeczypospolitej Polskiej obywateli państw członkowskich Unii Europejskiej i członków ich rodzin (GI-DP-023/141-143/06); do projektu rozporządzenia Ministra Obrony Narodowej w sprawie prowadzenia ewidencji wojskowej (GI-DP-023/77/06); do projektu rozporządzenia Ministra Sprawiedliwości w sprawie szczegółowych zasad prowadzenia strony internetowej w celu wykonywania środka karnego — opublikowania wizerunku sprawcy, sposobu i trybu umieszczania oraz usuwania z tej strony podlegających opublikowaniu informacji oraz podmiotów do tego uprawnionych (GI-DOLiS-023/7/06).

²⁰² Brak wyraźnego określenia zakresu danych osobowych może prowadzić do naruszenia zasady adekwatności, określonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którą administrator może gromadzić dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane.

²⁰³ Uwagi w przedmiotowej kwestii zostały zgłoszone przez Generalnego Inspektora m.in. do projektu rozporządzenia Rady Ministrów zmieniającego rozporządzenie w sprawie ustalenia okoliczności i przyczyn wypadków przy pracy oraz sposobu ich dokumentowania, a także zakresu informacji zamieszczanych w rejestrze wypadków przy pracy (GI-DP-023/125/06); do projektu rozporządzenia Ministra Pracy i Polityki Społecznej w sprawie określenia standardu podstawowych usług świadczonych przez specjalistyczne ośrodki wsparcia dla ofiar przemocy w rodzinie, a także szczegółowych kierunków prowadzenia oddziaływań korekcyjno – edukacyjnych (GI-DP-023/30/06); do projektu rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych (GI-DP-023/112-113/06); do projektu ustawy o spółdzielni europejskiej (GI-DP-023/9/06).

prawa do prywatności (art. 47 Konstytucji Rzeczypospolitej Polskiej) i ochrony danych osobowych (art. 51 Konstytucji Rzeczypospolitej Polskiej). W tej kwestii wskazywał on uchybienia projektodawców polegające na wprowadzeniu w ustawach ograniczeń powyższych praw i wolności obywatelskich bez wykazania niezbędności tych ograniczeń w demokratycznym państwie prawnym ze względu na bezpieczeństwo lub porządek publiczny, bądź ochronę środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób (art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej).²⁰⁴ Zasygnalizować także należy, iż w niektórych projektach aktów prawnych znalazły się unormowania, które bez jakiegokolwiek uzasadnienia głęboko ingerowały w sferę prywatności (a nawet intymności) osób fizycznych.²⁰⁵ Dokonując oceny przepisów z punktu widzenia standardów konstytucyjnych Generalny Inspektor wskazywał na – ugruntowane w tym przedmiocie – orzecznictwo Trybunału Konstytucyjnego, który w szeregu orzeczeń zawarł wytyczne dotyczące dopuszczalności ingerencji ustawodawcy w sferę praw i wolności obywatelskich.²⁰⁶

Do zaopiniowania Generalnemu Inspektorowi Ochrony Danych Osobowych zostało przedłożonych kilkanaście **projektów rozporządzeń dotyczących instytucji finansowych**,²⁰⁷ spośród których część stanowiła akty wykonawcze do ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych (Dz. U. Nr 146, poz. 1546 ze zm.),²⁰⁸ część – akty wykonawcze do ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. Nr 183, poz. 1538 ze zm.),²⁰⁹ część – akty wykonawcze do ustawy z dnia 29 września 1994 r. o rachunkowości (tekst jednolity: Dz. U. z 2002 r. Nr 76, poz. 694 ze zm.)²¹⁰ oraz jeden projekt aktu wykonawczego do ustawy z dnia 29 lipca 2005 r.

²⁰⁴ Uwagi do projektu ustawy o zmianie ustawy o Policji, zmianie ustawy o Straży Granicznej oraz niektórych innych ustaw (GI-DP-023/14–15/06) oraz uwagi wspólne do projektów ustaw: o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990 oraz treści tych dokumentów oraz o zmianie innych ustaw; o zmianie ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu; o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw (GI-DP-023/33, 34, 35/06).

²⁰⁵ Projekt ustawy o osobach kierujących pojazdami (GI-DP-023/107/06); projekt rozporządzenia Prezesa Rady Ministrów zmieniającego rozporządzenie w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2006 (GI-DP-023/300/05/06, GI-DP-023/307/05/06).

²⁰⁶ Tytułem przykładu wskazać można: orzeczenie Trybunału Konstytucyjnego z dnia 24 czerwca 1997 roku sygn. akt K. 21/96, OTK ZU z 1997 roku, zesz. 2, poz. 23 – uzasadnienie; wyrok Trybunału Konstytucyjnego z dnia 11 kwietnia 2000 roku sygn. akt K. 15/98, OTK ZU z 2000 roku, zesz. 3, poz. 86 – uzasadnienie.

²⁰⁷ Pismo Ministerstwa Finansów z dnia 1 marca 2006 r. o sygn. FI/PKS/116/2006. Odpowiedź GIODO z dnia 20 marca 2006 r. o sygn. GI-DP-023/37-52/06.

²⁰⁸ Np. projekt rozporządzenia Rady Ministrów zmieniającego rozporządzenie w sprawie szczegółowych warunków wykonywania przez towarzystwo funduszy inwestycyjnych działalności w zakresie zarządzania zbiorczymi portfelami papierów wartościowych, projekt rozporządzenia Rady Ministrów zmieniającego rozporządzenie w sprawie sprawozdań finansowych zbiorczego portfela papierów wartościowych oraz inne (brak uwag).

²⁰⁹ Np. projekt rozporządzenia Ministra Finansów w sprawie wymogów, jakim powinny odpowiadać wnioski domów maklerskich o wydanie zezwolenia na niektóre czynności w ramach prowadzonej działalności maklerskiej (brak uwag), projekt rozporządzenia Ministra Finansów w sprawie wzorów wniosków o wpis na listę maklerów papierów wartościowych oraz na listę doradców inwestycyjnych (brak uwag), projekt rozporządzenia Ministra Finansów w sprawie wykazu tytułów uprawniających do ubiegania się o wpis na listę doradców inwestycyjnych (brak uwag) i inne.

²¹⁰ Np. projekt rozporządzenia Ministra Finansów zmieniającego rozporządzenie w sprawie szczegółowych zasad rachunkowości funduszy inwestycyjnych (brak uwag).

o nadzorze nad rynkiem kapitałowym (Dz. U. Nr 183, poz. 1537 ze zm.).²¹¹ Uwagi Generalnego Inspektora, zgłoszone do niektórych z nich, dotyczyły w zasadzie kwestii braku określenia zakresu danych osobowych w projektowanych przepisach, co mogło w praktyce wiązać się z naruszeniem zasady adekwatności przetwarzania danych osobowych wyrażonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.²¹² Ponadto, w projekcie rozporządzenia Ministra Finansów w sprawie określenia warunków technicznych i organizacyjnych wymaganych do prowadzenia działalności maklerskiej przez firmę inwestycyjną oraz do prowadzenia rachunków papierów wartościowych przez bank powierniczy, Generalny Inspektor zakwestionował zasadność i celowość wyłączenia z zabezpieczeń przed niekontrolowanym dostępem osób nieuprawnionych podmioty w postaci punktów przyjmowania zleceń (ust. 6) oraz zagranicznej firmy inwestycyjnej (ust. 7), a także brak uregulowania okresu, przez jaki mają być przechowywane dane zawarte w rejestrze skarg składanych na działalność firmy inwestycyjnej (§ 14).

W związku z pracami nad zmianą **ustaw o Policji oraz o Straży Granicznej**²¹³ Generalny Inspektor zakwestionował przepisy wprowadzające nowe zasady składania przez funkcjonariuszy Policji i funkcjonariuszy Straży Granicznej oświadczeń majątkowych. W oświadczeniu majątkowym znaleźć się miały bowiem nie tylko informacje obejmujące prywatny majątek funkcjonariusza oraz majątek objęty małżeńską wspólnością ustawową, lecz także odrębny majątek jego małżonka oraz majątek innych osób, które pozostają z nim we wspólnym gospodarstwie domowym.²¹⁴ Zdaniem Generalnego Inspektora tak daleka ingerencja w prywatność osób pozostających z funkcjonariuszem w określonym stosunku osobistym, rodzi wątpliwość co do zgodności przyjętego rozwiązania z zasadą proporcjonalności wyrażoną w art. 31 ust. 3 Konstytucji RP. Ponadto, w bogatym orzecznictwie Trybunału Konstytucyjnego panuje ugruntowany pogląd, że prawo do ochrony życia prywatnego sformułowane w art. 47 Konstytucji RP²¹⁵ obejmuje także ochronę tajemnicy danych dotyczących sytuacji majątkowej obywatela.²¹⁶ Dodatkowo, zakres danych objętych oświadczeniem majątkowym funkcjonariusza miał być określony w rozporządzeniu wykonawczym, nie zaś w ustawie, co w świetle

²¹¹ Projekt rozporządzenia Ministra Finansów w sprawie szczegółowego trybu przeprowadzania kontroli podmiotów podlegających nadzorowi Komisji Papierów Wartościowych i Giełd (brak uwag).

²¹² § 55 projektu rozporządzenia Ministra Finansów w sprawie trybu i warunków pożyczania maklerskich instrumentów finansowych, z udziałem firm inwestycyjnych oraz banków powierniczych – co do zakresu informacji, jakie ma zawierać rejestr zleceń; § 2 ust. 3 oraz § 3 ust. 2 projektu rozporządzenia Ministra Finansów w sprawie szczegółowych zasad organizacyjnego wydzielenia działalności maklerskiej banku – co do zakresu informacji, jakie ma zawierać lista osób wykonujących czynności przyjmowania zleceń nabycia lub zbycia maklerskich instrumentów finansowych; § 48 ust. 1 pkt 1, § 50 ust. 1 pkt 1, § 51 ust. 1 pkt 1, § 52 ust. 1 pkt 1 oraz § 74 ust. 1 pkt 1 projektu rozporządzenia Ministra Finansów w sprawie zakresu, trybu, formy oraz terminów dostarczania informacji przez niektóre podmioty prowadzące działalność maklerską oraz rachunki papierów wartościowych – co do danych osobowych stron umowy.

²¹³ Przekazane pismem z dnia 20 stycznia 2006 r. o sygn. L-I-2270/05 i L-I-2271/05. Odpowiedź GIODO z dnia 3 lutego 2006 r. o sygn. GI-DP-023/14-15/06.

²¹⁴ Art. 1 pkt 23 projektu ustawy o zmianie ustawy o Policji oraz art. 1 pkt 8 projektu ustawy o Straży Granicznej.

²¹⁵ Zgodnie z tym przepisem, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

wyroku Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. (sygn. akt K 32/04) – zdaniem Generalnego Inspektora może być uznane za sprzeczne z art. 51 ust. 5 Konstytucji RP.²¹⁷ Uwagi zostały uwzględnione.²¹⁸

Nieprawidłowości z punktu widzenia ustawy o ochronie danych osobowych zawierał także **projekt ustawy o zmianie ustawy o czasie pracy kierowców oraz o zmianie niektórych innych ustaw**.²¹⁹ Pojawiła się, podobnie jak w wielu innych projektach aktów prawnych, kwestia braku określenia wyraźnego (poprzez użycie zwrotu „w szczególności”) zakresu danych, jakie mają być gromadzone w poszczególnych dokumentach²²⁰ oraz konstrukcja zobowiązująca pracodawcę do przechowywania rozkładu czasu pracy kierowcy przez co najmniej rok po upływie okresu nim objętego,²²¹ nie wyznaczając przy tym maksymalnego czasu przechowywania tego dokumentu.²²² Generalny Inspektor zakwestionował także proponowane zwolnienie podmiotów prowadzących warsztaty w zakresie napraw, instalacji lub sprawdzania tachografów cyfrowych z obowiązku zgłoszenia GIODO do rejestracji zbiorów danych osobowych pobranych z tachografów cyfrowych i kart do nich oraz przechowywanych w celu przekazania tych danych właścicielom.²²³ Uwagi Generalnego Inspektora zostały uwzględnione.

Wątpliwości z punktu widzenia ustawy o ochronie danych osobowych wywołał także przekazany do zaopiniowania **projekt ustawy o osobach kierujących pojazdami**.²²⁴ Projektowane przepisy nakładały na lekarza przeprowadzającego badanie kandydata na kierującego albo kierującego, obowiązek przekazywania staroście właściwemu ze względu na miejsce zamieszkania osoby badanej ankiety dotyczącej stanu jej zdrowia. Generalny Inspektor zakwestionował legalność i celowość przekazania staroście informacji o stanie zdrowia zawartych w ankiecie. Projektowane przepisy nie

²¹⁶ Orzeczenie TK z dnia 24 czerwca 1997 r., sygn. akt K 21/96, OTK ZU z 1997 r., zesz. 2, poz. 23 – uzasadnienie; wyrok TK z dnia 11 kwietnia 2000 r., sygn. akt K 15/98, OTK ZU z 2000 r., zesz. 3, poz. 86 – uzasadnienie.

²¹⁷ Zgodnie z art. 51 ust. 5 Konstytucji RP, zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

²¹⁸ Oświadczenia majątkowe funkcjonariuszy Policji i Straży Granicznej będą obejmowały majątek odrębny funkcjonariusza oraz majątek objęty małżeńską wspólnością majątkową.

²¹⁹ Pismo Ministerstwa Transportu z dnia 5 września 2006 r. o sygn. ML-2w-020-49/2006. Odpowiedź GIODO z dnia 17 października 2006 r. o sygn. GI-DP-023/183/06.

²²⁰ Rozwiązanie takie pozostaje w sprzeczności z wiążącą administratorów danych zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych).

²²¹ Art. 31f ust. 3 projektu ustawy, „Rozkład czasu pracy kierowcy jest przechowywany przez pracodawcę lub podmiot, na rzecz którego wykonywane są przewozy przez co najmniej rok po upływie okresu nim objętego”.

²²² Art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych nakłada na administratorów danych obowiązek zapewniania, by przetwarzane przez nich dane były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania.

²²³ Wyłączenie od obowiązku rejestracji dotyczyć może jedynie zbiorów o charakterze szczególnym i wymaga każdorazowo wyczerpującego uzasadnienia. Zaproponowana regulacja wymogu tego nie spełniała, a zbiór podlegający – zgodnie z projektem – wyłączeniu od obowiązku rejestracji nie wykazywał żadnych specyficznych cech przemawiających za takim szczególnym potraktowaniem.

²²⁴ Pismo Ministerstwa Transportu z dnia 8 maja 2006 r. o sygn. ML2c-020-3-06/623311. Odpowiedź GIODO z dnia 19 maja 2006 r. o sygn. GI-DP-023/107/06.

stwarzały bowiem pełnej gwarancji ochrony danych,²²⁵ jak również trudno było wskazać cel, dla którego starosta miałby gromadzić dane o stanie zdrowia kierujących pojazdami.²²⁶ Ponadto, projektowane przepisy przyznawały osobom, które w imieniu odpowiedniego starosty lub wojewody kontrolują przebieg szkolenia (przebieg egzaminu), uprawnienia do prowadzenia niejawniej obserwacji za pomocą urządzenia technicznego służącego do zapisu obrazu i dźwięku. Generalny Inspektor wskazał, iż wzgląd na elementarne swobody obywatelskie w państwie demokratycznym przemawia za ograniczeniem prawa do stosowania technik operacyjnych wyłącznie do odpowiednio przeszkolonych i nadzorowanych funkcjonariuszy Policji oraz służb specjalnych. Przepisy projektowanej ustawy miały na celu także gromadzenie w Centralnej Ewidencji Kierowców informacji nie tylko o kierowcach, ale także m.in. o lekarzach uprawnionych do przeprowadzania badań lekarskich i psychologach uprawnionych do wykonywania badań psychologicznych w zakresie psychologii transportu, przez co powodowały niezgodność tego zakresu z samym brzmieniem nazwy przedmiotowej bazy.²²⁷ Prace nad ostatecznym kształtem ustawy o osobach kierujących pojazdami nie zostały zakończone w omawianym okresie sprawozdawczym.

Generalny Inspektor opiniował zmiany zaproponowane do **rozporządzenia Rady Ministrów w sprawie ustalenia okoliczności i przyczyn wypadków przy pracy oraz sposobu ich dokumentowania, a także zakresu informacji zamieszczanych w rejestrze wypadków przy pracy** (Dz. U. Nr 115, poz. 744 ze zm.).²²⁸ Zgłosił zastrzeżenia do zawartego w § 16 ust. 2 projektu sformułowania wskazującego, że w rejestrze wypadków przy pracy, prowadzonym przez pracodawcę, umieszcza się „inne informacje, których zamieszczenie w rejestrze jest celowe.” Jeśli bowiem uznać, że przez określenie *inne informacje* można rozumieć dane osobowe w myśl art. 6 ustawy o ochronie danych osobowych, to katalog tych informacji powinien być wyraźnie określony (sprecyzowany) w projektowanym przepisie. Wątpliwości wzbudziło także niejasne sformułowanie „ciężkość wypadku” (§ 6 ust. 1 pkt 5 projektu rozporządzenia), gdyż pojęcie to nie występuje ani w Kodeksie pracy, ani w ustawie z dnia 6 marca 1981 r. o Państwowej Inspekcji Pracy (tekst jednolity: Dz. U. z 2001 r. Nr 124, poz. 1362 ze zm.), a we wzorze protokołu ustalenia okoliczności i przyczyn wypadku przy pracy stanowiącego załącznik do rozporządzenia Ministra Gospodarki i Pracy z dnia 16 września 2004 r. w sprawie wzoru protokołu ustalenia okoliczności i przyczyn wypadku przy pracy (Dz. U. Nr

²²⁵ Zgodnie z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych o stanie zdrowia bez zgody osoby, której dotyczą, jest dopuszczalne w oparciu o przepis szczególny innej ustawy, stwarzający przy tym pełne gwarancje ich ochrony.

²²⁶ Dla realizacji zadań starosty jako organu administracji publicznej wystarczające jest uzyskiwanie kopii orzeczeń lekarskich o istnieniu lub braku przeciwwskazań zdrowotnych do kierowania pojazdami nie zaś dokumentacji medycznej, w oparciu o którą orzeczenia te zapadły.

²²⁷ Generalny Inspektor wskazał zatem na konieczność nowelizacji art. 100a ust. 1 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (tekst jednolity: Dz. U. z 2005 r. Nr 108, poz. 908 ze zm.) i zmiany nazwy bazy danych na odpowiadającą zakresowi danych, jakie będą w niej zbierane.

²²⁸ Pismo z dnia 14 czerwca 2006 r. o sygn. DPR-IV-026-5-EK/06. Odpowiedź GIODO z dnia 23 czerwca 2006 r. o sygn. GI-DP-023/125/06.

227, poz. 2298) jest mowa o okolicznościach wypadku, przyczynach wypadku, skutkach wypadku, rodzaju wypadku (indywidualny, zbiorowy, śmiertelny, powodujący czasową niezdolność do pracy). Uwagi Generalnego Inspektora zostały uwzględnione.²²⁹

Opiniując **projekt rozporządzenia Ministra Pracy i Polityki Społecznej w sprawie określenia standardu podstawowych usług świadczonych przez specjalistyczne ośrodki wsparcia dla ofiar przemocy w rodzinie, a także szczegółowych kierunków prowadzenia oddziaływań korekcyjno – edukacyjnych**²³⁰ Generalny Inspektor zgłosił zastrzeżenia do § 1 ust. 1 pkt 1 lit c, zgodnie z którym standard podstawowych usług świadczonych przez specjalistyczny ośrodek wsparcia dla ofiar przemocy w rodzinie obejmuje w zakresie interwencyjnym diagnozę sytuacji rodzinnej ofiary przemocy w rodzinie. Wątpliwości wzbudziło bowiem ogólne pojęcie „diagnoza sytuacji rodzinnej”, z którego można domniemywać, iż będą w tym przypadku przetwarzane pewne, bliżej nie określone, informacje dotyczące sytuacji rodzinnej ofiary przemocy w rodzinie, w tym stanowiące dane osobowe w rozumieniu art. 6 ustawy. W konsekwencji przedmiotowy zapis może być interpretowany zbyt szeroko, a tym samym brak wskazania jednolitego zakresu informacji dotyczących sytuacji rodzinnej może być rozpatrywany w kontekście naruszenia zasady adekwatności, określonej w art. 26 ust. 1 pkt 3 ustawy. W związku z tym Generalny Inspektor zaproponował, aby sformułowano treść przedmiotowego przepisu w taki sposób, który nie będzie budził wątpliwości co do zakresu informacji mieszczących się w pojęciu „diagnoza sytuacji rodzinnej”.²³¹

Na szczególną uwagę zasługują także dwa projekty aktów prawnych przedłożone do zaopiniowania Generalnemu Inspektorowi Ochrony Danych Osobowych.

Pierwszy z nich to **projekt ustawy o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego** wraz z projektami aktów wykonawczych do tej ustawy.²³² W odniesieniu do jednego z projektów aktów wykonawczych, tj. **projektu rozporządzenia Ministra Sprawiedliwości w sprawie sposobu, zakresu i trybu wykonywania kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego**, organ ochrony

²²⁹ Rozporządzenie weszło w życie w dniu 12 grudnia 2006 r. (Dz. U. Nr 215, poz. 1582). Rejestr wypadków przy pracy zawiera: imię i nazwisko poszkodowanego, miejsce i datę wypadku, informacje dotyczące skutków wypadku dla poszkodowanego, datę sporządzenia protokołu powypadkowego, stwierdzenie, czy wypadek jest wypadkiem przy pracy, datę przekazania do Zakładu Ubezpieczeń Społecznych wniosku o świadczenia z tytułu wypadku przy pracy, liczbę dni niezdolności do pracy oraz inne informacje, nie będące danymi osobowymi, których zamieszczenie w rejestrze jest celowe, w tym wnioski i zalecenia profilaktyczne zespołu powypadkowego (§ 16 ust. 2). Sformułowanie „ciężkość wypadku” zastąpiono zwrotem „rodzaj i skutki wypadku”.

²³⁰ Pismo z dnia 10 lutego 2006 r. o sygn. DPS-II-073-888-2-MB/06. Odpowiedź GIODO z dnia 27 lutego 2006 r. o sygn. GI-DP-023/30/06.

²³¹ Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 6 lipca 2006 r. w sprawie określenia standardu podstawowych usług świadczonych przez specjalistyczne ośrodki wsparcia dla ofiar przemocy w rodzinie, a także szczegółowych kierunków prowadzenia oddziaływań korekcyjno – edukacyjnych (Dz. U. Nr 127, poz. 890) weszło w życie w dniu 1 sierpnia 2006 r. – sformułowanie „diagnoza sytuacji rodzinnej” zastąpiono określeniem „rozpoznanie sytuacji ofiary przemocy w rodzinie i opracowanie planu pomocy”.

²³² Przekazane pismem z dnia 20 kwietnia 2006 r. o sygn. P. I. 4020/15/05. Odpowiedź GIODO z dnia 12 maja 2006 r. o sygn. GI-DP-023/97/06.

danych osobowych wskazał, że doprecyzowania wymaga przepis nakładający na skazanego zgłaszającego się do systemu dozoru elektronicznego obowiązek podania „danych osobowych i informacji o zmianie tych danych” (§ 4 ust. 2 projektu). Zgodnie bowiem z art. 6 ust. 1 ustawy o ochronie danych osobowych pojęcie „dane osobowe” obejmuje swoim zakresem wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. A zatem celowym byłoby w tym przypadku zastąpienie ogólnego sformułowania „dane osobowe” enumeratywnym wyliczeniem katalogu danych, do których podania zobowiązany byłby skazany w momencie zgłoszenia do systemu dozoru elektronicznego. Z kolei § 7 ust. 2 **projektu rozporządzenia Ministra Sprawiedliwości w sprawie określenia rodzaju elektronicznych urządzeń rejestrujących i środków technicznych oraz trybu wyboru i warunków, jakie musi spełniać upoważniony podmiot dozoru przy wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego** odwoływał się w swojej treści do nieobowiązującego już (od dnia 1 maja 2004 r.) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521 ze zm.). Prace legislacyjne nad wskazanymi projektami aktów prawnych nie zostały zakończone w omawianym okresie sprawozdawczym.

Drugi zaś, to **projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw**.²³³ Generalny Inspektor zakwestionował rozbieżność pomiędzy treścią projektowanych przepisów (wprowadzanego przez art. 5 pkt 6 ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw) Oddziału 6 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. Nr 90, poz. 557 ze zm.), a odpowiadającym im regulacjom zawartym w projektowanym **rozporządzeniu Ministra Sprawiedliwości w sprawie szczegółowych zasad prowadzenia strony internetowej w celu wykonywania środka karnego – opublikowania wizerunku sprawcy, sposobu i trybu umieszczania oraz usuwania z tej strony podlegających opublikowaniu informacji oraz podmiotów do tego uprawnionych**. Zgodnie bowiem z art. 199a § 1 Kodeksu karnego wykonawczego, wykonanie środka karnego jakim jest opublikowanie wizerunku sprawcy, polega (co do zasady) na umieszczeniu na stronie internetowej prowadzonej przez Ministerstwo Sprawiedliwości (lub działający na jego zlecenie podmiot) fotografii przedstawiającej twarz skazanego łącznie z informacjami odnośnie jego imienia, nazwiska, daty i miejsca urodzenia oraz określeniem typu czynu, za który został skazany. W myśl zaś § 3 ust. 1 powołanego projektu rozporządzenia, opublikowaniu na stronie internetowej administrowanej przez Departament Centrum Ogólnopolskich Rejestrów Sądowych i Informatyzacji Resortu ma podlegać tzw. „karta wizerunku sprawcy”, na którą

²³³ Pismo z dnia 24 listopada 2006 r. o sygn. DL-P-I-4000-61/06. Odpowiedź GIODO z dnia 8 grudnia 2006 r. o sygn. GI-DOLiS-023/7/06.

składają się: fotografia przedstawiająca twarz skazanego, jego imię (imiona), nazwisko, data i miejsce urodzenia, data wydania i data uprawomocnienia się orzeczenia, a także określenie sądu, który je wydał oraz informacja, za jakie przestępstwo i jaką karę orzeczono wobec sprawcy. Niekonsekwencja powstawała także na tle **projektowanego art. 199a § 3 Kodeksu karnego wykonawczego**, w myśl którego opublikowanie wizerunku sprawcy miało nastąpić na okres 6 miesięcy licząc od dnia umieszczenia na stronie internetowej, podczas, gdy § 4 ust. 1 wspomnianego projektu rozporządzenia w kwestii okresu publikacji „karty wizerunku sprawcy” odsyłał wprost do postanowień zawartych w wyroku skazującym. W uzasadnieniu organ ochrony danych osobowych stwierdził, iż skoro wykonywanie środka karnego – opublikowanie wizerunku sprawcy – w sposób immanentny wiąże się z przetwarzaniem danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, a zgodnie z dyspozycją zawartą w ust. 2 pkt 2 powołanego przepisu, przetwarzanie danych tego rodzaju bez zgody osoby, której one dotyczą może nastąpić jedynie w oparciu o przepis rangi ustawowej, nie można zaakceptować sytuacji, w której rozporządzenie wykonawcze przewiduje szerszy zakres przetwarzanych danych, aniżeli ustawa, jak również w sposób odmienny ustala okres dopuszczalnego przetwarzania tych danych.²³⁴ Dodatkowo, biorąc pod uwagę przewidzianą w art. 178b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 ze zm.) zasadę automatyzmu w orzekaniu środka karnego – opublikowania wizerunku sprawcy.²³⁵ Generalny Inspektor zasygnalizował, iż skoro upublicznienie wizerunku skazanego opatrzonego szeregiem informacji o skazaniu stanowi istotną ingerencję w sferę prywatności jednostki, to ocena celowości zastosowania tego środka powinna zostać pozostawiona niezawisłemu sądowi. W omawianym okresie sprawozdawczym nie zakończono prac nad opisywanym projektem.

W 2006 roku kontynuowane były prace legislacyjne nad zmianami ustawy – **Prawo telekomunikacyjne**. Poselski projekt zmian do tej ustawy²³⁶ nakładał na operatorów publicznych sieci telekomunikacyjnych lub dostawców publicznie dostępnych usług telekomunikacyjnych, obowiązek przechowywania przez okres 5 lat danych transmisyjnych dotyczących abonentów i użytkowników końcowych, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa i porządku publicznego (tzw. „danych retencyjnych”).²³⁷ Kwestionując tak długi okres przechowywania tych danych Generalny Inspektor podtrzymał uwagi wyrażone w piśmie

²³⁴ Analogiczna uwaga, związana z uregulowaniem w rozporządzeniu, zamiast w ustawie, kwestii przetwarzania danych szczególnie chronionych, została zgłoszona do art. 42a Kodeksu karnego wykonawczego (wprowadzanego przez art. 5 pkt 1 ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw) i wydano na jego podstawie (art. 42a § 8) – rozporządzenia Ministra Sprawiedliwości w sprawie Funduszu Pomocy Ofiarom Przestępstw.

²³⁵ Zgodnie z proponowanym brzmieniem art. 178b Kodeksu karnego, „Wymierzając sprawcy karę na podstawie art. 178 § 1 lub skazując za przestępstwo z art. 178a § 1 sąd orzeka opublikowanie wizerunku sprawcy”.

²³⁶ Pismo z dnia 20 czerwca 2006 r. o sygn. PS-100/06. Odpowiedź GIODO z dnia 5 lipca 2006 r. o sygn. GI-DP-023/311/05/06.

²³⁷ Projektowany art. 165 ust. 1 Prawa telekomunikacyjnego.

z dnia 6 grudnia 2005 r. o sygn. GI-DP-023/311/05.²³⁸ Dodatkowo wskazał, iż Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE przewiduje przechowywanie „danych retencyjnych” przez okres co najmniej 6 miesięcy i nie dłużej niż 2 lata od daty połączenia,²³⁹ wskazując jednocześnie, iż w szczególnych okolicznościach istnieje możliwość przedłużenia maksymalnego okresu zatrzymywania o ograniczony okres czasu.²⁴⁰ Rząd wyrażając opinię w sprawie rozwiązań zaproponowanych w poselskim projekcie zmian do ustawy – Prawo telekomunikacyjne podzielił uwagi Generalnego Inspektora i zgłosił negatywne stanowisko do tego projektu.²⁴¹ Poselski projekt ustawy został odrzucony na posiedzeniu Sejmu w dniu 8 września 2006 r. Aktualnie trwają dalsze prace nad zmianami do ustawy – Prawo telekomunikacyjne związane z kolejnym projektem dotyczącym przedłużenia okresu przechowywania danych retencyjnych. Również do tego projektu Generalny Inspektor zgłosił zastrzeżenia w kwestii niedopuszczalności przedłużenia okresu przechowywania tych danych ponad wskazany w Dyrektywie 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE.²⁴²

W omawianym roku sprawozdawczym 2006, do zaopiniowania Generalnemu Inspektorowi Ochrony Danych Osobowych przedłożono **3 poselskie projekty ustaw: 1) o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa komunistycznego z lat 1944 – 1990 oraz treści tych dokumentów oraz o zmianie innych ustaw, 2) o zmianie ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, 3) o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw.**²⁴³ Ich przepisy, zwłaszcza te zrównujące status osób będących pracownikami i współpracownikami służb specjalnych ze statusem osób, które były przez te służby prześladowane (osoby pokrzywdzone), wzbudzały wątpliwości

²³⁸ Informacje na ten temat można odnaleźć w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, Część II, lit. K, Telekomunikacja, str. 182-183.

²³⁹ Zgodnie z Artykułem 6 „Państwa członkowskie gwarantują, że wymienione w art. 5 kategorie danych są zatrzymywane na okresy nie krótsze niż 6 miesięcy oraz nie dłuższe niż dwa lata od daty połączenia”.

²⁴⁰ Stosownie do Artykułu 12, „Państwo członkowskie znajdujące się w szczególnych okolicznościach, uzasadniających przedłużenie maksymalnego okresu zatrzymywania, o którym mowa w art. 6, o ograniczony okres czasu, może podjąć niezbędne środki. Państwo członkowskie niezwłocznie powiadamia Komisję oraz informuje pozostałe państwa członkowskie o środkach podjętych na podstawie tego artykułu, oraz wskazuje na przyczyny ich podjęcia.”

²⁴¹ Projekt dokumentu *Stanowisko rządu wobec poselskiego projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne* (Druk nr 681) zawarty w piśmie z dnia 11 sierpnia 2006 r., znak: ML4s-020-191/06.

²⁴² Pismo Ministerstwa Transportu z dnia 12 września 2006 r. o sygn. ML2-k-020-28/06. Odpowiedź GIODO z dnia 16 października 2006 r. o sygn. GI-DP-023/179/06.

²⁴³ Projekty 1) i 2) przekazane pismem z dnia 22 lutego 2006 r. o sygn. PS – 33/06, projekt 3) przekazany pismem z dnia 1 marca 2006 r. o sygn. PS – 34/06. Odpowiedź GIODO z dnia 9 marca 2006 r. o sygn. GI-DP-023/33,34,35/06.

z punktu widzenia zgodności z Konstytucją RP, zwłaszcza z prawem do prywatności i informacyjnego samookreślenia.²⁴⁴ Generalny Inspektor podkreślił, że przewidywane w projektach wprowadzenie powszechnego dostępu do informacji zawartych w dokumentach osób pełniących funkcje publiczne może prowadzić do ponownego naruszenia praw osób pokrzywdzonych, gdyż osoba pełniąca funkcję publiczną może być jednocześnie osobą pokrzywdzoną, a zatem powinna sama decydować, jakie informacje jej dotyczące mogą być udostępnione.²⁴⁵ Zakwestionował także sądową weryfikację dokumentów i informacji polegającą na możliwości skierowania powództwa przeciwko Instytutowi Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu do sądu cywilnego oraz fakt, że treść zaświadczenia²⁴⁶ w kwestionowanym przez obywatela brzmieniu ma być powszechnie dostępna (w Internecie) pomimo wytoczenia przez niego powództwa. Organ ochrony danych osobowych podniósł także argument, że jedna z podstawowych zasad postępowania cywilnego statuująca, że ciężar dowodu spoczywa na powodzie, nie będzie mogła być zrealizowana, ponieważ możliwość uzyskania wszystkich dokumentów (dowodów) posiada Rzecznik Interesu Publicznego i sąd lustracyjny, które to organy, według projektu wskazanego wyżej w pkt 1, miały jednak zostać zlikwidowane. Zwrócono także uwagę na konieczność – jeśli zostanie przyjęta konstrukcja postępowania cywilnego – uregulowania szczegółowego trybu i terminów rozpatrywania przez sądy cywilne spraw z powództwa przeciwko Instytutowi Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu. Ponadto, sprzeczne z zasadami praworządności pozostawały przepisy art. 5 ust. 2 i art. 6 ust. 3 projektu ustawy o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa komunistycznego z lat 1944 – 1990 oraz treści tych dokumentów, oraz o zmianie innych ustaw²⁴⁷ z których wynikało, że po wydaniu zaświadczenia mogą być wydawane kolejne. W istocie oznaczało to, że żadne z wydanych zaświadczeń nie może mieć charakteru

²⁴⁴ Stosownie do art. 31 ust. 3 Konstytucji RP, ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

²⁴⁵ Zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego „ochrona życia prywatnego, gwarantowana konstytucyjnie co do zasady w art. 47, obejmuje sobą także autonomię informacyjną (art. 51 Konstytucji) oznaczającą prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów”.

²⁴⁶ Zgodnie z art. 6 ust. 1 projektu ustawy o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa komunistycznego z lat 1944 – 1990 oraz treści tych dokumentów, oraz o zmianie innych ustaw, urzędowego potwierdzenia co do faktu istnienia w archiwum Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu dokumentów organów bezpieczeństwa państwa z lat 1944 – 1990, dotyczących danej osoby, dokonuje organ zaświadczający w formie zaświadczenia.

²⁴⁷ Osoby ubiegające się o pełnienie funkcji publicznych wskazanych w art. 4, urodzone przed dniem 1 sierpnia 1972 roku, obowiązane są do przedłożenia właściwemu spośród organów wymienionych odpowiednio w ust. 4 lub ust. 6, aktualnego urzędowego potwierdzenia, o którym mowa w ust. 1. Za aktualne uważa się urzędowe potwierdzenie wydane wobec danej osoby jako ostatnie spośród dotychczas wobec niej wydanych (art. 5 ust. 2). W przypadku, gdyby po wydaniu zaświadczenia danej osobie stwierdzono istnienie w archiwum Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu dokumentu organu bezpieczeństwa państwa z lat 1944 – 1990, dotyczącego tej osoby, a nieznanego dotychczas organowi zaświadczającemu, organ ten wszczyna z urzędu postępowanie w sprawie wydania zaświadczenia (art. 6 ust. 3 zd. 1).

ostatecznego, a tym samym obywatel nie może być pewny swojej sytuacji prawnej. W projekcie ustawy o zmianie ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz w projekcie ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw, Generalny Inspektor zakwestionował proponowane wyłączenie zastosowania ustawy o ochronie danych osobowych do działalności Instytutu Pamięci Narodowej.²⁴⁸ W uzasadnieniu wskazał, iż opiniowana ustawa nie zawiera własnych regulacji w zakresie zabezpieczeń zgromadzonych przez IPN zbiorów przed ich nieuprawnionym udostępnianiem, zmienianiem czy usuwaniem, co przy całkowitym wyłączeniu ustawy o ochronie danych osobowych może stanowić naruszenie art. 51 Konstytucji RP oraz obowiązujących Polskę aktów Unii Europejskiej.

W związku z toczącymi się pracami nad **projektem ustawy o Centralnym Biurze Antykorupcyjnym**²⁴⁹ Generalny Inspektor Ochrony Danych Osobowych zgłosił uwagi, które dotyczyły zarówno często powtarzających się – z punktu widzenia ustawy o ochronie danych osobowych – błędów legislacyjnych, jak np. brak w przepisach jednolitego zakresu danych osobowych,²⁵⁰ brak wskazania terminu określającego, w jakim czasie ma nastąpić zniszczenie materiałów zgromadzonych podczas kontroli operacyjnej,²⁵¹ brak spójności terminologii zawartej w przepisach projektu z terminologią ustawy o ochronie danych osobowych,²⁵² jak również zakwestionował przepis wyłączający spod jego kontroli przetwarzanie danych osobowych przez CBA,²⁵³ uznając takie rozwiązanie za naruszające standardy przyjęte w Unii Europejskiej, gdzie organy policyjne, charakter których – według projektu – ma mieć CBA, poddane są kontroli niezależnych organów do spraw ochrony danych osobowych.²⁵⁴

²⁴⁸ Z 3 projektów powstał jeden projekt ustawy o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944 – 1990 oraz treści tych dokumentów. Ustawa ta (z dnia 18 października 2006 r.) została uchwalona przez Sejm i opublikowana w Dzienniku Ustaw z dnia 30 listopada 2006 r. Nr 218, poz. 1592.

²⁴⁹ Projekt przekazany pismem z dnia 16 grudnia 2005 r. o sygn. SMK-10-6(2)/05/w/MB. Odpowiedź GIODO z dnia 9 stycznia 2006 r. o sygn. GI-DP-023/320/06.

²⁵⁰ Art. 15 ust. 26 pkt 3 i 8 projektu ustawy, zgodnie z którym notatka, w której funkcjonariusz dokumentuje fakt zastosowania środka przymusu bezpośredniego powinna zawierać w szczególności dane osoby, wobec której zastosowano środek przymusu bezpośredniego oraz dane dotyczące ewentualnych świadków zdarzenia.

²⁵¹ Art. 17 ust. 3 zd. 2 projektu, zgodnie z którym w razie nieudzielenia przez sąd zgody Szef CBA wstrzymuje kontrolę operacyjną oraz poleca protokolarnie, komisyjne zniszczenie materiałów zgromadzonych podczas jej stosowania.

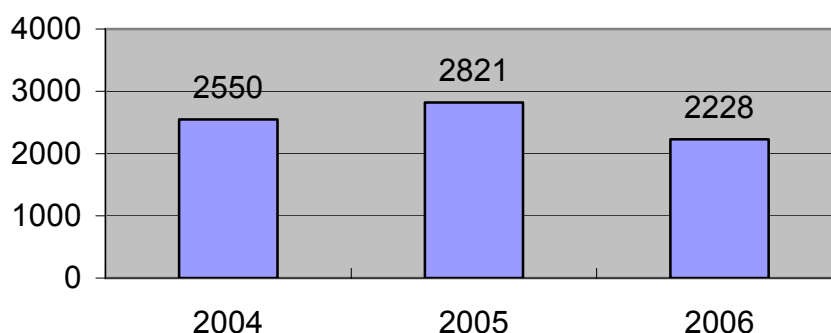
²⁵² Art. 22 ust. 1 projektu ustawy, zgodnie z którym w zakresie swojej właściwości CBA może uzyskiwać informacje, w tym także niejawne, gromadzić je, sprawdzać i przetwarzać. Stosownie natomiast do art. 7 pkt 2 ustawy o ochronie danych osobowych, gromadzenie i sprawdzanie danych osobowych stanowi ich przetwarzanie. Uwaga nieuwzględniona.

²⁵³ Art. 163 projektu ustawy o Centralnym Biurze Antykorupcyjnym zawartego w Druku sejmowym nr 275. Pismo GIODO z dnia 22 marca 2006 r. o sygn. GI-DP-023/64/06.

²⁵⁴ Uwaga nieuwzględniona – zgodnie z art. 178 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708), która weszła w życie w dniu 24 lipca 2006 r., „W ustawie (...) o ochronie danych osobowych (...) w art. 43 ust. 2 otrzymuje brzmienie: W odniesieniu do zbiorów, o których mowa w ust. 1 pkt 1 i 3, oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Centralne Biuro Antykorupcyjne oraz Wojskowe Służby Informacyjne, Generalnemu Inspektorowi nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1, 3-5 oraz w art. 15-18.”

6. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

Udzielanie odpowiedzi na pytania z zakresu ochrony danych osobowych stanowi istotny element działalności edukacyjnej Generalnego Inspektora. W roku sprawozdawczym 2006, do GIODO wpłynęło 2228 pytań z prośbą o interpretację przepisów ustawy o ochronie danych osobowych i aktów wykonawczych do niej oraz przepisów dotyczących ochrony danych osobowych zawartych w innych aktach prawnych. Porównanie liczby pytań skierowanych do Generalnego Inspektora w latach 2004 – 2006 przedstawia poniższy wykres.



Wykres 27: Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do Generalnego Inspektora w latach 2004–2006.

Podobnie jak w roku 2005, większość pytań kierowana była do Generalnego Inspektora drogą elektroniczną. Przeważająca liczba pytań dotyczyła stosowania przepisów innych, niż ustawa o ochronie danych osobowych. Co ciekawe, pytania takie zadają często podmioty, których zadania są szczegółowo uregulowane w dotyczących ich aktach prawnych; w tym również w zakresie przetwarzania danych osobowych. Z taką sytuacją mamy do czynienia m.in. w przypadku zakładów opieki zdrowotnej,²⁵⁵ czy organów właściwych w zakresie geodezji i kartografii.²⁵⁶ Podmioty te zwracają się zatem do Generalnego Inspektora z prośbą o interpretację swoich własnych przepisów.

6.1. Interpretacja przepisów

Podobnie jak w latach ubiegłych najliczniejszą grupę stanowiły pytania z zakresu przetwarzania danych przez **organy administracji publicznej**. Pytania zgłaszali zarówno obywatele – petenci

²⁵⁵ Przetwarzanie danych zawartych w dokumentacji medycznej znajdującej się w dyspozycji zakładów opieki zdrowotnej reguluje rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz. U. Nr 247, poz. 1819).

²⁵⁶ Przetwarzanie danych zawartych w ewidencji gruntów i budynków reguluje ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (tekst jednolity: Dz. U. z 2005 r. Nr 240, poz. 2027 ze zm.) i wydane na jej podstawie rozporządzenie Ministra Rozwoju Regionalnego i Budownictwa z dnia 29 marca 2001 r. w sprawie ewidencji gruntów i budynków (Dz. U. Nr 38, poz. 454).

rozmaitych urzędów, jak i administratorzy danych – jednostki samorządu terytorialnego, organy administracji państwowej, ośrodki pomocy społecznej, urzędy stanu cywilnego, organy podatkowe, organy celne. Spośród tematów poruszanych w pytaniach nadesłanych w 2006 r. dotyczących przetwarzania danych przez organy administracji publicznej na uwagę zasługuje zagadnienie przekazywania danych między tymi organami. Zasadniczo przesłanką legalizującą tego typu działania mogą być tylko przepisy prawa regulujące zasady funkcjonowania określonego rodzaju podmiotów (art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych). Dla przykładu, organy podatkowe mogą udostępniać dane objęte tajemnicą podatkową tylko podmiotom wskazanym w Ordynacji podatkowej. Z uwagi na fakt, iż w takich sytuacjach kwestie udostępniania danych regulują właściwe przepisy szczególne, odwoływanie się do ogólnych przepisów ustawy o ochronie danych osobowych nie jest uzasadnione. Za niezgodne z prawem uznać należy przekazywanie danych między organami administracji publicznej z ominięciem przepisów prawa, np. na mocy zawartych między tymi organami porozumień. Przykładem takiego działania jest Integrująca Platforma Elektroniczna, która zakłada przekazywanie danych z zakresu geodezji i kartografii przetwarzanych na szczeblu lokalnym organom centralnym, podczas gdy w obecnym stanie prawnym brak jest podstaw do takiego działania.

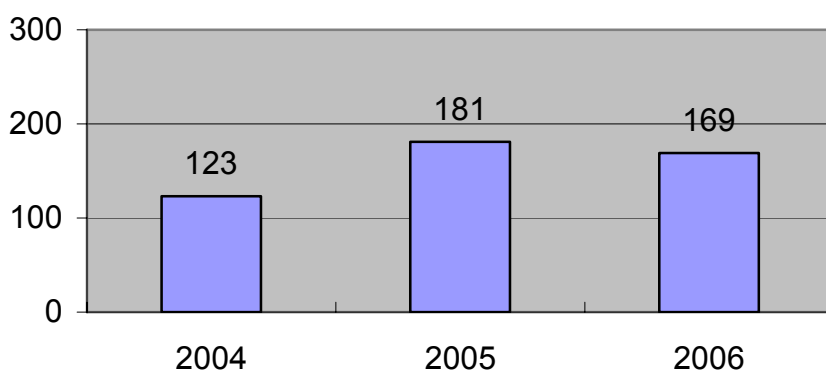
W 2006 roku zmniejszyło się zainteresowanie problematyką przetwarzania danych przez **spółdzielnie mieszkaniowe, wspólnoty mieszkaniowe, zarządców nieruchomości, товариства будownицтва сполечного**. Mniejsza liczba pytań dotyczących tej problematyki świadczy, iż zagadnienia budzące wątpliwości, które powodowały masowy napływ pytań w latach ubiegłych, np. jawność zadłużenia członków wspólnot mieszkaniowych/spółdzielni, jawność wynagrodzenia władz spółdzielni i jej pracowników, zostały dostatecznie wyjaśnione. W takich sprawach GODO informował, iż jakkolwiek Prawo spółdzielcze umożliwia członkom spółdzielni sprawowanie kontroli nad działalnością jej organów, w tym zapewnia dostęp do tworzonych przez nie dokumentów, np. sprawozdań finansowych (art. 18 § 2 pkt 3), to udostępnienie członkom spółdzielni informacji o wynagrodzeniu pracowników nie znajduje oparcia w przepisach prawa.

Analizując tematykę pytań wskazać należy, iż stale zwiększająca się liczba wspólnot mieszkaniowych i często praktykowane powierzanie zarządu nieruchomością wspólną zarządcy skutkuje problemami, np. związanymi z ograniczaniem przez zarządcę dostępu do prowadzonej przez niego dokumentacji zarządowi wspólnoty czy jej członkom.²⁵⁷ Wielu zarządców nie jest również świadomych, że przetwarzają dane osobowe członków wspólnoty jedynie jako podmioty, którym

²⁵⁷ Np. GI-DP-024/1814/06. Generalny Inspektor podkreślał, zarządca nieruchomości wspólnej zobowiązany jest działać tylko w granicach i na podstawie przepisów prawa oraz postanowień umowy o zarządzanie nieruchomością. Zarządca wykonuje swoje obowiązki w interesie i na rzecz wspólnoty mieszkaniowej i jego działania nie mogą mieć na celu utrudniania zarządowi wspólnoty wykonywania jego ustawowych praw i obowiązków. Jego obowiązek udostępnienia członkom wspólnoty danych osobowych innych członków wspólnoty nie może być zatem kwestionowany.

przetwarzanie danych powierzono.²⁵⁸ Zatem nie mogą oni samodzielnie decydować o celach i środkach przetwarzania tych danych.

W omawianym 2006 roku, utrzymała się bardzo wysoka liczba pytań z zakresu przetwarzania danych w **Internecie**.



Wykres 28: Liczbowe zestawienie pytań o interpretację przepisów dotyczących przetwarzania danych osobowych w Internecie skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004–2006.

Problemy, który pojawiały się w tym obszarze były podobne do problemów z lat ubiegłych i dotyczyły m.in.:

- przetwarzania danych w serwisach aukcyjnych,²⁵⁹
- niewłaściwego odbierania zgody na przetwarzanie danych,
- przesyłania ofert marketingowych poprzez Internet, tzw. spamming²⁶⁰,
- prowadzenia na stronach internetowych różnego rodzaju rejestrów i wykazów na podstawie przepisów prawa.

Podmioty prowadzące strony internetowe często uzależniają możliwość wypełnienia, np. formularza rejestracyjnego, od wyrażenia zgody na przetwarzanie danych osobowych w różnych celach, w tym marketingowych. W tych sytuacjach Generalny Inspektor sygnalizował, iż powyższa praktyka narusza przepisy o ochronie danych osobowych. Po interwencji GODO administratorzy stron

²⁵⁸ Na mocy art. 31 ustawy o ochronie danych osobowych, administrator danych może powierzyć przetwarzanie danych innemu podmiotowi. Zgodnie z ust. 2 wyżej powołanego artykułu, podmiot, któremu dane powierzono może je przetwarzać wyłącznie w celu i zakresie przewidzianym w umowie. Podmiot taki obowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ten ponosi odpowiedzialność jak administrator danych (art. 31 ust. 3 ustawy o ochronie danych osobowych).

²⁵⁹ Np. GI-DP-024/117/06, GI-DP-024/317/06, GI-DP-024/1165/06.

²⁶⁰ Np. GI-DP-024/293/06, GI-DP-024/320/06.

usuwali nieprawidłowości w tym zakresie. W sprawach związanych z przesyłaniem przez Internet niechcianych ofert marketingowych, Generalny Inspektor odsyłał do ustawy o świadczeniu usług drogą elektroniczną oraz ustawy z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny, których przepisy zakazują przesyłania nie zamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Działanie takie stanowi również czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.

Często pojawiającym się problemem pozostaje bezprawne ujawnienie danych osobowych na forach internetowych.²⁶¹ Generalny Inspektor wskazywał w takich przypadkach na art. 14 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204 ze zm.) regulujący tryb usuwania danych osobowych opublikowanych przez użytkownika Internetu w systemie teleinformatycznym podmiotu świadczącego usługi drogą elektroniczną. Zgodnie z treścią tego przepisu, zgłoszenie usługodawcy prowadzącemu portal internetowy wiarygodnej informacji o bezprawnym charakterze wpisu, powinno skutkować natychmiastowym jego usunięciem.

Podobnie jak miało to miejsce w latach ubiegłych bardzo wielu pytających interesowała problematyka przetwarzania danych w związku z **zatrudnieniem**. Co istotne, pytania wnosili prawie wyłącznie pracownicy. Tematyka poruszanych pytań była bardzo podobna do tej z lat ubiegłych. Pytania dotyczyły m.in. zakresu danych gromadzonych w związku z funkcjonowaniem zakładowego funduszu świadczeń socjalnych, zakresu danych pracownika i kandydata do pracy gromadzonych przez pracodawcę oraz przetwarzania danych przez związki zawodowe.

Z nadsyłanych pytań wynika, iż coraz częściej pracodawcy wykorzystują nowoczesne technologie w celu kontroli i nadzoru pracownika, np. poprzez wykorzystywanie kamer video w miejscu pracy,²⁶² prowadzenie ewidencji czasu pracy przy wykorzystaniu danych biometrycznych pracownika, np. odcisku palca.²⁶³ Niektórzy pracodawcy stosują programy komputerowe pozwalające im przeglądać treść poczty elektronicznej pracownika, czy treść rozmów prowadzonych przez niego przez komunikator internetowy. Temat ten nie był jeszcze przedmiotem analizy doktryny, jak również nie został poruszony w orzecznictwie sądowym.

Wśród pytań zwraca uwagę duże zainteresowanie problematyką powierzenia i dalszego powierzenia danych osobowych. Z uwagi na fakt, iż coraz częściej spółki prawa handlowego zlecają wykonanie różnych usług podmiotom trzecim (rekrutacja pracowników, rozliczanie wynagrodzeń, prowadzenie dokumentacji finansowo - księgowej, serwis informatyczny, marketing), zachodzi

²⁶¹ Np. GI-DP-024/1478/06, GI-DOLiS-024/6/06.

²⁶² GI-DP-024/1863/06.

potrzeba powierzania tym podmiotom przetwarzania danych. Stąd też liczne pytania o formę umowy powierzenia, jej treść, zakres odpowiedzialności podmiotu, któremu przetwarzanie danych powierzono i o możliwość dalszego powierzenia przetwarzania danych.²⁶⁴

W 2006 r. Generalny Inspektor otrzymał ponadto wiele pytań o dopuszczalność gromadzenia przez podmioty świadczące usługi w zakresie dostarczania przesyłek, numeru PESEL osób odbierających przesyłkę.²⁶⁵ Z uwagi na liczne pisma sygnalizujące występowanie tej praktyki, legalność przetwarzania danych przez podmioty świadczące niniejsze usługi stała się przedmiotem postępowania administracyjnego i czynności kontrolnych. Po przeprowadzeniu kontroli Generalny Inspektor nakazał zaprzestanie pozyskiwania oraz innych operacji z numerem PESEL.²⁶⁶

6.2. Działalność informacyjna

W celu zapewnienia powszechnego dostępu do informacji, Generalny Inspektor w 2006 r. tradycyjnie już, korzystając z pośrednictwa mediów (prasa, radio, telewizja, agencje informacyjne) i wykorzystując wszelkie inne formy kontaktu, organizował konferencje prasowe, udzielał wywiadów i odpowiadał na pytania dziennikarzy, którzy indywidualnie występowali o opinię. Nową, niestosowaną dotychczas formą były dyżury telefoniczne Generalnego Inspektora w redakcjach gazet. Z uwagi na zwiększającą się popularność Internetu Generalny Inspektor prowadził i poszerzał informacje zawarte na głównej stronie internetowej oraz w Biuletynie Informacji Publicznej. Duży krąg odbiorców informacji zapewniły również publikacje książkowe, szkolenia oraz konferencje o charakterze naukowym organizowane przez GODO. W 2006 r. informacje do pojedynczych odbiorców Generalny Inspektor kierował zarówno w formie pisemnej, jak też odpowiadając na telefoniczne pytania oraz poprzez organizowane indywidualne spotkania pracowników GODO z osobami zainteresowanymi tematyką ochrony danych osobowych. Jednocześnie Generalny Inspektor zapewnił powszechny odbiór tych informacji, poprzez publikację swoich opinii w prasie i na stronie internetowej (www.godo.gov.pl).

a) Współpraca z mediami

Wobec ogromnego zainteresowania tematyką ochrony danych osobowych, w 2006 r. Generalny Inspektor Ochrony Danych Osobowych, podobnie jak w latach ubiegłych, odpowiadał na liczne pytania zadawane przez przedstawicieli prasy o zasięgu ogólnopolskim i lokalnym.

Spektrum zadawanych pytań było bardzo szerokie, ale można ocenić, że w 2006 r. dziennikarze dopytywali najczęściej o zasady działania systemu e-godo; wyniki misji oceniającej

²⁶³ Problematyka ta omówiona została w *Sprawozdaniu Generalnego Inspektora Ochrony Danych Osobowych z działalności w roku 2005*, Część II, lit. H, Oświata.

²⁶⁴ Np. GI-DP-024/1171/06, GI-DP-024/1536/06.

²⁶⁵ Np. GI-DP-024/1018/06, GI-DP-024/1127/06.

²⁶⁶ Decyzja z dnia 12 stycznia 2007 r. o sygn. GI-DEC-DIS-7/07.

w związku z planowanym przystąpieniem Polski do strefy Schengen; kwestie zabezpieczenia danych w kontekście konieczności wydawania upoważnień osobom, które w imieniu pracodawców przetwarzają dane osobowe klientów bądź pracowników; wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie, który zapadł dnia 30 maja 2006 r. w związku z zawiadomieniem przez Generalnego Inspektora organów ścigania w sprawie niezgodnego z prawem przetwarzania danych przez IPN; umorzenia zaległości podatkowych; bezpieczeństwa danych w sytuacjach wyrzucania na śmietnik nie zanonimizowanych dokumentów zawierających dane osobowe i przekazywanie danych osobowych pasażerów linii lotniczych zawartych w systemach rezerwacyjnych (passenger name record data) do Stanów Zjednoczonych. Również komentarze Generalnego Inspektora do ustawy o ochronie danych osobowych oraz jego opinie w indywidualnych sprawach ukazywały się w prasie lub emitowane były przez stacje radiowe i telewizyjne.

b) Konferencje prasowe

Okazją do spotkania z dziennikarzami w dniu 11 maja 2006 r. na konferencji prasowej była zorganizowana przez Generalnego Inspektora konferencja, pt. „Bezpieczeństwo Publiczne a Ochrona Danych Osobowych” (Warszawa, dnia 11-12 maja 2006 r.).

W dniu 7 lipca 2006 r. w Biurze Generalnego odbyło się spotkanie z dziennikarzami połączone z inauguracją „Elektronicznej platformy komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych”, e-giudo.

W dniu 12 lipca 2006 r. odbyła się konferencja prasowa, pt. „Ochrona danych osobowych wczoraj, dziś, jutro”, podsumowująca osiem lat działalności Generalnego Inspektora Ochrony Danych Osobowych.

c) Dyżury telefoniczne Generalnego Inspektora

W 2006 r. Generalny Inspektor Ochrony Danych Osobowych rozpoczął cykl dyżurów telefonicznych w redakcji „Pulsu Biznesu”, w trakcie których osoby telefonujące do redakcji mogły uzyskać od Generalnego Inspektora informacje w sprawach związanych z ochroną danych osobowych.

d) Publikacje GODO

W 2006 r. Generalny Inspektor Ochrony Danych Osobowych opracował i wydał następujące publikacje książkowe:

- „26. Międzynarodowa Konferencja Ochrony Prywatności i Danych Osobowych, Prawo do prywatności - prawo do godności”, która stanowi polskojęzyczną wersję publikacji z 2005 roku, pt. „26th International Conference on Privacy and Personal Data Protection”,
- „Ochrona danych osobowych – wczoraj, dziś, jutro”- książka stanowi podsumowanie ośmioletniej działalności pierwszego w Polsce organu do spraw ochrony danych osobowych,

- „ABC ochrony danych osobowych”- książka wydana w ramach przygotowań do obchodzonego po raz pierwszy w dniu 28 stycznia 2007 r., Dnia Ochrony Danych Osobowych.

e) Szkolenia, staże

W trakcie szkoleń i staży pracownicy innych organów zapoznawali się z regulacjami dotyczącymi ochrony danych osobowych oraz uzyskiwali informacje na temat przetwarzania danych osobowych w sektorach związanych z ich pracą. Szkolenia kierowane były zarówno do instytucji publicznych, jak i prywatnych. W trakcie szkoleń omawiane były zasady ochrony danych osobowych oraz przepisy prawa odnoszące się do ochrony danych osobowych ze szczególnym uwzględnieniem specyfiki instytucji, dla której szkolenie było przeprowadzane. Przy okazji tych spotkań ich uczestnicy mieli okazję zadawać pytania oraz uzyskać porady dotyczące rozwiązania konkretnych problemów, jakie pojawiały się w związku z ochroną danych w ich instytucjach.

f) Konferencje organizowane przez Generalnego Inspektora oraz przez inne podmioty, w których uczestniczył GIODO

Generalny Inspektor zapraszany był do udziału w seminariach i spotkaniach organizowanych przez inne podmioty zarówno z sektora publicznego, jak i prywatnego, w trakcie których mógł podzielić się wiedzą i praktycznym doświadczeniem w stosowaniu przepisów o ochronie danych osobowych. Generalny Inspektor czynnie uczestniczył w takich spotkaniach; wygłaszał referaty, brał również udział w dyskusjach mających na celu udoskonalenie norm służących ochronie danych osobowych oraz praktyki ich stosowania.

Również na spotkaniach organizowanych przez Generalnego Inspektora zapraszani byli goście z kraju, jak i z zagranicy – przedstawiciele organów do spraw ochrony danych osobowych, autorytety naukowe, dziennikarze. Jako przykład tego typu spotkania można wymienić konferencję, pt. „Bezpieczeństwo Publiczne a Ochrona Danych Osobowych", która odbyła się w dniach 11-12 maja 2006 r. w Warszawie.

g) Informacja telefoniczna

Kolejnym istotnym instrumentem polityki informacyjnej była możliwość zwracania się do GIODO z pytaniami dotyczącymi ustawy o ochronie danych osobowych, jej stosowania wprost bądź w powiązaniu z innymi przepisami prawa, które odpowiednio do zakresu regulują przetwarzanie danych. W ramach tej części polityki informacyjnej wyróżnić można:

1. odpowiedzi udzielane na indywidualne, pisemne pytania dotyczące interpretacji przepisów prawa,
2. informacje ustne przekazywane drogą telefoniczną przez prawników zatrudnionych u Generalnego Inspektora,
3. możliwość osobistego kontaktu z pracownikami Biura, w siedzibie Biura GIODO.

W połowie 2006 r. specjalna linia telefoniczna obsługiwana przez Zespół Prasowy została przeniesiona do Departamentu Orzecznictwa, Legislacji i Skarg, gdzie jest obsługiwana przez prawników, którzy udzielają informacji o kwestiach związanych ze stosowaniem ustawy o ochronie danych osobowych.

h) Internet

Od momentu założenia w 1999 r. strony internetowej www.giodo.gov.pl obserwuje się stały wzrost odwiedzalności strony. Strona jest codziennie aktualizowana i wzbogacana o nowe artykuły, a także kontrolowana pod kątem zgodności z obowiązującym stanem prawnym.

W 2006 r. dodana została nowa rubryka „Opinie GIODO”, gdzie Generalny Inspektor Ochrony Danych Osobowych komentuje bieżące wydarzenia ściśle związane z ochroną prywatności i danych osobowych.

W celu wykonania obowiązków wynikających z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, ze zm.) w Biurze Generalnego Inspektora Ochrony Danych Osobowych wdrożony został system informatyczny o nazwie „Elektroniczna platforma komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych” (e-giodo). System e-giodo zapewnił dostęp drogą elektroniczną do informacji zawartych w prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych, jawnym rejestrze zbiorów danych osobowych, jak również umożliwił zgłaszanie zbiorów danych osobowych do rejestracji i dokonywanie ich aktualizacji za pośrednictwem Internetu.

7. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych

Jednym z zadań Generalnego Inspektora jest uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych. Zadanie to realizowane jest przede wszystkim poprzez udział Generalnego Inspektora oraz jego przedstawicieli w pracach grup roboczych, konferencjach, seminariach, a także różnych formach współpracy z innymi organami ochrony danych osobowych.

W działalności międzynarodowej Generalnego Inspektora należy również wyróżnić udzielanie przez niego odpowiedzi na napływające z zagranicy pytania dotyczące interpretacji i stosowania polskich przepisów o ochronie danych osobowych.

W omawianym roku sprawozdawczym 2006, wśród różnych form działalności międzynarodowej szczególne znaczenie miała współpraca Generalnego Inspektora z europejskimi rzecznikami ochrony danych osobowych na forum Unii Europejskiej. Współpraca ta odnosiła się zarówno do zagadnień związanych z przetwarzaniem danych osobowych w I jak i III filarze UE.

Różne formy współpracy wielostronnej pomiędzy rzecznikami ochrony danych osobowych umożliwiają efektywną wymianę informacji oraz wypracowywanie rozwiązań dotyczących ochrony danych osobowych. Szczególne znaczenie w tym zakresie miała współpraca na forum Unii Europejskiej. Współpraca ta odnosiła się zarówno do zagadnień związanych z przetwarzaniem danych osobowych w I i III filarze UE. W pierwszej kolejności należy podkreślić rolę współpracy w ramach Grupy Roboczej Art. 29 ds. ochrony danych osobowych, która została ustanowiona na podstawie art. 29 Dyrektywy 95/46/WE.²⁶⁷ W 2006 r. Grupa Robocza Art. 29 przyjęła szereg dokumentów zawierających opinie oraz wytyczne w zakresie przetwarzania danych osobowych w sektorze komunikacji elektronicznej w związku ze świadczeniem usług skanowania wiadomości elektronicznych; świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE; przeglądem ram regulacyjnych dotyczących sieci i usług łączności elektronicznej, ze szczególnym uwzględnieniem dyrektywy o prywatności i łączności elektronicznej), danych dotyczących pasażerów linii lotniczych (PNR), które są przekazywane przez przewoźników lotniczych do władz amerykańskich (opinia w sprawie wyroku Europejskiego Trybunału Sprawiedliwości z dnia 30 maja 2006 r. w połączonych sprawach C-317/04 i C-318/04 dotyczących przekazywania danych dotyczących pasażerów (PNR) do Stanów Zjednoczonych Ameryki i pilnej konieczności przygotowania nowej umowy), a także dotyczących inicjatywy e-Call, przekazywania danych osobowych w systemie SWIFT oraz uznawania i wykonywania decyzji oraz współpracy w zakresie obowiązków alimentacyjnych. W 2006 r. Grupa Robocza przyjęła również dokumenty w sprawie zastosowania unijnych zasad ochrony danych do wewnętrznych systemów informowania o nieprawidłowościach w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych oraz jurysdykcji, obowiązującego prawa, uznawania i wykonywania decyzji oraz współpracy w zakresie obowiązków alimentacyjnych. (lista przyjętych dokumentów znajduje się w załączniku nr 6).

W ramach Grupy Roboczej Art. 29 funkcjonują różnego rodzaju podgrupy powoływane w celu analizy szczegółowych zagadnień dotyczących ochrony danych osobowych oraz w celu przygotowywania dokumentów na posiedzenia plenarne. W 2006 r. Generalny Inspektor uczestniczył m.in. w pracach zespołu roboczego do spraw przetwarzania danych w Internecie, zespołu do spraw danych medycznych oraz zespołu do spraw wykonywania przepisów o ochronie danych osobowych. Należy zaznaczyć, że w ramach prac Grupy Roboczej Art. 29 prowadzone są we wszystkich państwach członkowskich skoordynowane kontrole w określonych sektorach gospodarki.

²⁶⁷ Więcej informacji o Grupie Roboczej Art. 29 znajdują się na stronach internetowych: http://www.giodo.gov.pl/238/id_art/920/ oraz http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

Duże znaczenie w codziennej działalności Generalnego Inspektora odgrywa także współpraca w ramach Warsztatów na temat rozpatrywania spraw.²⁶⁸ Warsztaty odbywają się dwa razy do roku. Generalny Inspektor Ochrony Danych Osobowych uczestniczył w XIII Warsztatach, które miały miejsce w Madrycie w dniach 27-28 marca 2006 r. oraz w XIV Warsztatach, które miały miejsce w Helsinkach w dniach 13-14 listopada 2006 r. Spotkania w ramach Warsztatów pozwalają na poznanie sposobu rozpatrywania spraw przez inne organy ochrony danych osobowych. W czasie spotkań omawiane były zagadnienia przetwarzania danych w związku z wprowadzaniem nowoczesnych technologii w wielu sektorach życia.

W 2006 r. Generalny Inspektor brał udział w pracach Wspólnego Organu Nadzorczego nad Europolem.²⁶⁹ Organ ten zajmuje się nadzorem nad przetwarzaniem danych osobowych w ramach Europejskiego Urzędu Policji i zajmuje się zagadnieniami ogólnymi związanymi z ochroną danych przetwarzanych przez tę instytucję. Sprawy indywidualne z zakresu przetwarzania danych osobowych przez Europol rozpatrywane są przez Komitet Rewizyjny Wspólnego Organu Nadzorczego nad Europolem, w pracy którego Generalny Inspektor uczestniczy od 2004 r.

W omawianym roku sprawozdawczym 2006, Wspólny Organ Nadzorczy opiniował m.in. wniosek dotyczący decyzji Rady w sprawie wglądu do danych Systemu Informacji Wizowej dla organów państw członkowskich odpowiedzialnych za wewnętrzne bezpieczeństwo oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw; projekt decyzji zarządu ustanawiającej przepisy w sprawie ustaleń regulujących wdrożenie pod względem administracyjnym udziału urzędników Europolu do wspólnych zespołów dochodzeniowych; inicjatywę mającą na celu zmianę Aktu Rady z dnia 3 listopada 1998 r. w sprawie przyjęcia zasad mających zastosowanie do akt analitycznych Europolu oraz propozycję decyzji umawiających się stron konwencji o Europolu wprowadzającej artykuł 6A konwencji w sprawie ustanowienia Europejskiego Urzędu Policji.

Ponadto, Generalny Inspektor jako obserwator uczestniczył w pracach Wspólnego Organu Nadzorczego nad Systemem Schengen oraz Wspólnego Organu Nadzorczego nad Cłami.²⁷⁰

W 2006 r. Generalny Inspektor kontynuował współpracę z Europejskim Inspektorem Ochrony Danych w ramach nadzoru nad systemem EURODAC²⁷¹ utworzonym na podstawie rozporządzenia Rady (WE) Nr 2725/2000 z dnia 11 grudnia 2000 r. w sprawie utworzenia "EURODAC" w celu porównywania odcisków linii papilarnych ze względu na efektywne stosowanie Konwencji

²⁶⁸ W ramach Warsztatów na temat rozpatrywania spraw stworzona została platforma internetowa umożliwiająca szybkie przekazywanie pomiędzy uczestnikami bieżących informacji dotyczących rozpatrywanych spraw.

²⁶⁹ Więcej informacji o Wspólnym Organie Nadzorczym nad Europolem znajduje się na stronie internetowej: http://www.giodo.gov.pl/238/id_art/923/.

²⁷⁰ Więcej informacji o Wspólnym Organie Nadzorczym nad Systemem Schengen oraz Wspólnym Organem Nadzorczym nad Cłami znajduje się na stronie internetowej: <http://www.giodo.gov.pl>.

Dublińskiej.²⁷² Nadzór nad tym systemem wykorzystywanym do ustalania właściwości państwa do rozpatrywania wniosków o udzielenie azylu sprawowany jest na szczeblu Unii Europejskiej przez Europejskiego Inspektora Ochrony Danych, a na szczeblu krajowym przez organy ochrony danych osobowych państw członkowskich. Z uwagi na konieczność prowadzenia równoległego nadzoru na obu tych szczeblach Europejski Inspektor Ochrony Danych nawiązał ścisłą współpracę z poszczególnymi krajowymi organami nadzorczymi, w celu podejmowania skoordynowanego nadzoru nad wskazanym powyżej systemem. W ramach tego nadzoru w 2006 r. badano funkcjonowanie systemu EURODAC na poziomie europejskim oraz poziomie krajowym oraz sposób wykorzystywania przez organy krajowe informacji uzyskanych z systemu.²⁷³

W okresie od stycznia do kwietnia 2006 r. Generalny Inspektor przewodniczył Grupie Roboczej do spraw Policji, której działalność w 2006 roku nabrała szczególnej intensywności w związku z licznymi inicjatywami dotyczącymi przetwarzania danych osobowych w trzecim filarze UE. Inicjatywy te dotyczyły, np. przekazywania (wymiany) danych osobowych pomiędzy organami policyjnymi oraz wzajemnego dostępu do policyjnych baz danych w poszczególnych państwach członkowskich Unii Europejskiej (kompatybilność policyjnych systemów). Należy dodać, że dokumenty wypracowane przez Grupę Roboczą do spraw Policji stanowią podstawę oficjalnych dokumentów przyjmowanych przez Konferencję Europejskich Organów Ochrony Danych.

Generalny Inspektor brał udział w pracach dotyczących ochrony danych osobowych na forum Rady Europy, w tym w szczególności w pracach Komitetu Konsultacyjnego ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.²⁷⁴ Jedną z bardzo ważnych inicjatyw podjętych przez Komitet w 2006 r. była propozycja ustanowienia Dnia Ochrony Danych. W efekcie, na wniosek Komitetu w dniu 26 kwietnia 2006 r., na swoim 962 spotkaniu, Komitet Ministrów Rady Europy zdecydował o ustanowieniu Dnia Ochrony danych Rady Europy, który będzie obchodzony 28 stycznia każdego roku.

W 2006 r. Generalny Inspektor brał udział w spotkaniach członków grupy ekspertów (PSG) współpracujących w Europejską Agencją Bezpieczeństwa Informacji i Sieci (ENISA). Jest to Agencja Unii Europejskiej, której celem jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Wspólnoty Europejskiej. Agencja wspiera Komisję Europejską, Państwa Członkowskie oraz kręgi gospodarcze w celu spełnienia wymogów bezpieczeństwa sieci i informacji.²⁷⁵

²⁷¹ EURODAC jest europejską bazą odcisków palców przeznaczoną wyłącznie do identyfikacji osób ubiegających się o azyl w krajach UE lub poza nią, które ukończyły 14 rok życia Więcej informacji zob. http://europa.eu.int/comm/justice_home/

²⁷² Konwencja Dublińska podpisana w dniu 15 czerwca 1990 r. w Dublinie wyznacza państwo odpowiedzialne za rozpatrywanie wniosków o azyl złożonych w jednym z Państw Członkowskich Wspólnot Europejskich. Konwencja Dublińska nie wchodzi w zakres prawa wspólnotowego, lecz jest osobnym aktem prawa międzynarodowego.

²⁷³ Raport w tej sprawie zostanie przygotowany w roku 2007.

²⁷⁴ Więcej o działalności Rady Europy w dziedzinie ochrony danych osobowych na stronie internetowej: www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/.

²⁷⁵ Więcej informacji o Agencji można znaleźć na stronie internetowej: <http://www.enisa.eu.int/>.

W działalności Generalnego Inspektora dużą rolę odgrywa współpraca dwustronna, która polega na bezpośredniej wymianie informacji, pomocy przy prowadzeniu postępowań administracyjnych, czy wizytach roboczych. Uzyskana pomoc niejednokrotnie przyczyniała się do zebrania materiału dowodowego niezbędnego do rozstrzygania rozpatrywanych spraw administracyjnych. Uzyskane zaś przez Generalnego Inspektora informacje o charakterze porównawczym są wykorzystywane w dalszej jego pracy. W maju 2006 r. w Warszawie gościli przedstawiciele rumuńskiego organu ochrony danych osobowych. Wizyta ta stała się okazją do przedstawienia gościom funkcjonowania polskiego organu ochrony danych osobowych oraz wzajemnej wymiany doświadczeń dotyczących wdrażania przepisów o ochronie danych osobowych.

Generalny Inspektor uczestniczył w licznych konferencjach i seminariach o charakterze międzynarodowym. Do najważniejszych z nich należy zaliczyć poniżej opisane wydarzenia.

W dniach 2 i 3 listopada 2006 r. w Londynie, Generalny Inspektor brał udział w 28 Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności. Uczestnikami spotkania byli przedstawiciele organów ochrony danych i prywatności z całego świata. Tematem przewodnim Konferencji było „Społeczeństwo nadzorowane”. W trakcie obrad zastanawiano się przede wszystkim nad skutkami istnienia "społeczeństwa pod nadzorem". Podczas sesji zamkniętej Konferencji, Rzecznicy przyjęli inicjatywę mającą na celu odbudowanie znaczenia ochrony danych osobowych i zapewnienie efektywnego działania organów ochrony danych. Rzecznicy dyskutowali na temat swojej roli i wyzwań, które stoją przed nimi w związku z postępującymi zmianami w dziedzinie nowych technologii. Rzecznicy ocenili, że największe wyzwania stoją przed nimi w obszarze edukacji społecznej, aby uświadomić społeczeństwu wagę ochrony danych osobowych oraz rozpocząć intensywne i długofalowe kampanie na rzecz podniesienia poziomu świadomości społecznej. Wreszcie Rzecznicy powinni usprawnić wymianę informacji pomiędzy sobą oraz ocenić swoją efektywność.

W dniach 24-25 kwietnia 2006 r. Generalny Inspektor brał udział w Wiosennej Konferencji Europejskich Organów Ochrony Danych, która odbyła się w Budapeszcie. W trakcie obrad poruszono m.in. problematykę dotyczącą ochrony danych osobowych w III filarze UE, technologii RFID oraz geolokalizacji, narodowych baz danych medycznych oraz elektronicznej karty medycznej, danych genetycznych, ochrony danych przetwarzanych w celach historycznych i naukowych, a także efektywności organów ochrony danych osobowych. W dniu 25 kwietnia 2006 r. przyjęto deklarację w sprawie zapewnienia odpowiednich ram ochrony danych osobowych w III filarze UE oraz rezolucję o akredytacji na konferencję organów ochrony danych osobowych z Andory, Macedonii, Rumunii i Słowenii. Należy zaznaczyć, że Generalny Inspektor przez rok poprzedzający tegoroczną Konferencję pełnił funkcję sekretariatu Komitetu Akredytacyjnego, którego zadaniem była ocena przedłożonych wniosków o akredytację oraz przygotowanie raportu dla Konferencji.

Należy zauważyć, że Wiosenne Konferencje Europejskich Organów Ochrony Danych (*Spring Conferences of European Data Protection Authorities*) są najważniejszymi, corocznymi spotkaniami rzeczników ochrony danych osobowych z państw członkowskich Unii Europejskiej oraz innych państw europejskich. Konferencje te mają charakter zamknięty, gdyż udział w nich mogą brać jedynie organy ochrony danych osobowych.

Kolejne konferencje poświęcane były różnym aspektom ochrony danych osobowych w Europie, a ich uczestnicy podejmowali działania ukierunkowane nie tylko na wdrażanie unijnych przepisów, ale również na monitorowanie ich przestrzegania w poszczególnych krajach. W szczególności poruszane były kwestie związane ze stosowaniem postanowień Dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Przedmiotem obrad była również ochrona danych osobowych przetwarzanych na potrzeby współpracy policji, jak też współpracy sądów w sprawach karnych i cywilnych, czyli działania podejmowane w ramach trzeciego filaru Unii Europejskiej.

W dniach 24-26 maja 2006 r. w Warnie (Bułgaria) odbyło się 8 Spotkanie Rzeczników Ochrony Danych Osobowych Europy Środkowej i Wschodniej. Obrady były poświęcone przetwarzaniu danych osobowych w związku z wideo-nadzorem i geolokalizacją. Omawiano także kwestie związane z wolnością słowa, marketingiem politycznym oraz wdrażaniem dorobku Schengen.

Należy zaznaczyć, że coroczne Spotkania Rzeczników Ochrony Danych Osobowych z Europy Środkowo-Wschodniej zainicjowane zostały w 2001 roku przez polskiego Generalnego Inspektora Ochrony Danych Osobowych.²⁷⁶ Ich celem jest bieżące omawianie wspólnych problemów związanych z ochroną danych osobowych występujących w krajach Europy Środkowej i Wschodniej oraz wymiana doświadczeń nabytych w ciągu ostatnich lat. Pierwotnym celem tego forum było zharmonizowanie działań pomiędzy organami ochrony danych osobowych, które dopiero od niedawna rozpoczęły wdrażanie ustawodawstwa w tym zakresie. Stanowią one doskonałą platformę wymiany doświadczeń pomiędzy rzecznikami ochrony danych osobowych w tym regionie.

W związku z zachodzącymi w Europie procesami integracyjnymi, jednym z głównych celów Spotkań była wymiana doświadczeń związanych z wdrażaniem w krajowych systemach prawnych ustawodawstwa wspólnotowego z dziedziny ochrony danych osobowych. Po przystąpieniu do Unii Europejskiej większości państw uczestniczących w Spotkaniach cel ten uległ zmianie. Obecnie Spotkania mają służyć pomocą tym państwom, które dopiero rozpoczęły wprowadzanie przepisów o ochronie danych osobowych.

²⁷⁶ Szerzej o współpracy rzeczników ochrony danych z państw Europy Środkowej i Wschodniej w *Sprawozdaniu z działalności Generalnego Inspektora Ochrony Danych Osobowych za rok 2003 i 2004* oraz na stronie internetowej: <http://www.cecprivacy.org>.

O czym już była mowa wcześniej, w dniach 11-12 maja 2006 r. w Warszawie odbyła się zorganizowana przez Generalnego Inspektora Konferencja, pt. "Bezpieczeństwo Publiczne a Ochrona Danych Osobowych", nad którą honorowy patronat objął Marszałek Sejmu RP Marek Jurek.

Zaproszeni goście - reprezentujący krajowe urzędy ochrony danych, Radę Europy, Komisję Europejską, środowiska naukowe, a także podmioty i samorządy gospodarcze - dyskutowali o kształcie ochrony danych osobowych w przypadkach zapobiegania zagrożeniom bezpieczeństwa publicznego.

Uczestnicy konferencji próbowali odpowiedzieć na pytanie: czy, a jeśli tak, to gdzie są granice ingerencji w prywatność osoby, jeśli jest podejmowana w imię ochrony bezpieczeństwa publicznego. Czy przyczyną poszerzenia zakresu informacji o obywatelach gromadzonych przez podmioty publiczne może być zapobieganie aktom terroru, przestępczości?

Uczestnicy Konferencji zastanawiali się też nad gromadzeniem danych osobowych przez podmioty prywatne realizujące obowiązki nałożone na nie przepisami prawa. Czy realizacja obowiązków, takich jak, np. ciążące na bankach w związku z przeciwdziałaniem i zwalczaniem oszustw finansowych lub dotyczących przechowywania i wykorzystywania danych przez dostawców usług telekomunikacyjnych pod hasłem ochrony bezpieczeństwa publicznego, nie jest tylko niepotrzebną ingerencją w prywatność i czy nie spowoduje u obywateli poczucia, że są śledzeni i inwigilowani? Czy pomiędzy prawem do poczucia bezpieczeństwa a prawem do prywatności jest szansa na kompromis? Podczas obrad przedyskutowane zostały m.in. tematy dotyczące relacji pomiędzy ochroną praw człowieka i podstawowych wolności a zapewnieniem bezpieczeństwa publicznego, ograniczenia prywatności w kontekście obowiązków sektora bankowego związanych z przeciwdziałaniem i zwalczaniem oszustw finansowych, ochrony danych osobowych w obszarze wolności, sprawiedliwości i bezpieczeństwa, przetwarzania danych szczególnie chronionych przez organy wymiaru sprawiedliwości, ochrony prywatności w kontekście wprowadzenia Systemu Informacyjnego Schengen drugiej generacji (SIS II), czy też obowiązków dostawców usług telekomunikacyjnych w zakresie przechowywania i dalszego wykorzystywania danych transmisyjnych konsumentów.

W ramach działalności międzynarodowej Generalnego Inspektora należy odnotować jego udział w procesie wdrażania dorobku prawnego Schengen. W dniach 30 – 31 stycznia 2006 r. grupa ekspertów z Unii Europejskiej, zgodnie z mandatem nadanym Decyzją Komitetu ds. Ewaluacji i wdrożenia dorobku prawnego Schengen przy grupie roboczej ds. Ewaluacji Schengen, odwiedziła Polskę celem dokonania okresowej oceny wdrożenia dorobku prawnego Schengen w Polsce.

Zgodnie z postanowieniami art. 114 ust. 1 Konwencji Wykonawczej do Układu z Schengen [dalej: KWS] każda ze stron Konwencji ma obowiązek wyznaczyć organ nadzorczy odpowiedzialny, zgodnie z prawem krajowym, za przeprowadzanie niezależnego nadzoru nad danymi krajowego modułu Systemu Informacyjnego Schengen oraz kontrolę czy przetwarzanie i wykorzystywanie danych

wprowadzonych do tego systemu nie narusza praw osób, których dane dotyczą. W Polsce rolę takiego organu będzie pełnił Generalny Inspektor Ochrony Danych Osobowych.

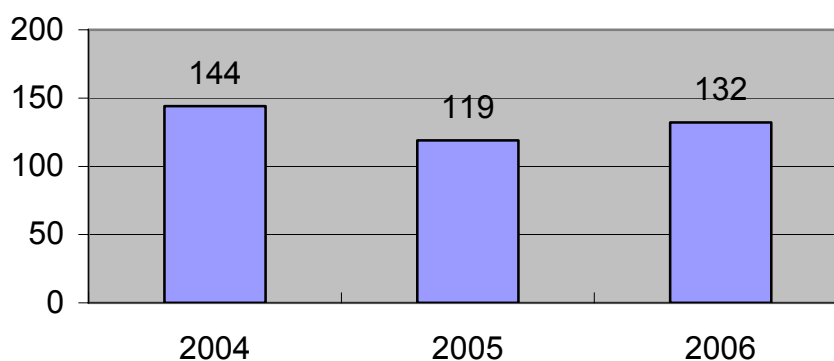
Wyniki misji oceniającej zostały oficjalnie przyjęte w Brukseli, w dniu 10 marca 2006 r. Z przedstawionego raportu wynika, że Polska jest dobrze przygotowana w zakresie ochrony danych osobowych do wejścia pod koniec 2007 r. do układu z Schengen. Pomimo dobrej oceny zespół oceniający wskazał jeszcze kilka problemów do rozwiązania. Między innymi zalecono większy udział GIODO w pracy zespołów roboczych, których zadaniem jest wdrożenie przepisów układu z Schengen oraz zorganizowanie akcji informacyjnej. Zwrócono również uwagę na konieczność przeprowadzenia kontroli w wybranych konsulatach RP znajdujących się w państwach spoza Unii Europejskiej. Eksperci podkreślili także, że Generalny Inspektor powinien mieć zapewnione odpowiednie fundusze umożliwiające mu pełną realizację nowych obowiązków związanych z wdrażaniem dorobku prawnego Schengen.

Część II. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2006 roku

Oceniając wyniki przeprowadzonych **kontroli** stwierdzić należy, że większość jednostek miała problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także z prawidłowym opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych. Wiele zastrzeżeń wzbudzały także stosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń i kategorii danych objętych ochroną, tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Nieprawidłowości w tym zakresie stwierdzono w szczególności w toku kontroli podmiotów udzielających świadczeń zdrowotnych. Liczne uchybienia występowały również w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych. Trudności z prawidłowym wypełnieniem obowiązków określonych w przepisach rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych miały podmioty ze wszystkich sektorów opisanych w Sprawozdaniu z działalności Generalnego Inspektora Ochrony Danych Osobowych za rok 2006 [dalej: Sprawozdanie]. Dużo mniej problemów jednostki kontrolowane miały natomiast z prawidłowym wykonaniem podstawowych obowiązków określonych w przepisach o ochronie danych osobowych. Nieprawidłowości w tym zakresie dotyczyły m.in. nie dopełnienia obowiązku zgłoszenia

prorowadzonych zbiorów do rejestracji Generalnemu Inspektorowi oraz zbierania w szerszym zakresie danych osobowych niż wynika to z przepisów prawa.

W 2006 r. przeprowadzone zostały 132 kontrole zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

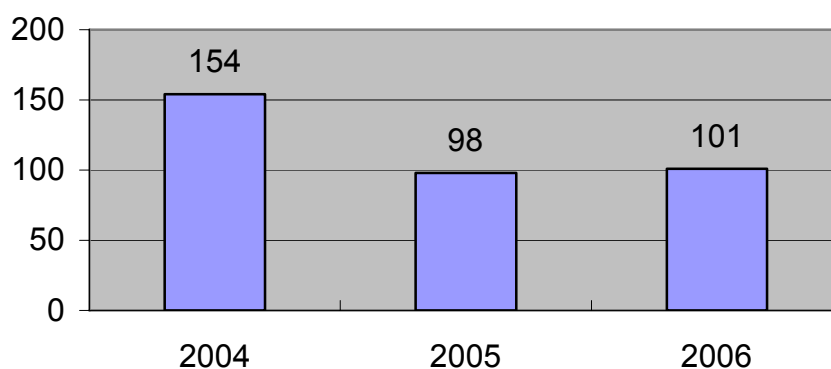


Wykres 1: Porównanie liczby przeprowadzonych kontroli w latach 2004 – 2006.

Najczęściej czynnościom kontrolnym poddawane były podmioty z sektorów administracji publicznej, ubezpieczeń społecznych, majątkowych i osobowych oraz instytucji finansowych. Na szczególną uwagę zasługuje fakt przeprowadzenia tzw. **kontroli sektorowych**, którymi objęto w omawianym roku sprawozdawczym 2006, jednostki organizacyjne Zakładu Ubezpieczeń Społecznych (14) oraz placówki Straży Granicznej (7). Ich wyniki zobrazowały sposób podejścia do problematyki ochrony danych osobowych oraz pozwoliły na sformułowanie wniosków co do zasad i sposobu przetwarzania danych osobowych przez podmioty należące do tych sektorów. Ponadto, w 2006 r. dużo uwagi poświęcono na sprawdzenie, czy podmioty, wobec których Generalny Inspektor wydał decyzje nakazujące usunięcie uchybień w procesie przetwarzania danych osobowych, przywróciły stan zgodny z prawem. W tym celu przeprowadzonych zostało 46 kontroli sprawdzających wykonanie decyzji administracyjnych, w toku których stwierdzono, że zdecydowana większość podmiotów poddanych kontroli wykonywała wydane wobec nich decyzje. Tylko w nielicznych przypadkach²⁷⁷ jednostki kontrolowane nie przywróciły stanu zgodnego z prawem, skutkiem czego było skierowanie do organu powołanego do ścigania przestępstw zawiadomienia o popełnieniu przestępstwa.²⁷⁸ Łącznie w 2006 r. Generalny Inspektor wydał 101 decyzji w związku z przeprowadzonymi kontrolami.

²⁷⁷ Np. kontrole GI-DIS-K-411/80/06 i GI-DIS-K-411/81/06.

²⁷⁸ Zawiadomienia z dnia 31.01.2007 r., nr GI-DIS-K-411/80/06/78/07 i GI-DIS-K-411/81/06/79/07, do Prokuratury Rejonowej Warszawa – Śródmieście o popełnieniu przestępstwa określonego w art. 53 ustawy o ochronie danych



Wykres 2: Porównanie liczby decyzji wydanych w związku z przeprowadzonymi kontrolami w latach 2004 – 2006.

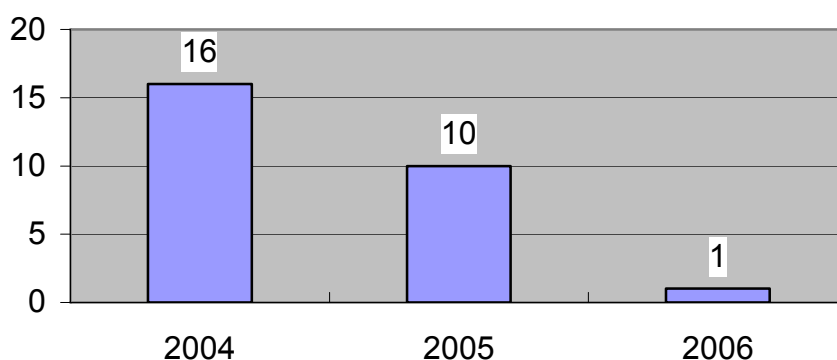
Obowiązki określone w przepisach o ochronie danych nie były wykonywane przez jednostki kontrolowane najczęściej z powodu błędnej interpretacji tych przepisów oraz ich niekonsekwentnego stosowania. Częstą przyczyną, w szczególności w przypadku podmiotów z sektora służby zdrowia, był również brak odpowiednich środków finansowych, niezbędnych do pokrycia kosztów związanych z wdrożeniem rozwiązań zapewniających prawidłowe spełnienie wymogów. W niektórych przypadkach przyczyny powyższego stanu rzeczy wynikały jednak nie tylko z braku odpowiednich środków finansowych, ale także z niewłaściwego podejścia osób odpowiedzialnych za przetwarzanie danych osobowych do problematyki ochrony tych danych, a nawet z lekceważenia przepisów. Świadczy o tym w szczególności nie wykonywanie nawet tych obowiązków, które nie pociągają za sobą nadmiernych kosztów finansowych, np. brak ewidencji osób upoważnionych do przetwarzania danych osobowych, czy też nie wyznaczenie administratora bezpieczeństwa informacji.

Na podkreślenie zasługuje fakt, że w większości przypadków stwierdzone w trakcie kontroli uchybienia były usuwane przez jednostki kontrolowane w toku postępowania. Natomiast do nielicznych należały sytuacje składania przez te jednostki wniosków o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora oraz zaskarżania decyzji do Wojewódzkiego Sądu Administracyjnego w Warszawie. Należy także podnieść, że w zdecydowanej większości przypadków Wojewódzki Sąd Administracyjny w Warszawie oddalał skargi, podzielając stanowisko zajmowane przez Generalnego Inspektora Ochrony Danych Osobowych w zaskarżonych decyzjach.

Na podstawie ustaleń z kontroli przeprowadzonych w 2006 r. należy stwierdzić, że w porównaniu z latami ubiegłymi osoby odpowiedzialne za przetwarzanie danych osobowych

osobowych, polegającego na zaniechaniu wykonania obowiązku zgłoszenia zbioru danych osobowych klientów do rejestracji Generalnemu Inspektorowi, oraz w art. 51 ustawy o ochronie danych osobowych, polegającego na umożliwieniu dostępu do danych osobowych osobom nieuprawnionym.

wykazały większą świadomość zagrożeń związanych z przetwarzaniem danych osobowych, a tym samym świadomość konieczności zapewnienia odpowiednich środków organizacyjnych i technicznych zapewniających ochronę tych danych. Konsekwencją było większe wyczulenie na prawidłowe dopełnienie obowiązków wynikających z przepisów o ochronie danych osobowych, co oczywiście nie oznacza, że obowiązki te zostały wykonane w sposób właściwy. Niestety, powyższe spostrzeżenia nie dotyczą wszystkich podmiotów, w których przeprowadzono kontrole. Zdarzały się bowiem inspekcje, które wykazywały, że jednostki kontrolowane nie wykonywały większości obowiązków wynikających z przepisów o ochronie danych osobowych.



Wykres 3: Skargi wniesione do Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Naczelnego Sądu Administracyjnego w związku z przeprowadzonymi kontrolami w latach 2004 – 2006.

W ramach zadań kontrolnych związanych z **oceną zabezpieczeń technicznych**, przeprowadzone zostały 124 **kontrole**, w tym 26 należących do kategorii **kontroli kompleksowych**, obejmujących całość problematyki związanej z ochroną danych osobowych. Pozostałe kontrole należały do kategorii kontroli częściowych i obejmowały wybrane zagadnienia dotyczące przetwarzania danych osobowych w systemach informatycznych. Czterdzieści jeden z kontroli częściowych miało charakter kontroli sprawdzającej wykonanie zaleceń pokontrolnych. W sumie skontrolowano 485 systemów informatycznych wykorzystywanych do przetwarzania danych osobowych.

Jak wynika z poniżej przedstawionego zestawienia, liczba skontrolowanych systemów informatycznych, od 2004 roku ma tendencję wzrostową.

- rok 2004 = 123 kontrole, obejmujące 359 systemów informatycznych,
- rok 2005 = 116 kontroli, obejmujących 456 systemów informatycznych,
- rok 2006 = 124 kontrole, obejmujące 485 systemów informatycznych.

Stopień wypełnienia w poszczególnych latach (od roku 2004 do 2006) wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie i rozporządzeniu przedstawiony został poniżej w formie wykresów statystycznych. Porównanie stopnia realizacji poszczególnych wymogów ustawy w latach 2004 - 2006 wskazuje wyraźnie, że największy wzrost odnotowano w odniesieniu do technicznych warunków przetwarzania danych osobowych, a zwłaszcza w obszarze wymagań dotyczących funkcjonalności systemów informatycznych. W roku 2006 o wiele więcej systemów informatycznych, niż w latach poprzednich posiadało funkcjonalności umożliwiające odnotowanie informacji, o których mowa w § 7 rozporządzenia. W analizowanym 2006 r. stopień spełnienia wymagań formalno-organizacyjnych kształtował się na niezmiennym w stosunku do poprzedniego roku poziomie i wynosił niewiele ponad 80%. Stwierdzone uchybienia w przeważającej mierze dotyczyły niewłaściwej treści takich dokumentów, jak polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych, czy ewidencja użytkowników upoważnionych do przetwarzania danych osobowych, a nie jak miało to miejsce w latach ubiegłych całkowitego braku wspomnianych dokumentów.

O czym już była mowa wcześniej, z uwagi na różnorodność systemów informatycznych, działania kontrolne obejmowały szeroki zakres rozwiązań technologicznych - od najbardziej zaawansowanych opartych o skomplikowane mechanizmy bazodanowe po najprostsze, gdzie zbiory danych osobowych przetwarzane były z wykorzystaniem powszechnie dostępnych aplikacji biurowych, takich jak, np. Ms Excel.

W przypadku rozbudowanych systemów informatycznych zaobserwowano, że firmy stosują coraz częściej globalne podejście do rozwiązywania problemów bezpieczeństwa przetwarzania. Wdrożenie procedur wyznaczających sposób i zasady postępowania w zakresie bezpieczeństwa, w połączeniu z zaawansowanymi rozwiązaniami technicznymi nadzorującymi logiczną i fizyczną ochroną danych, przynoszą pożądane efekty. Powodują one podnoszenie poziomu stosowanych zabezpieczeń, zwłaszcza w odniesieniu do systemów informatycznych o strukturze scentralizowanej, w których przetwarzane są duże zbiory danych osobowych. Zdecydowana większość instytucji, przetwarzających dane osobowe za pomocą wspomnianych wyżej systemów informatycznych wprowadziła również skomplikowane mechanizmy i narzędzia zarządzania tożsamością użytkowników. Umożliwiały one bardzo dokładne określanie zakresu upoważnień do przetwarzania danych.

W 2006 roku zaobserwowano dalszy wzrost liczby systemów informatycznych, w których przez Internet przetwarzane są dane osobowe. Coraz częściej wykorzystywana transmisja danych z wykorzystaniem sieci publicznej niesie za sobą konieczność wyboru zabezpieczeń na odpowiednio wysokim poziomie dla występujących w takich okolicznościach zagrożeń. Podobnie jak ma to miejsce w przypadku instytucji wykorzystujących skomplikowane systemy bazodanowe, również firmy

wykorzystujące Internet w procesie przekazywania danych zastosowały środki kryptograficznej ochrony danych oraz inne skomplikowane mechanizmy uniemożliwiające naruszenie przez osoby nieupoważnione integralności tych danych. Wdrożenie tak rozbudowanych mechanizmów zabezpieczeń spowodowane jest świadomością administratorów danych, co do istnienia wysokiego ryzyka związanego z transmisją danych w Internecie. Dzięki temu tylko w około 5% skontrolowanych jednostkach wskazano uchybienia dotyczące nieprawidłowości w przetwarzaniu danych przy użyciu sieci publicznych.

W przypadku systemów informatycznych zainstalowanych na pojedynczych stanowiskach nie podłączonych do sieci komputerowych oraz zbiorów przetwarzanych lokalnie na stacjach komputerowych w pojedynczych plikach, typu edytor tekstu, arkusz kalkulacyjny, czy lokalna baza danych, kluczową rolę odgrywały zabezpieczenia fizyczne obszaru przetwarzania danych osobowych oraz wprowadzone zabezpieczenia logiczne stacji roboczych, takie jak, np. wprowadzenie odrębnych identyfikatorów oraz odpowiednio skomplikowanych haseł dostępu do systemu informatycznego. Dla zbiorów danych przetwarzanych w formie pojedynczych plików tworzonych za pomocą aplikacji typu Ms Excel, czy Ms Word, wymagania dotyczące poziomu zabezpieczeń realizowane były na właściwym poziomie. Inspektorzy GODO zaobserwowali tu jednak problem ze spełnieniem wymogu § 7 ust. 2 rozporządzenia, czyli z automatycznym odnotowywaniem informacji o dacie pierwszego wprowadzenia danych oraz identyfikatorze użytkownika wprowadzającego dane do systemu. Większość z poddanych kontroli zbiorów, które przetwarzane były w jednej z wymienionych powyżej aplikacji nie spełniał wskazanego wymogu.

Reasumując stwierdzić należy, że poziom dostosowania procesu przetwarzania danych osobowych do wymogów ustawy i rozporządzenia w kontrolowanych przez GODO jednostkach, wydaje się z każdym rokiem ulegać poprawie. Znaczący wpływ na wzrastający poziom bezpieczeństwa przetwarzania danych osobowych ma wzrost świadomości istniejących zagrożeń wśród pracowników. Świadomość ta umacniana jest poprzez stałe szkolenia kadry pracowniczej w zakresie obowiązujących przepisów i rzeczywistej potrzebie przykładania dużej wagi do zagadnień związanych z bezpieczeństwem przetwarzania danych.

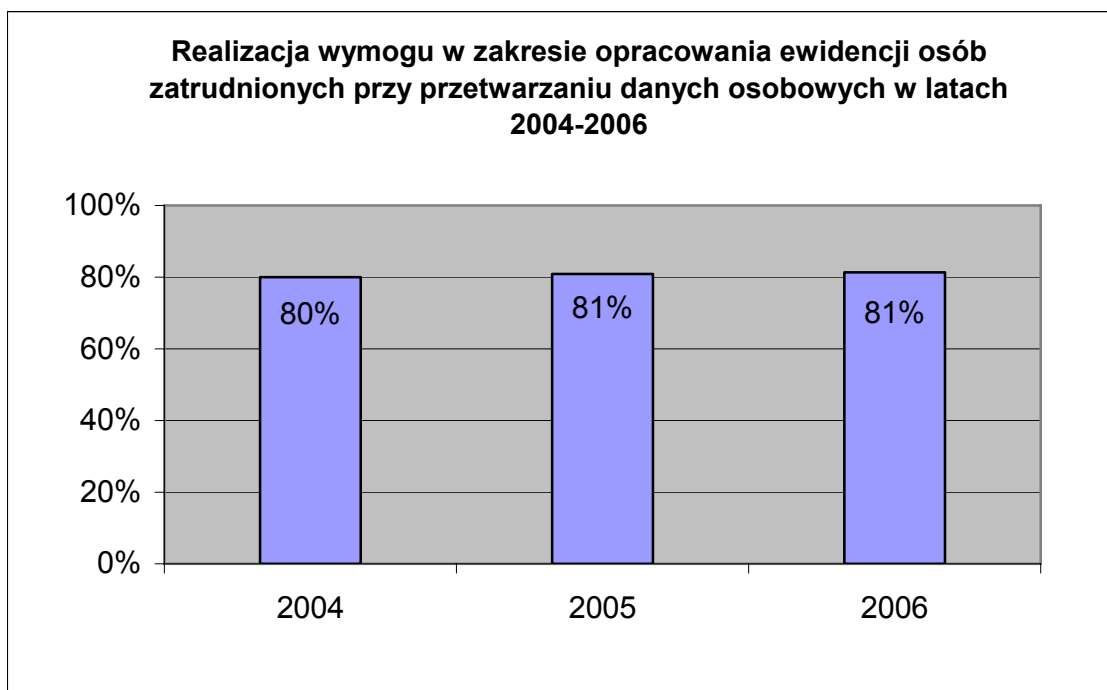
Stopień wypełnienia wymogów formalnych i organizacyjnych odnoszących się do warunków, jakim powinny odpowiadać urządzenia i systemy informatyczne używane do przetwarzania danych osobowych przedstawiono poniżej. Poszczególne zestawienia obrazują procentowe wyniki kontroli w odniesieniu do ogólnej liczby kontroli w danym roku lub ogólnej liczby kontrolowanych w danym roku systemów informatycznych. W zestawieniach tych przyjęto zasadę, że warunki odnoszące się do wymaganych funkcjonalności systemów informatycznych oceniane były w skali procentowej do liczby kontrolowanych systemów. Pozostałe natomiast, odnoszące się, np. do dokumentacji procesu

przetwarzania, czy też, np. obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oceniano w skali procentowej w stosunku do liczby kontrolowanych podmiotów.

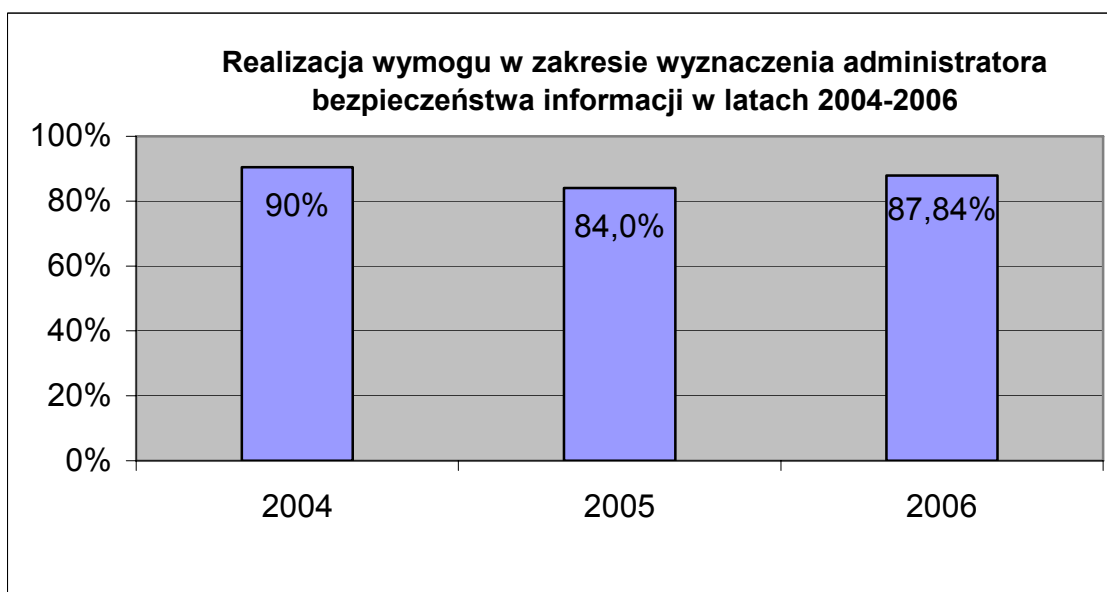
Co do stopnia wypełnienia wymogów formalnych i organizacyjnych, jednostkę statystyczną stanowił kontrolowany podmiot. Przewidziane obowiązki do wypełnienia uznawano w niniejszej ocenie jako zrealizowane, jeśli kontrolowana jednostka posiadała odpowiednie dokumenty i zawierały one co najmniej połowę wymaganej treści. Stopień wykonania przez kontrolowane podmioty poszczególnych warunków przedstawiono na *Wykresach. 4-7*.



Wykres 4: Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych.

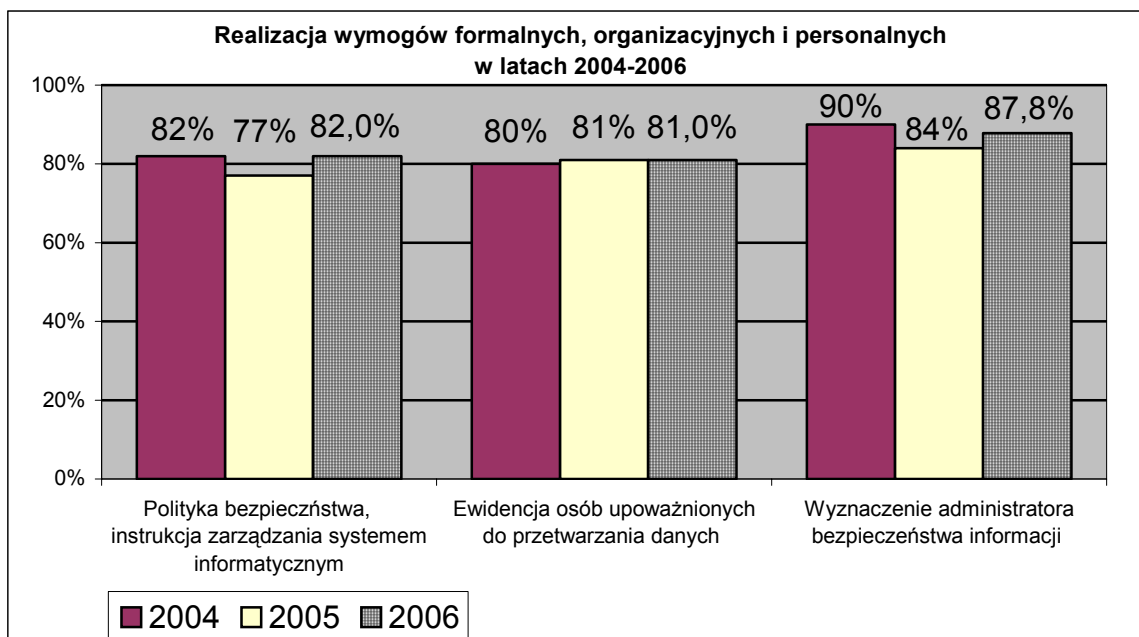


Wykres 5: Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

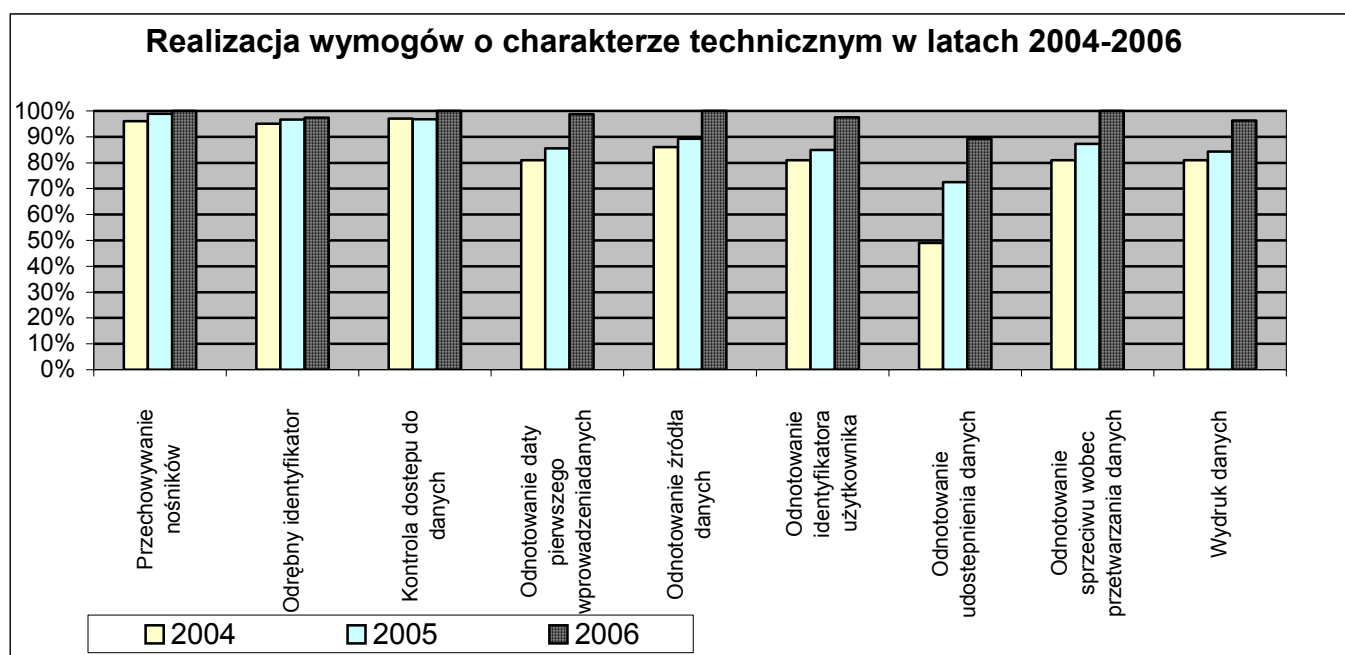


Wykres 6: Stopień realizacji obowiązku wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji.

Stopień wypełnienia wymogów formalnych, organizacyjnych i personalnych odnoszących się do warunków, jakim powinny odpowiadać urządzenia i systemy informatyczne używane do przetwarzania danych osobowych zestawiono na poniższym *Wykresie 7*:

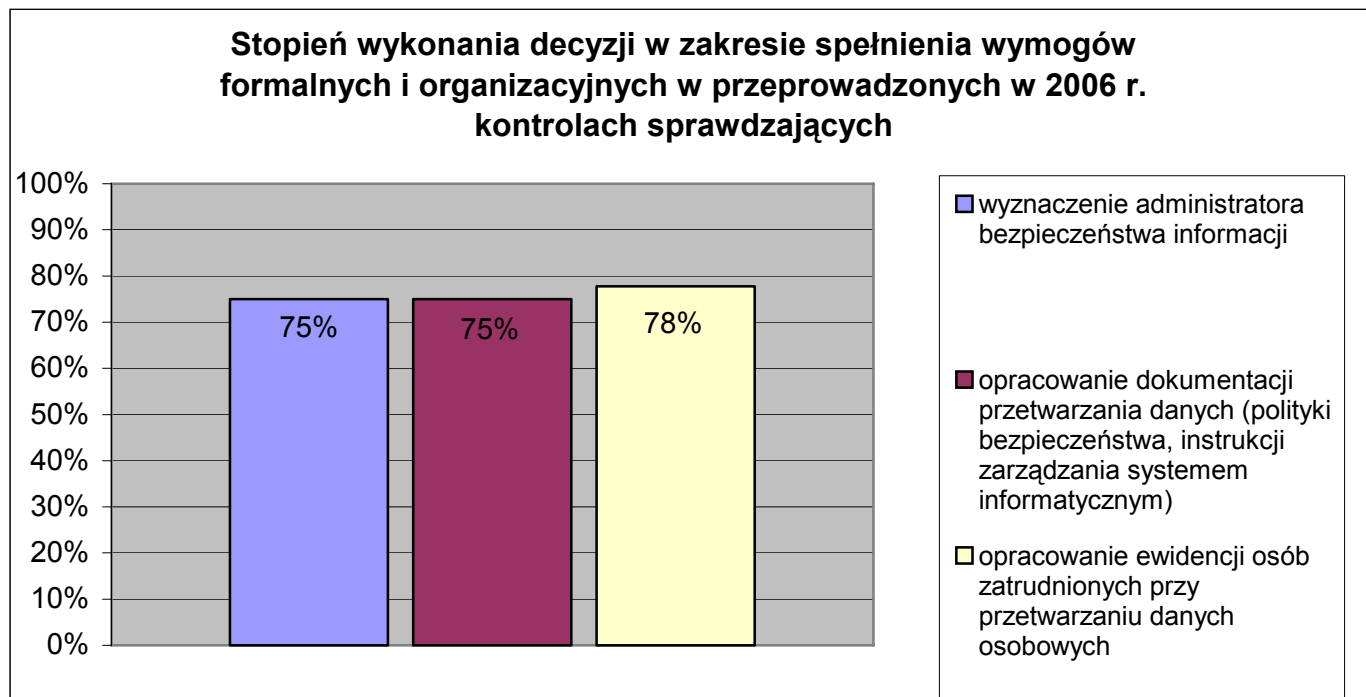


Jednostkę statystyczną w zestawieniach odnoszących się do stopnia realizacji technicznych warunków przetwarzania danych stanowił kontrolowany system lub kontrolowany zbiór danych. Przewidziane warunki uznawano dla kontrolowanego systemu/zbioru jako zrealizowane, jeśli system posiadał wymaganą funkcjonalność, lub funkcjonalność ta była realizowana przy użyciu dedykowanych modułów programowych zgodnie z warunkami określonymi w § 7 ust. 4 rozporządzenia.

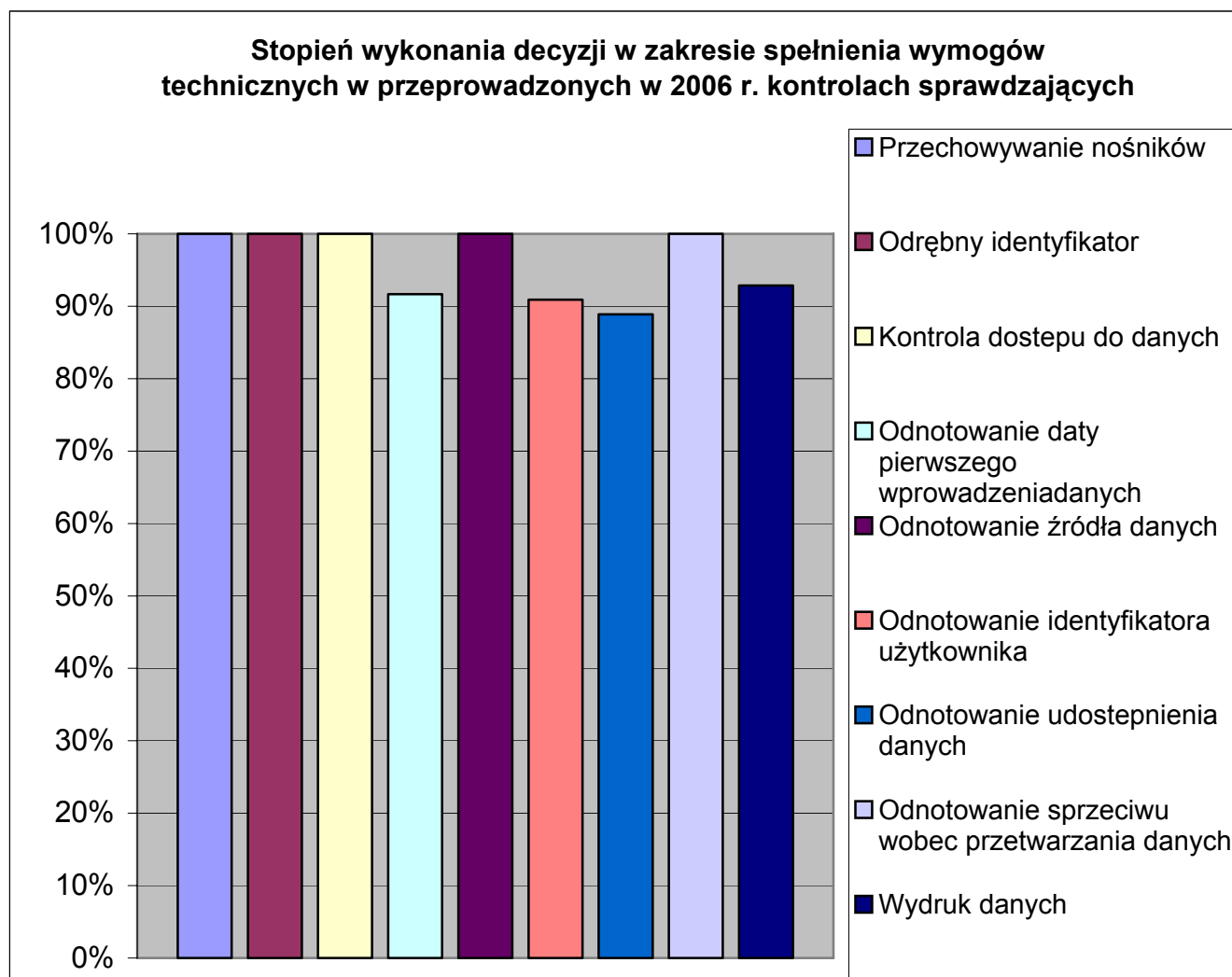


Wykres 8: *Stopień realizacji wymogów technicznych w latach 2002 – 2006.*

Stopień wykonania decyzji administracyjnych wydanych przez Generalnego Inspektora w zakresie wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie i rozporządzeniu, przedstawiony został na poniższych Wykresach 9-10.



Wykres 9: Stopień wykonania decyzji w zakresie spełnienia wymogów formalnych i organizacyjnych w przeprowadzonych w 2006 r. kontrolach sprawdzających.



Wykres 10: Stopień wypełnienia wymogów technicznych w przeprowadzonych w 2006 r. kontrolach sprawdzających

Przeprowadzone kontrole sprawdzające wykazały, że stopień wykonania przez kontrolowane jednostki decyzji Generalnego Inspektora Ochrony Danych Osobowych w zakresie dotyczącym prowadzenia dokumentacji wynosił około 75%. Natomiast stopień wykonania przez kontrolowane jednostki decyzji odnośnie wymogów technicznych oscyluje między 90% - 100%.

W omawianym roku sprawozdawczym 2006, odnotowano nieznaczny spadek **skarg** w porównaniu z rokiem ubiegłym. Ich ocena pod kątem znajomości i efektywności stosowania w praktyce zasad ochrony danych osobowych prowadzi do wniosku, iż zagadnienia te w dalszym ciągu przysparzają sporo problemów i to zarówno podmiotom z sektora publicznego, jak i prywatnego.

W dalszym ciągu zauważalne są wątpliwości interpretacyjne co do przesłanki zgody. Przesłanka ta błędnie traktowana jest jako jedyna uzasadniająca wszelkie operacje na danych osobowych, mimo istnienia innych przesłanek legalizujących proces przetwarzania danych osobowych.

Np. w sytuacji, gdy przetwarzanie danych osobowych następuje w związku z wykonywaniem zadań wynikających z ustaw szczególnych, pobieranie zgody jest zbędne. Powyższe uchybienia spotyka się zarówno w sektorze publicznym, jak i prywatnym. W sektorze publicznym problemy dotyczą głównie ośrodków pomocy społecznej, które pobierają od osób starających się o przyznanie świadczeń z pomocy społecznej zgodę na przeprowadzenie wywiadu środowiskowego, które to uprawnienie jest realizacją obowiązku wynikającego z przepisów ustawy o pomocy społecznej. Obserwowane jest także nieprawidłowe umieszczanie tego typu klauzul w treści rozporządzeń wykonawczych do ustaw nakładających na organy administracji publicznej określone obowiązki. W rezultacie podmioty z sektora publicznego mają problemy z wydaniem, np. decyzji administracyjnych, czy też przeprowadzeniem stosownych dowodów w ramach wiążących je procedur. W sektorze prywatnym z błędną interpretacją przesłanki zgody można było się spotkać z reguły w sytuacjach zawierania wszelkiego rodzaju umów. Pobierana wówczas zgoda na przetwarzanie danych osobowych dla celów związanych z realizacją danej umowy łączona jest z przetwarzaniem danych w innych celach, np. w celach marketingowych lub udostępniania danych innym podmiotom. Z kwestią odbierania zgody związany był zatem także problem nie zapewniania przez administratorów opcjonalności jej wyrażania. Sytuacje te dotyczyły głównie sektora mediów, podmiotów świadczących usługi za pośrednictwem sieci Internet, firm marketingowych oraz incydentalnie - banków i firm telekomunikacyjnych.

W analizowanym 2006 roku, wciąż sporne są kwestie dotyczące upubliczniania danych osobowych w sytuacji braku przepisu, który stanowiłby podstawę prawną do takiego działania, a jednocześnie działania takie nie poprzedza zgoda osób zainteresowanych. Nieprawidłowości te odnotowuje się od lat po stronie wspólnot i spółdzielni mieszkaniowych, które mimo wyposażenia w różne prawne środki dyscyplinujące swoich członków - dłużników, rozpowszechniają informacje o nich w miejscach publicznych, do których dostęp mają podmioty nieupoważnione. Zjawisko takie pojawiło się także po stronie pracodawców, którzy upubliczniają dane osobowe byłych pracowników, z którymi prowadzą spory na stronach internetowych mimo braku podstaw prawnych do takiego działania. Wiele wątpliwości skarżących wynika z nieznanomości obowiązujących przepisów, stąd też upatrują w sposób błędny naruszeń ustawy o ochronie danych osobowych przez organy i instytucje państwowe w sposobie prowadzenia tych postępowań oraz w treści wydanych przez nie rozstrzygnięć. Problem ten jest szczególnie widoczny na tle rozpatrywanych skarg z sektora wymiaru sprawiedliwości i administracji publicznej, gdzie istniejące procedury (karna, cywilna i administracyjna) są podstawą do zbierania i udostępniania danych osobowych, a ocena rzetelności prowadzenia tych postępowań należy nie do GIODO, ale organów nadzoru w trybie instancyjnym. Nieznajomość przepisów należy często przypisać także samym administratorom danych, którzy mając specjalne regulacje ustawowe wskazujące komu i w jakich sytuacjach można udostępniać dane, niezasadnie odmawiają udostępnienia danych (np. spółdzielnie odmawiają udostępnienia informacji swoim członkom o innych członkach

spółdzielni zawartych w rejestrze spółdzielców) z powołaniem się na przepisy o ochronie danych osobowych.

Podmioty przetwarzające dane osobowe, i to zarówno z sektora publicznego, jak i prywatnego, wciąż mają problemy z należyтым wypełnianiem obowiązku informacyjnego wynikającego z art. 24 i art. 25 ustawy oraz ignorują uprawnienia kontrolne osób, których dane osobowe przetwarzają. Pisma o realizację uprawnień kontrolnych pozostają bez odpowiedzi, albo też odpowiedź jest przekazywana z wielomiesięcznym opóźnieniem mimo wyznaczonego ustawowo terminu 30 dni. Realizacja obowiązków informacyjnych i uprawnień kontrolnych ma szczególne znaczenie dla zapewnienia osobom, których danymi posługuje się administrator, realnej kontroli nad przetwarzaniem danych osobowych. W dobie wysoko rozwiniętej komunikacji elektronicznej, a co za tym idzie pozyskiwania danych osobowych za pomocą ogólnodostępnych sieci publicznych, brak informacji o podmiocie, który pozyskuje dane rodzi uzasadnione podejrzenie nielegalnego handlu tymi danymi. W sytuacjach, gdy postępowania wskazywały na nielegalność działań, a podmiotu odpowiedzialnego za powyższe nie można było zidentyfikować (co miało miejsce zwłaszcza w sprawach, gdzie siedziba administratora danych miała się mieścić w państwach trzecich) GODO kierował zawiadomienia o popełnieniu przestępstwa uznając, iż większe instrumenty operacyjne posiadają organy ścigania. W analizowanym 2006 roku, nadal jednak widoczna była tendencja odmowy wszczęcia, bądź umarzania przez te organy postępowań karnych zainicjowanych przez Generalnego Inspektora, z uwagi na znikomą społeczną szkodliwość czynu lub niewykrycie sprawcy czynu. Powyższa tendencja zdaje się świadczyć o tym, iż przedstawiciele organów ścigania nadal nie dostrzegają wagi problemu, jakim jest nieprzestrzeganie zasad przetwarzania danych osobowych, choć w wielu przypadkach na konieczność ponownej analizy sprawy wskazywał im uwagę Minister Sprawiedliwości wskutek wystąpień GODO.

Znacząco spadła liczba skarg dotycząca zakresu danych pozyskiwanych, np. dla zawarcia umów. Jest to szczególnie widoczne w sektorach, w których wprowadzono stosowne regulacje ustawowe, np. w sektorze bankowości i telekomunikacji. Nie oznacza to, iż w sektorach tych nie odnotowano nieprawidłowości w procesie przetwarzania danych osobowych. Wraz z wejściem w życie nowych przepisów Prawa bankowego, sporna okazała się bowiem kwestia przetwarzania danych osobowych klientów banków terminowo wywiązujących się ze swoich zobowiązań w zbiorach BIK i ZBP, po wygaśnięciu łączących ich z bankami umów. Ponieważ w tym zakresie jedyną przesłanką powinna być zgoda każdego z tzw. rzetelnych klientów, banki odmawiały usuwania danych ze zbiorów ww. instytucji uzasadniając tę okoliczność 3-letnim okresem dostosowawczym dla wprowadzenia nowych przepisów. Z taką interpretacją w przypadku składanych indywidualnie skarg GODO nie mógł się zgodzić. Orzecznictwo sądów administracyjnych podzieliło stanowisko GODO wskazując, że ww. okres dostosowawczy odnosi się do zapewnienia przez banki odpowiedniej infrastruktury

technicznej dla usunięcia danych osobowych wszystkich klientów banków, którzy nie wyrażą zgody na ich figurowanie w zbiorach instytucji, o których mowa w Prawie bankowym.

Podsumowując, w roku sprawozdawczym 2006, orzeczenia sądów administracyjnych zapadłe na skutek skarg wniesionych od decyzji Generalnego Inspektora Ochrony Danych Osobowych, w dużej mierze dotyczyły spraw z zakresu udostępnienia danych w związku z cesją wierzytelności. W orzeczeniach tych uznano brak kompetencji GODO do oceny realizacji umów cywilnych i przesądzone o dopuszczalności egzekwowania przez wierzyciela swych praw wobec dłużników oraz przekazywanie tych danych podmiotom trzecim na podstawie przesłanki prawnie usprawiedliwionych celów administratora danych. Sądy w wydawanych rozstrzygnięciach często przyznawały słuszność stanowiskom organu ochrony danych osobowych odnoszącym się do braku podstaw do jego ingerencji w tok postępowań prowadzonych na podstawie odrębnych regulacji prawnych.

W 2006 r. odnotować należy spadek skarg na niewłaściwe zabezpieczenia danych osobowych zawartych w dokumentacji prowadzonej przez administratorów danych. O ile odnotowano w latach ubiegłych znaczną liczbę tego typu naruszeń po stronie pracodawców, podmiotów świadczących usługi medyczne czy ubezpieczeniowe, to w omawianym roku sprawozdawczym 2006 sygnały w tym zakresie nie występowały, choć nadal przedmiotem wielu skarg było udostępnienie danych osobom nieupoważnionym w zakresie, np. danych zastrzeżonych.

Z kolei analiza przesyłanych Generalnemu Inspektorowi Ochrony Danych Osobowych do **zaopiniowania projektów aktów normatywnych** prowadzi do wniosku, iż podmioty inicjujące proces legislacyjny – czy to z sektora publicznego czy prywatnego – zainteresowane są pozyskiwaniem coraz szerszych uprawnień z zakresu przetwarzania danych osobowych.

I tak, w sektorze prywatnym projektowane przepisy często wprowadzały sformułowania umożliwiające przechowywanie dokumentacji zawierającej dane osobowe przez zbyt długi okres, czego przykładem może być nowelizacja przepisów regulujących działalność sektora bankowego m.in. pod kątem możliwości przetwarzania przez banki danych osobowych ich byłych klientów do celów statystycznych przez okres 12 lat. Nie brakowało również prób rozszerzania poprzez projektowane przepisy katalogu podmiotów mających dostęp do różnorodnych ewidencji zawierających dane osobowe, w tym dane sensytywne. O powyższe uprawnienie wnosiły m.in. firmy ubezpieczeniowe. Pojawiły się również projekty aktów normatywnych przewidujących zwolnienie określonej grupy podmiotów z konieczności dopełniania obowiązków wynikających z przepisów ustawy o ochronie danych osobowych. Fundusze inwestycyjne zainteresowane były, np. zwolnieniem ich z obowiązku informacyjnego, określonego w art. 25 ustawy o ochronie danych osobowych.

Z kolei wśród uchybień powtarzających się w toku prac legislacyjnych inicjowanych przez podmioty sektora publicznego wskazać należy na częste formułowanie delegacji ustawowych do wydawania rozporządzeń wykonawczych regulujących kwestie przetwarzania danych osobowych

natury szczególnie chronionej. Działo się tak często w sektorze służby zdrowia. Generalny Inspektor spotkał się również z sytuacją wprowadzania przepisów wyłączających proces przetwarzania danych osobowych spod jego kompetencji kontrolnych (przepis w tym zakresie pojawił się w ustawie regulującej działalność Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu) lub przyznawania organom administracji publicznej zbyt daleko idących uprawnień do ingerowania w sferę intymności osoby fizycznej (próby wprowadzenia przepisów przyznających organom samorządu terytorialnego uprawnień do pozyskiwania danych o stanie zdrowia czy opracowywania formularzy statystycznych zawierających pytania odnośnie kontaktów seksualnych).

Działania podejmowane przez Generalnego Inspektora Ochrony Danych Osobowych w związku z uczestnictwem tego organu w procesie tworzenia prawa – inicjowanego tak przez podmioty działające w sektorze prywatnym, jak i publicznym – zmierzały również do wyeliminowania błędów polegających na używaniu przez projektodawców w treści przesyłanych do zaopiniowania aktów normatywnych sformułowań mogących powodować trudności interpretacyjne, jak np.: „inne informacje”, „dane umożliwiające identyfikację osoby”, „imienna lista osób”. GIODO sygnalizował również niezgodność z przepisami ustawy o ochronie danych osobowych wprowadzania otwartego katalogu danych osobowych, których możliwość przetwarzania przewiduje się poprzez używanie zwrotu „w szczególności”. Częste tego typu zwroty pojawiały się w projektach z sektora zatrudnienia.

W 2006 r. do Generalnego Inspektora wpłynęło 10 wniosków o **udzielenie zgody na przekazanie danych osobowych do państwa trzeciego**. Stosunkowo niewielkie zainteresowanie administratorów danych możliwością przekazywania danych osobowych do państwa trzeciego na podstawie zgody Generalnego Inspektora wiąże się przede wszystkim z tym, że duża liczba międzynarodowych transferów danych odbywa się w ramach Europejskiego Obszaru Gospodarczego. Nie ma więc konieczności stosowania przepisów rozdziału 7 ustawy o ochronie danych osobowych, które regulują przekazywanie danych do państwa trzeciego. Ponadto, administratorzy danych korzystają z możliwości zastosowania innych przesłanek upoważniających do przekazywania danych do państwa trzeciego, określonych w art. 47 ust. 1, 2 lub 3 ustawy o ochronie danych osobowych, tym samym zgoda Generalnego Inspektora jest zbędna. Należy także zauważyć niewielką świadomość istnienia szerokich możliwości zastosowania uregulowanych prawem wspólnotowym wzorcowych klauzul umownych, które mogą stanowić podstawę wyrażenia zgody przez Generalnego Inspektora.

Generalny Inspektor jest uprawniony do udzielenia zgody na przekazanie danych osobowych do państwa trzeciego, pod warunkiem zapewnienia przez administratora danych odpowiedniego zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. Można to osiągnąć przede wszystkim poprzez przyjęcie odpowiednich zobowiązań umownych, do których przede wszystkim należy zaliczyć:

- a) wzorcowe klauzule umowne przyjęte przez Komisję Europejską,²⁷⁹
- b) wiążące reguły korporacyjne.²⁸⁰

W roku sprawozdawczym 2006 do Generalnego Inspektora wpływały jedynie wnioski, w których administratorzy danych powoływali się na zastosowanie wzorcowych klauzul umownych ustanowionych przez Komisję Europejską (jest to rozwiązanie preferowane przez większość organów ochrony danych osobowych w Unii). Jak dotąd nie wpłynęły do Generalnego Inspektora formalne wnioski o wyrażenie zgody na przekazanie danych do państwa trzeciego na podstawie wiążących reguł korporacyjnych, aczkolwiek Generalny Inspektor, wraz z innymi organami ochrony danych osobowych, brał udział w procedurze koordynacyjnej, mającej na celu wspólne zatwierdzenie projektów wiążących reguł korporacyjnych przedłożonych przez kilka międzynarodowych korporacji. Procedura ta poprzedza formalne złożenie wniosku o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego i wydanie decyzji administracyjnej przez Generalnego Inspektora.²⁸¹

Zadeklarowanie przez wnioskodawcę zastosowania wzorcowych klauzul umownych określonych decyzjami Komisji Europejskiej powoduje konieczność porównania przez Generalnego Inspektora przyjętych przez wnioskodawcę rozwiązań z treścią wzorcowych klauzul umownych.

²⁷⁹ Komisja Europejska na mocy art. 26 ust. 4 Dyrektywy 95/46/WE jest uprawniona do uznania w drodze decyzji, że określone wzorcowe klauzule umowne zapewniają odpowiednią ochronę danych osobowych oraz praw i wolności jednostek. Decyzje te wymagają, aby państwa członkowskie nie odmawiały uznania zabezpieczeń ustanowionych we wzorcowych klauzulach umownych określonych w decyzjach za zapewniające odpowiedni poziom ochrony danych osobowych. Nie wyłącza to jednak obowiązku spełnienia pozostałych wymogów nałożonych przez właściwe przepisy krajowe. Komisja Europejska wydała trzy takie decyzje: decyzję KE z dnia 15 czerwca 2001 r. 2001/497/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych do państw trzecich na podstawie Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 181/19, z 4.07.2001); decyzję z dnia 27 grudnia 2004 r. 2004/915/WE zmieniającą decyzję 2001/497/WE w zakresie alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz. Urz. WE L 385/19, z 29.12.2004). Powołane decyzje wprowadziły dwa zestawy klauzul umownych, które administrator danych może wykorzystać w przypadku przekazywania danych do innego administratora danych w państwie trzecim. Trzecia decyzja KE z dnia 27 grudnia 2001 r. 2002/16/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych przetwarzanych w krajach trzecich na podstawie Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. UE L 006, z 10.01.2002) wprowadziła wzorcowe klauzule umowne mające zastosowanie do przekazywania danych osobowych w przypadku powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy o ochronie danych osobowych.

²⁸⁰ Wiążące reguły korporacyjne są odrębnym instrumentem prawnym, który szczególną rolę może odegrać w przypadku przekazywania danych osobowych w ramach międzynarodowych korporacji. Jest to stosunkowo nowe rozwiązanie prawne, które z jednej strony może zapewnić większą elastyczność, z drugiej zaś zagwarantować w ramach korporacji jednolity, a zarazem wysoki poziom ochrony praw osób, których dane dotyczą, bez względu na poziom ochrony danych osobowych zapewniony na terytorium poszczególnych państw.

²⁸¹ Por. np. GI-DP-071/262/06. Biorąc pod uwagę, że wiążące reguły korporacyjne w zamierzeniu mają mieć charakter powszechny, europejskie organy ochrony danych osobowych przyjęły procedurę współpracy, której celem jest wspólne rozpatrywanie wniosków o wyrażenie zgody na przekazywanie danych osobowych, na podstawie wiążących reguł korporacyjnych (dokument roboczy WP 107 przyjęty w dniu 14 kwietnia 2005 r.). Dokument ten jest dostępny w wersji elektronicznej na stronie internetowej: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

Ponadto Generalny Inspektor bada również okoliczności planowanego transferu danych (w tym również przyjęte przez odbiorcę danych organizacyjne i techniczne środki zabezpieczeń).²⁸²

W 2006 r. znacznie zwiększyła się liczba państw, do których administratorzy danych zamierzali przekazać dane. Oprócz Stanów Zjednoczonych Ameryki, Indii, czy Sri Lanki, wnioski dotyczyły także m.in.: Antyli Holenderskich, Brazylii, Wysp Dziewiczych, Chile, Kolumbii, Ekwadoru, Jamajki, Meksyku, Trynidadu i Tobago, Urugwaju, Wenezueli, Nowej Zelandii, Hongkongu, Japonii Korei Południowej, Filipin, Tajlandii, Wietnamu, Egiptu, Izraela, Maroko, Federacji Rosyjskiej, Republiki Południowej Afryki i Turcji.²⁸³

Generalny Inspektor rozpatrywał również wniosek dotyczący przekazywania danych osobowych do odbiorcy z siedzibą w Argentynie, którą Komisja Europejska uznała za państwo zapewniające odpowiedni poziom ochrony danych osobowych.²⁸⁴ Uznanie przez Komisję Europejską danego państwa za zapewniające odpowiednią ochronę jest równoznaczne z tym, iż zapewnia ono takie same gwarancje ochrony, jakie są zapewnione na terytorium Rzeczypospolitej Polskiej. Tym samym spełniona jest przesłanka określona w art. 47 ust. 1 ustawy o ochronie danych osobowych, a Generalny Inspektor obowiązany był umorzyć postępowanie administracyjne w omawianym zakresie z powodu bezprzedmiotowości.²⁸⁵ Podobnie został rozstrzygnięty wniosek dotyczący przekazania danych osobowych do Kanady²⁸⁶.

Z punktu widzenia **rejestracji zbiorów danych osobowych**, nie można kategorycznie stwierdzić, iż rok 2006 przyniósł zasadnicze zmiany, które pozwoliłyby uznać, że problematyka ochrony danych osobowych na trwale zakorzeniła się w świadomości prawnej administratorów danych. Należy przy tym pamiętać, iż dla większości administratorów zgłoszenie zbioru do rejestracji stanowi

²⁸² Wnioskodawca powinien przedstawić dowody pozwalające na potwierdzenie zapewnienia przez niego odpowiedniego zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osób, których dane dotyczą. Dlatego Generalny Inspektor wymaga wskazania: stron takiego transferu danych osobowych, kategorii danych, ich zakresu, celu oraz czasu trwania proponowanych operacji przekazywania danych, środków podjętych w celu zagwarantowania przez strony zamierzające przekazywać dane osobowe, praw osób, których dane dotyczą, w tym np. przedstawić treść konkretnej umowy (np. zawierającej wzorcowe klauzule umowne) stanowiącej podstawę przekazania danych, środków organizacyjno – technicznych, które odbiorca danych zapewni w celu zabezpieczenia przekazywanych danych (dokładny opis).

²⁸³ GI-DP-444/8/06, GI-DP-404/6/06, GI-DP-404/5/06.

²⁸⁴ Komisja Europejska na mocy art. 25 ust. 6 Dyrektywy jest uprawniona do stwierdzenia w drodze decyzji, że dane państwo trzecie zapewnia odpowiedni stopień ochrony, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji z Komisją Europejską, w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych. Komisja Europejska wydała w dniu 30 czerwca 2003 r. decyzję 2003/490/WE w sprawie właściwej ochrony danych osobowych w Argentynie (Dz. Urz. UE L 168 z 5. 07. 2003). Zgodnie z jej art. 1 dla celów art. 25 ust. 2 dyrektywy 95/46/WE, Argentyna jest traktowana jako państwo zapewniające odpowiedni poziom bezpieczeństwa w odniesieniu do danych osobowych przekazywanych ze Wspólnoty.

²⁸⁵ GI-DEC-DESiWM-543/06/1315.

²⁸⁶ GI-DEC-DP-358/06/988. Komisja Europejska wydała w dniu 20 grudnia 2001 r. decyzję 2002/2/WE w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych (Dz. Urz. UE L 2/13 z 4. 01. 2002). Na mocy jej art. 1 Kanada uznawana jest za kraj zapewniający odpowiedni poziom ochrony danych osobowych przekazywanych ze Wspólnoty do odbiorców objętych przepisami kanadyjskiej ustawy o ochronie informacji osobowych i dokumentów elektronicznych.

pierwszy kontakt z zasadami ochrony danych osobowych. Przygotowanie do zgłoszenia zbioru danych do rejestracji daje możliwość, czy też wręcz wymusza, zapoznanie się z przepisami regulującymi tę dziedzinę prawa, zweryfikowanie stanu faktycznego i dostosowanie do obowiązujących wymogów. Z formalnego punktu widzenia, w dalszym ciągu przy wypełnianiu formularza zgłoszenia, administratorzy danych popełniają wiele błędów, co skutkuje koniecznością wyjaśnienia nieprawidłowości, czy też nieścisłości, występujących w zgłoszonych wnioskach. Pozytywnym aspektem postępowań wyjaśniających jest niewątpliwie edukacja. Administratorzy danych otrzymują w ten sposób fachowe wskazówki, a co za tym idzie szansę dostosowania prowadzonej działalności do wymogów określonych właściwymi przepisami prawa.

Postępowanie rejestracyjne w wielu przypadkach ujawniło nieznaną przepisy ustawy o ochronie danych osobowych lub wręcz ignorowanie wynikających z niej obowiązków. Nawet podmioty realizujące zadania publiczne, w szczególności powołane do wykonywania działań wyznaczonych przepisami prawa, nie zawsze należycie wywiązywały się z obowiązku rejestracji (np. jednostki samorządowe prowadzące zbiory oświatowe), bądź też w ogóle go nie wykonywały (np. szkoły wyższe). Nieprawidłowości ujawnione w procesie rejestracji dotyczyły generalnie wszystkich elementów ujętych w ramy zgłoszenia zbioru danych osobowych. Wśród najczęściej powtarzających się uchybień należy wymienić: nieadekwatny (zbyt szeroki), w stosunku do celu przetwarzania, zakres danych osobowych pozyskiwanych do zbioru, brak wskazania przesłanki legalności przetwarzania danych, a także sposobu zbierania i udostępniania danych osobowych. Podobnie jak w latach ubiegłych, wiele nieprawidłowości występowało w części zgłoszenia dotyczącej opisu środków technicznych i organizacyjnych, o których mowa w art. 36 – 39 ustawy o ochronie danych osobowych. Ponadto duże trudności administratorom danych sprawiała kwestia ustalenia poziomu bezpieczeństwa przetwarzania danych w systemie informatycznym.

Generalny Inspektor Ochrony Danych Osobowych, zauważając problemy administratorów danych związane z prawidłową realizacją obowiązku rejestracyjnego, opracował, wdrożył i udostępnił na swojej stronie internetowej program wspomagający wypełnianie formularza zgłoszenia. Dająca się zauważyć wśród administratorów danych coraz większa popularność tego programu pozwala przypuszczać, iż liczba nieprawidłowo zgłaszanych do rejestracji zbiorów danych będzie stopniowo malała.

Biorąc pod uwagę ogół spraw związanych z rejestracją zbiorów podkreślić należy, iż wykonywanie przez Generalnego Inspektora Ochrony Danych Osobowych zadań związanych z rejestracją zbiorów danych osobowych jest procesem ciągłym. Dotyczy to zarówno podmiotów ze sfery publicznej jak i sektora prywatnego. Błędne byłoby bowiem stwierdzenie, iż organy administracji publicznej ostatecznie wykonały obowiązek rejestracji zbiorów danych przetwarzanych przez te podmioty w celu realizacji zadań przyznanych im właściwymi przepisami prawa. Zmiany zachodzące

w obowiązujących przepisach, w tym zmiany kompetencyjne, obligują administratorów danych działających w sferze publicznej do nieustannego monitorowania procesu przetwarzania danych osobowych i aktualizowania pierwotnie dokonanych zgłoszeń, tak aby odzwierciedlony był w nich aktualny stan faktyczny i prawny, w którym funkcjonują zbiory danych osobowych. Ponadto dodatkowe zadania przyznawane tym organom skutkują tworzeniem nowych, podlegających obowiązkowi rejestracji, zbiorów danych osobowych. Podmioty prywatne zaś, często rozszerzają czy przekształcają swoją działalność, z czym w szczególności związane jest stosowanie nowych rozwiązań w zakresie zabezpieczania zbiorów. Rozwój działalności ww. podmiotów powoduje powstawanie nowych zbiorów danych osobowych lub zmiany w zbiorach istniejących dotychczas. To wszystko powinno znaleźć odzwierciedlenie w stosownym zgłoszeniu. W niektórych sektorach można zatem zaobserwować nie tylko wzrost wniosków o rejestrację zbiorów danych osobowych, lecz także większą liczbę aktualizacji zgłoszeń, np. w branżach związanych ze świadczeniem usług.

Mimo obserwowanej dynamiki napływu zgłoszeń zbiorów danych do rejestracji, przed Generalnym Inspektorem Ochrony Danych osobowych w dalszym ciągu stoi zadanie aktywizowania administratorów danych w celu dopełnienia przez nich obowiązku rejestracyjnego. Zdarzają się bowiem dziedziny, w których funkcjonują zbiory danych nie zgłoszone do rejestracji przez zobowiązane do tego podmioty. Realizacji powyższego zadania służą w szczególności sygnalizacje kierowane przez Generalnego Inspektora m.in. do podmiotów nadzorujących ww. administratorów danych.

Część III. Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych

Do ustawowych obowiązków Generalnego Inspektora Ochrony Danych Osobowych należy przedłożenie Sejmowi raz w roku sprawozdania ze swej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych. Analizy tej Generalny Inspektor dokonuje m.in. w oparciu o wyniki kontroli bezpośrednich, przeprowadzonych u administratorów danych osobowych, skarg dotyczących naruszeń ochrony danych, wydawanych opinii prawnych, orzecznictwa sądów administracyjnych oraz opinii środowisk naukowych.

W obliczu przedstawionych w Sprawozdaniu - w oparciu o treść skarg i ustaleń pokontrolnych - zagrożeń sfery prywatności i danych osobowych, Generalny Inspektor Ochrony Danych Osobowych zobowiązany jest do wnikliwej analizy swoich dotychczasowych działań na tym polu i poszukiwania coraz skuteczniejszych środków ich ochrony. Zagrożenia bezpieczeństwa danych osobowych mogą wpływać z różnych, nie zawsze możliwych do przewidzenia źródeł. Dopiero praktyka stosowania przepisów o ochronie danych osobowych weryfikuje ich skuteczność i przydatność na co dzień.

Źródło zagrożenia prawa do ochrony danych osobowych mogą stanowić przepisy obowiązującego prawa – i to zarówno ustawy o ochronie danych, jak też innych aktów. Źródeł tych zagrożeń należy upatrywać w braku przejrzystości przepisów, stosowaniu nieostrych znaczeniowo pojęć, tendencjom wyłączania ustawy o ochronie danych osobowych mocą innych ustaw, nie uwzględnianiu w przepisach obowiązującego prawa ustawowych uprawnień różnych podmiotów do pozyskiwania danych osobowych, a także częstym praktykom umarzania przez organy ścigania i sąd spraw o naruszenie ochrony danych osobowych.

Ustawa o ochronie danych osobowych ma charakter generalny w odniesieniu do tematyki ochrony danych, co oznacza, że jej dopełnienie stanowią przepisy innych ustaw odnoszących się do różnych dziedzin życia społecznego. Obserwowany brak transparentności niektórych z tych aktów powoduje trudności interpretacyjne wśród podmiotów obowiązanych do ich stosowania. Na przykład, ustawodawca projektując przepisy nie uwzględnił w nich wszystkich uprawnionych obecnie podmiotów do przetwarzania danych osobowych. W takiej sytuacji znalazła się Straż Miejska, która nie mogła inicjować i prowadzić postępowań w sprawach o wykroczenia - do czego zobowiązuje ją prawo – z uwagi na odmowę udostępnienia im danych o sprawcach wykroczeń przez banki czy operatorów sieci telekomunikacyjnych. Do niedawna w podobnej sytuacji były jeszcze Ośrodki Pomocy Społecznej, które nie mogły pozyskiwać danych z Zakładu Ubezpieczeń Społecznych objętych tajemnicą ubezpieczeniową, dla potrzeb prowadzonych przez siebie postępowań. Stało się tak dlatego, że ustawodawca nie uwzględnił Ośrodków Pomocy Społecznej w katalogu podmiotów uprawnionych do pozyskiwania informacji z zakresu ubezpieczeń społecznych.

Z informacji, jakie pojawiły się w prasie wynikało, że niektórzy przedsiębiorcy telekomunikacyjni odmawiali udostępnienia służbom obsługującym numery alarmowe (pogotowie ratunkowe, GOPR), danych lokalizacyjnych abonentów wywołujących połączenia z tymi numerami. Pomimo iż przepisy ustawy Prawo telekomunikacyjne w sposób jednoznaczny obligują operatorów publicznej sieci telefonicznej do zapewnienia służbom ustawowo powołanym do niesienia pomocy dostępu do identyfikacji linii wywołującej oraz danych dotyczących lokalizacji abonentów wywołujących połączenia z numerami alarmowymi bez ich uprzedniej zgody, w praktyce służbom wykonującym zadania ratownicze ww. podmioty odmawiały udostępnienia wnioskowanych danych, powołując się na ustawę o ochronie danych osobowych. Mamy tutaj do czynienia z przypadkami instrumentalnego traktowania ustawy i nieuzasadnionego zasłaniania się nią dla odmowy udostępnienia wnioskowanych danych. Takie zdarzenia wywołują zamieszanie wokół organu ochrony danych osobowych, a ustawa może zacząć być postrzegana, jako ograniczająca działalność różnych podmiotów.

W odniesieniu do problemów wynikających ze stosowania ustawy o ochronie danych osobowych, wskazać należy na potrzebę zapewnienia większej przejrzystości i skuteczności zawartych

w niej przepisów. Od lat poddawane są krytyce nieostre pojęcia ww. ustawy, zwłaszcza w odniesieniu do jej zakresu podmiotowego i przedmiotowego. Ponadto, analiza sposobu wykonywania przepisów o ochronie danych osobowych przez właścicieli baz danych, wskazuje na zasadność postulatów o nadanie Generalnemu Inspektorowi Ochrony Danych Osobowych prawa do nakładania kar pieniężnych, oraz prawa składania wniosków o stwierdzenie zgodności danego aktu prawnego z Konstytucją RP. W tym celu niezbędna jest jak najszybsza nowelizacja ustawy o ochronie danych osobowych.

Źródłem zagrożeń bezpieczeństwa danych osobowych może być także całkowite wyłączenie ustawy o ochronie danych osobowych mocą przepisów innych aktów prawnych. W oparciu o przedstawione w niniejszym Sprawozdaniu przykłady można wyraźnie zauważyć tendencje do deprecjonowania znaczenia ustawodawstwa z zakresu ochrony danych osobowych, wyrażające się w działaniach legislacyjnych zmierzających do wyłączenia przetwarzania danych przez niektóre podmioty spod kompetencji kontrolnych niezależnego organu do spraw ochrony danych osobowych,²⁸⁷ czy wręcz całkowitego zwolnienia pewnych instytucji z obowiązku stosowania regulacji zawartych w ustawie o ochronie danych osobowych.²⁸⁸ Występując przeciwko powyższym praktykom Generalny Inspektor wskazywał, że obowiązek zachowania nadzoru niezależnego organu nad przetwarzaniem danych osobowych przez wszystkie podmioty, wynika w sposób bezpośredni z wiążących Rzeczpospolitą Polską norm prawa europejskiego. Generalny Inspektor zauważył ponadto, że podmioty te powinny zadbać o to, aby do własnych regulacji wprowadzić przepisy, które będą gwarantowały ochronę przetwarzanych danych osobowych zarówno w systemach informatycznych, jak i papierowych. Wyłączenie mocą innych ustaw, ustawy o ochronie danych osobowych - przy jednoczesnym braku regulacji gwarantujących zabezpieczenie danych przetwarzanych m.in. w systemach informatycznych - naraża Państwo Polskie na zarzut ze strony instytucji europejskich, niespełnienia standardów międzynarodowych w tym zakresie.

Ponadto, organ do spraw ochrony danych osobowych wskazywał, że nie tylko całkowite wyłączenie spod ustawy, ale w ogóle – nawet jednostkowe zwolnienie od dopełnienia obowiązków określonych w jej przepisach wymaga, szczegółowego uzasadnienia.²⁸⁹

Warunkiem skutecznej ochrony danych osobowych jest również prawidłowa ocena zagrożeń przez administratora danych. Skoro bowiem decyduje on o celach i środkach przetwarzania danych, powinien mieć również świadomość ciężącej na nim odpowiedzialności za niezgodne z prawem

²⁸⁷ Projekt ustawy o Centralnym Biurze Antykorupcyjnym (GI-DP-023/320/05/06, GI-DP-023/64/06).

²⁸⁸ Projekty ustaw: o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990 oraz treści tych dokumentów oraz o zmianie innych ustaw; o zmianie ustawy z dnia 18 grudnia 1998 roku o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (GI-DP-023/33, 34, 35/06).

przetwarzanie danych osobowych. Pomimo wieloletniego obowiązywania ustawy o ochronie danych osobowych, wiele podmiotów – i to zarówno z sektora publicznego, jak i prywatnego, wykazuje niezrozumienie, a czasem wręcz lekceważenie dla zasad z niej wypływających. Na szczególną uwagę zasługuje zwłaszcza postawa instytucji publicznych (organów ścigania i wymiaru sprawiedliwości), zadaniem których jest zapewnienie poszanowania obowiązujących przepisów prawa, w tym przepisów karnych ustawy o ochronie danych osobowych. Tymczasem, zawiadomienia o popełnieniu przestępstwa przez podmioty uparczywie uchylające się od swoich obowiązków związanych ze sprawowaniem pieczy nad powierzonymi im danymi osobowymi, są najczęściej umarzane z powodu znikomej społecznej szkodliwości lub braku cech przestępstwa. Takie działania umacniają poczucie bezkarności w podmiotach naruszających prawo o ochronie danych.

Wysokim poziomem niewiedzy, co do zasad ochrony danych osobowych, wykazują się także osoby, których dane zostały naruszone. Większość osób nie uświadamia sobie, iż np. podpisanie zgody na przetwarzanie danych w celach marketingowych skutkować może udostępnieniem tych danych przez administratora innym podmiotom gospodarczym, a także – obrót tymi danymi w przestrzeni wirtualnej. Nieuczciwi przedsiębiorcy, którzy chcą uczynić z danych przedmiot handlu, często wymuszają oświadczenie zgody na dysponowanie danymi poprzez nie umieszczanie w deklaracji opcjonalności jej wyrażenia. Stąd tak bardzo istotne jest, aby jednostka przed podpisaniem dokumentu czy deklaracji, uważnie przeczytała formularz i zastanowiła się nad jego treścią. Ale możemy zaobserwować również sytuację odwrotną. A mianowicie nadgorliwość instytucji, które mając własne przepisy wystarczające do legalizacji procesu przetwarzania danych bez wymaganej zgody, dodatkowo pozyskują oświadczenia zgody na ich przetwarzanie.

Opisane powyżej przykłady zagrożeń bezpieczeństwa danych osobowych nie wynikają tylko z nieznamości przepisów o ochronie danych, bądź ich błędnej interpretacji. Na ten stan rzeczy składa się wiele przyczyn. Pokazują to wyniki badań sondażowych przeprowadzonych na zlecenie Generalnego Inspektora Ochrony Danych Osobowych przez TNS OBOP w roku 2007, dla których punktem odniesienia były wcześniejsze badania z roku 2004. Pokazały one, że choć wiedza obywateli na temat ustawy o ochronie danych osobowych utrzymuje się na tym samym poziomie, to jednak poziom ten jest w dalszym ciągu niski. Jedyna zauważalna zmiana, jaka dokonała się w ciągu ostatnich trzech lat, to odsetek osób, które zetknęły się z działaniami ustawy i kontakt ten zapamiętały – przekroczył on 50%. Najczęściej dotyczyło to sytuacji, w których obywatele zwracali się do różnych urzędów i instytucji z prośbą o udostępnienie im pewnych danych. W tym przypadku nieznacznie, ale

²⁸⁹ Uwagi do projektu ustawy o zmianie ustawy o czasie pracy kierowców oraz o zmianie niektórych innych ustaw (GI-DP-023/183/06) oraz do projektu ustawy o zmianie ustawy o funduszach inwestycyjnych (GI-DP-023/174-176/06).

jednak zwiększył się, odsetek osób, którym instytucja państwowa odmówiła udostępnienia danych z powołaniem się na przepisy ustawy o ochronie danych osobowych (w 2004 r. – 17%, w 2007 – 20%). Jedna piąta Polaków ma więc za sobą doświadczenie odmowy udzielenia im informacji przez zobowiązaną do tego instytucję publiczną – i to zarówno na skutek właściwego zastosowania, jak i nadużycia ustawy przez urząd, jak w przypadku odmowy udostępnienia przez operatorów sieci komórkowych służbom ratowniczym ustawowo powołanym do niesienia pomocy, dostępu do identyfikacji linii wywołującej oraz danych lokalizacyjnych abonentów wywołujących połączenia z numerami alarmowymi. Takie doświadczenie nasila się w miarę wzrostu wykształcenia u respondentów. Tak więc osoby z wyższym wykształceniem – wbrew potocznej opinii – nie radzą sobie w urzędach i instytucjach lepiej, niż pozostali.

W czasie, jaki upłynął od pierwszego badania w 2004 roku, nie nastąpiły istotne zmiany w poczuciu bezpieczeństwa danych osobowych. Tyle tylko, że poczucie bezpieczeństwa obywateli w odniesieniu do dotyczących ich danych osobowych zgromadzonych w bazach danych różnych urzędów, firm czy instytucji jest nadal **niskie**. W opinii przeszło połowy badanych (58%) dane chronione są źle. Na taki stan rzeczy wpływ mogło mieć kilka czynników:

- 1) negatywne doświadczenia własne respondentów lub ich znajomych;
- 2) szeroko nagłaśniane przez media informacje o naruszeniach bezpieczeństwa danych osobowych, np. „przecieki” z sądów lub Policji;
- 3) nieznajomość przepisów o ochronie danych osobowych;
- 4) ogólna nieufność obywateli wobec instytucji publicznych.

Szczególnie trzy pierwsze czynniki okazują się być istotne, ponieważ „ogólna nieufność obywateli wobec instytucji publicznych” (pkt 4) może powstać na skutek wystąpienia jednego, nałożenia się dwóch bądź wszystkich pozostałych ww. czynników. Ludzie z reguły boją się rzeczy, których nie znają i są skłonni surowiej je oceniać. Zwłaszcza jeśli oceniają przepisy prawa. Narzekanie i okazywanie niezadowolenia jest w badaniach nad percepcją przepisów prawa dość powszechną postawą u respondentów.

Jak wynika z badań TNS OBOP ogólna wiara w to, że instytucje dobrze chronią nasze dane osobowe jest jednak słaba – tylko 29 % badanych przyznało, że ich zdaniem dane są chronione dobrze. Wynik ten przekłada się na zróżnicowany stopień zaufania do najważniejszych instytucji, które gromadzą i przetwarzają dane osobowe, jak służba zdrowia, banki, Policja, urzędy skarbowe, władze lokalne czy pracodawcy. Do banków i służby zdrowia respondenci mają duże zaufanie (60%), do Policji i urzędów skarbowych średnio po 55%, natomiast władzom lokalnym i pracodawcom w zakresie przetwarzania danych osobowych ufa kolejno 44% i 39% badanych. Generalnie, w stosunku do każdej z wymienionych instytucji obywatele częściej deklarują zaufanie, niż jego brak. Tyle tylko, że ogólne poczucie braku bezpieczeństwa danych osobowych jest wśród obywateli polskich nadal

powszechnie wysokie (58%). Konsekwencją takiego stanu rzeczy jest niechęć społeczeństwa do jeszcze większego ograniczania przysługujących mu praw nawet z tytułu walki z poważnymi zagrożeniami, jak przestępczość zorganizowana czy międzynarodowy terrorizm.

Dla porównania warto przytoczyć wyniki badań Eurobarometru – badań zleconych przez Komisję Europejską w 2003 r. – w temacie dotyczącym ochrony danych osobowych w krajach Unii Europejskiej. Wyniki tych badań pokazują, że wiedza obywateli Unii o istnieniu niezależnego organu ds. ochrony danych osobowych, czy też prawa o ochronie danych osobowych jest niska. Około 68% badanych nie wiedziało o istnieniu takiego organu i taki sam procent badanych nie słyszało o istnieniu takiego prawa.²⁹⁰ Natomiast więcej niż 2/3 obywateli Unii (70% badanych) uważa, że poziom świadomości obywateli w zakresie ochrony danych osobowych w ich krajach jest niski.²⁹¹

Dotychczas najistotniejszym elementem sprawowania przez Generalnego Inspektora nadzoru nad wykonywaniem przepisów o ochronie danych osobowych było rozpatrywanie skarg oraz przeprowadzanie kontroli. Niemniej, w świetle sygnalizowanych w skargach i wnioskach pokontrolnych naruszeń przepisów ustawy o ochronie danych osobowych, środki te okazują się być niewystarczające. Waga ochrony danych osobowych wzrasta z rozwojem nowych technologii, handlu elektronicznego, postępującej informatyzacji instytucji prywatnych i publicznych. Zauważalna tendencja do poszerzania zakresu gromadzonych danych osobowych przez różne podmioty, łączenie baz danych, do których dostęp mają coraz liczniejsze grupy osób, itd. prowadzi do szeregu nadużyć, a w konsekwencji zagraża elementarnemu prawu jednostki, która oczekuje od Państwa ochrony swej prywatności i danych osobowych. Skuteczna realizacja tej ochrony jest możliwa tylko dzięki szerokiej współpracy różnych instytucji państwowych, większej staranności przy opracowywaniu nowych przepisów prawa, a także podwyższeniu poziomu świadomości prawnej społeczeństwa poprzez edukację – i to zarówno podmiotów przetwarzających dane, jak i osób fizycznych, których dane dotyczą.

Dla urzeczywistnienia prawa jednostki do poszanowania sfery jej prywatności w zakresie ochrony danych osobowych, konieczne staje się zatem wzmocnienie funkcji edukacyjnej organu ochrony danych osobowych. Temat ochrony danych osobowych nie jest bowiem powszechny w programach nauczania w szkołach średnich i wyższych. Stąd potrzeba wzmocnienia współpracy Generalnego Inspektora z instytucjami oświatowymi i środowiskami naukowymi. Ważne jest stworzenie systemu edukacji w zakresie tematyki związanej z danymi osobowymi, aby każdy z nas od najwcześniejszych lat nauki miał świadomość istnienia zagrożeń związanych z niezgodnym z prawem przetwarzaniem dotyczących nas danych osobowych i co do przysługujących nam praw. Dlatego też

²⁹⁰ Flash Eurobarometer 147, December 2003, s. 48-49.

²⁹¹ Ibidem, s.43.

Generalny Inspektor Ochrony Danych Osobowych w ramach polityki informacyjnej podejmuje szereg przedsięwzięć, by przeniknąć z informacją o prawach i obowiązkach wynikających z ustawy o ochronie danych osobowych do świadomości Polaków oraz polskich instytucji publicznych i prywatnych. Organizuje konferencje, szkolenia, warsztaty, wygłasza referaty w szkołach wyższych, udziela wywiadów, publikuje i odbywa dyżury telefoniczne. Jest też autorem koncepcji promowania prac magisterskich, doktorskich i innych opracowań o tematyce związanej z danymi osobowym. Stąd pilną staje się potrzeba stworzenia warunków przebywania ich autorów w Biurze i zapewnienia im możliwości pracy nad udostępnionymi materiałami. Dlatego też przed Generalnym Inspektorem staje kolejne zadanie – zorganizowania biblioteki i czyteln, gdzie swoje miejsce znalazłyby liczne materiały i publikacje polsko- i obcojęzyczne poświęcone problematyce danych osobowych, zgromadzone przez Generalnego Inspektora na przestrzeni prawie 10-letniej działalności organu. Przetłumaczone na język polski, stanowiąc będą cenne źródło wiedzy o danych osobowych dla szerokiego kręgu odbiorców (dziennikarzy, przedstawicieli świata nauki, studentów, a także pracowników Biura GIODO zainteresowanych poszerzaniem swej wiedzy z tego zakresu). Generalny Inspektor zamierza także cyklicznie wydawać biuletyn, na łamach którego swoje artykuły publikowałyby zarówno Generalny Inspektor i pracownicy Biura, jak i autorzy z zewnątrz. Dla pracowników naukowych zainteresowanych problematyką ochrony danych osobowych, takie wydawnictwo stanowiłoby pole do zamieszczania swoich specjalistycznych tekstów.

Działalność Generalnego Inspektora Ochrony Danych Osobowych na arenie międzynarodowej, pozwala na szerokie spojrzenie na problemy współczesnego, szybko rozwijającego się świata, stojącego wobec wyzwań nowych technologii. Wśród zadań dla krajowych organów Ochrony Danych na rok 2007, jakie dla przykładu wymienia Europejski Inspektor Ochrony Danych Osobowych, jest rozwiązanie problemu:

1. wykorzystania danych zebranych dla określonych celów (np. gospodarczych) do celów innych, np. związanych z przeciwdziałaniem i ściganiem przestępstw (np. dane imigracyjne, dane pasażerów linii lotniczych czy dane komunikacyjne);
2. z obszaru komunikacji elektronicznej (walka ze spamem i niechcianym oprogramowaniem);
3. zapewnienia bezpieczeństwa danych medycznych (systemy informacji medycznej, elektroniczne karty zdrowia, bezpieczeństwo produktów z tkanek ludzkich, itd.).

Pojawiają się także pytania o przyszłość Dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Regulacja przewidziana powyższą Dyrektywą miała służyć zabezpieczeniu jednolitego minimalnego poziomu ochrony prywatności osób fizycznych w związku z przetwarzaniem danych osobowych zawartych w zbiorach danych oraz

zapewnieniu możliwości swobodnego przepływu danych pomiędzy krajami członkowskimi. Tymczasem, wobec pojawiających się ww. nowych zagrożeń, również Dyrektywa 95/46/WE staje przed perspektywą zmian w jej zapisach.

Istotą propagowania idei ochrony danych osobowych ma być zapobieganie powstawaniu zagrożeń płynących z rozwoju nowych technologii. Rozwoju cywilizacji nie da się zahamować, ale poprzez wypracowanie pewnych standardów i mechanizmów kontroli nad tym procesem, można wyeliminować lub przynajmniej zminimalizować jego niepożądane skutki. Ważne jest, aby nowe technologie służyły, a nie szkodziły człowiekowi i społeczeństwu.

Na arenie międzynarodowej należy odnotować aktywny udział Generalnego Inspektora w procesie wdrażania dorobku prawnego Schengen. System Informacyjny Schengen ustanowiony został jako rekompensata zniesienia kontroli na granicach pomiędzy państwami obszaru Schengen. Gwarantuje on, że każde państwo będące stroną Konwencji Wykonawczej do Układu z Schengen [dalej: KWS] będzie posiadało zestaw informacji pozwalających na dostęp – przy użyciu zaawansowanych środków wyszukiwania – do wpisów dotyczących osób i ich majątku. Jest to istotne z punktu widzenia usprawnienia kontroli granicznej oraz innych rodzajów kontroli, np. policyjnej czy celnej prowadzonej w danym kraju oraz w celu wydawania wiz, dokumentów pobytowych i wykonywania przepisów prawa o cudzoziemcach. Włączenie do systemu Schengen jest bardzo ważne dla obywateli polskich ze względu na fakt, iż System ten wykorzystywany jest przede wszystkim do kontroli ruchu osobowego na granicach państw. Pozytywna ocena Polski, co do spełnienia wymagań unijnych pozwoli na przyłączenie jej do systemu Schengen, czego efektem będzie zniesienie kontroli wobec obywateli polskich na granicach wewnętrznych Unii Europejskiej.

O czym już była mowa wcześniej, grupa ekspertów z Unii Europejskiej odwiedziła nasz kraj, celem dokonania okresowej oceny wdrożenia dorobku prawnego Schengen w Polsce. Od opinii ekspertów zależeć będzie, czy wobec obywateli polskich zniesiona zostanie kontrola na granicach wewnętrznych Unii Europejskiej. Misja oceniająca zbadała m.in. prawne i faktyczne przygotowanie polskiego organu do spraw ochrony danych osobowych, jakim jest Generalny Inspektor Ochrony Danych Osobowych, do wypełniania funkcji organu nadzorczego, odpowiedzialnego – zgodnie z prawem krajowym - za przeprowadzanie niezależnego nadzoru nad danymi krajowego modułu Systemu Informacyjnego Schengen oraz kontrolę procesu przetwarzania i wykorzystywania danych wprowadzonych do tego systemu.

Misje oceniające organizowane są co 5 lat. Obejmują one zarówno państwa uczestniczące we współpracy Schengen, jak i państwa zamierzające nawiązać taką współpracę. Szczególne znaczenie mają misje oceniające tę drugą grupę państw, gdyż pozytywne przejście ewaluacji jest warunkiem przyłączenia tych państw do Systemu Informatycznego Schengen.

Wyniki misji oceniającej, były – co prawda – pozytywne dla naszego kraju, ale przed Generalnym Inspektorem postawionych zostało szereg ważnych zadań i kwestii do rozwiązania, jak: większy udział w pracach zespołów roboczych pracujących nad wdrożeniem przepisów układu Schengen, przeprowadzenie akcji informacyjnych na ten temat oraz zwiększenie liczby kontroli i to nie tylko w kraju, ale także poza jego granicami - w wybranych konsulatach RP znajdujących się w państwach spoza Unii Europejskiej. Eksperci podkreślili także, że Generalny Inspektor Ochrony Danych Osobowych, jako organ mający sprawować kontrolę nad przetwarzaniem danych w krajowym komponencie Systemu Informacyjnego Schengen, musi posiadać szerokie kompetencje w tym zakresie gwarantowane przepisami polskiego prawa, jak również zapewnione środki finansowe umożliwiające pełną realizację nowych obowiązków związanych z wdrażaniem dorobku prawnego Schengen.

W celu sprawnego wykonywania dotychczasowych zadań i przygotowywania się do nowych, Generalny Inspektor już poczynił istotne działania, aby wymienione powyżej zamierzenia mogły być sprawnie realizowane. Mianowicie, zmienił strukturę organizacyjną Biura. W omawianym okresie sprawozdawczym weszło w życie nowe rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 203, poz. 1494). Statut stanowiący załącznik do niniejszego rozporządzenia wprowadził zmiany w strukturze organizacyjnej Biura. Departament Prawny został połączony z Departamentem Skarg w nowy departament o nazwie Departament Orzecznictwa, Legislacji i Skarg, który przejął zadania zlikwidowanych departamentów, a z Departamentu Prawnego wyodrębniony został Departament Edukacji Społecznej i Współpracy Międzynarodowej.

Realizacja wszystkich wymienionych powyżej zamierzeń Generalnego Inspektora, zarówno z dziedziny edukacji społecznej, planowanego zwiększenia liczby kontroli, zwłaszcza sektorowych i tych przeprowadzanych poza Warszawą oraz związanych z wdrażaniem dorobku Schengen, a także dla sprawniejszego, niezakłóconego wypełniania obecnych zadań, koniecznością jest nowelizacja ustawy o ochronie danych osobowych, zwiększenie liczby etatów w Biurze i zapewnienia odpowiednich funduszy umożliwiających ich pełną realizację. Stąd postulat odpowiedniego zwiększenia budżetu Biura Generalnego Inspektora Ochrony Danych Osobowych na rok 2007.

ZAŁĄCZNIKI:

Załącznik nr 1 Wykaz wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2006 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego.

l.p.	Podmiot, do którego wystąpienie było skierowane	Data i sygnatura sprawy	Przedmiot
1.	Rzecznik Praw Obywatelskich	06.01.2006 r. GGI-024-1/06/11	Wystąpienie w sprawie oceny legalności powierzania przez jednostki samorządu terytorialnego, podmiotom prywatnym, w drodze umowy, uprawnień do wykonywania czynności z zakresu kontroli ruchu drogowego oraz czynności mających na celu sporządzenie dokumentacji związanej z nakładaniem grzywien w drodze mandatu karnego, na kierowców popełniających wykroczenia drogowe polegające na przekroczeniu dozwolonej prędkości.
2.	Komendant Główny Policji	06.01.2006 r. GGI-024-1/06/12	Wystąpienie w sprawie legalności wykonywania czynności kontroli ruchu drogowego przez podmioty prywatne.
3.	Komendant Główny Państwowej Straży Pożarnej	27.01.2006 r. DRZDO-400/4/06	Wystąpienie w sprawie podjęcia działań mających na celu dopełnienie obowiązku zgłoszenia do rejestracji zbiorów danych osobowych prowadzonych przez jednostki organizacyjne Państwowej Straży Pożarnej w związku z wykonywaniem przez nie ustawowych zadań.
4.	Minister Spraw Wewnętrznych i Administracji	03.02.2006 r. GI-DP-024/264/06	Wystąpienie w sprawie zapewnienia udziału Generalnego Inspektora Ochrony Danych Osobowych w pracach nad projektem ustawy wprowadzającej do polskiego prawa przepisy pozwalające na realizację postanowień Konwencji Wykonawczej Schengen oraz przepisy pozwalające na współpracę z Systemem Informacji Wizowej.
5.	Przewodniczący Sejmowej Komisji Administracji i Spraw Wewnętrznych	22.03.2006 r. DRZDO-400/7/06	Wystąpienie w sprawie nieprawidłowości w działaniach strażników straży gminnych przy wykonywaniu czynności z zakresu kontroli ruchu drogowego.
6.	Przewodniczący Sejmowej Komisji Sprawiedliwości i Praw Człowieka	22.03.2006 r. DRZDO-400/8/06	Wystąpienie w sprawie nieprawidłowości w działaniach strażników straży gminnych przy wykonywaniu czynności z zakresu kontroli ruchu drogowego.
7.	Minister Sprawiedliwości	05.04.2006 r. GI-DP-024/481/06	Wystąpienie w sprawie udzielania przez sądy informacji o treści zapadłych wyroków drogą telefoniczną.
8.	Minister Finansów	05.04.2006 r. GI-DP-024/513/06	Wystąpienie w sprawie nakładania przez dyrektorów Izb Skarbowych obowiązku składania przez pracowników Izb Skarbowych oświadczenia o działalności gospodarczej prowadzonej przez ich małżonków i członków rodzin.
9.	Generalny Inspektor Nadzoru Bankowego	10.04.2006 r. GI-DS-430/370/04	Wystąpienie o podjęcie działań mających na celu skorelowanie systemów informatycznych banków oraz systemu informatycznego Biura Informacji Kredytowej S.A. i wyeliminowanie opóźnień w aktualizowaniu danych przekazywanych przez banki do bazy „Kredytobiorcy” prowadzonej przez BIK S.A.
10.	Minister Skarbu Państwa	15.05.2006 r. GI-DS-430/837/05	Wystąpienie o podjęcie działań mających na celu zapewnienie przestrzegania przez prywatyzowane spółki ustawy o ochronie danych osobowych w sytuacji ich przetwarzania na liście pracowników uprawnionych do nieodpłatnego nabycia akcji w zakresie szerszym niż to wynika z przepisów prawa
11.	Prezes Zakładu Ubezpieczeń Społecznych	23.06.2006 r. GI-DP-024/1148/06 GI-DP-024/1169/06	Wystąpienie w sprawie celowości i zasadności umieszczania na nalepkach adresowych kierowanej przez terenowe jednostki organizacyjne ZUS do emerytów/rencistów korespondencji, oprócz ich danych adresowych, dodatkowo oznaczenia wskazującego symbol i numer pobieranego świadczenia (emerytury/renty).

12.	Prezes Urzędu Ochrony Konkurencji i Konsumentów	30.06.2006 r. GI-DP-024/984/06	Wystąpienie w sprawie rozważenia podjęcia działań przewidzianych w ustawie z dnia 15 grudnia 2000 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz. U. z 2005 r. Nr 244, poz. 2080 ze zm.) w celu zbadania, czy pobieranie przez Biuro Obsługi Klienta BIK S.A. opłat za przysyłanie listem poleconym informacji w formie raportów konsumenckich osobom zwracającym się o te informacje nie stanowi naruszenia zbiorowych praw konsumentów.
13.	Przewodniczący Sejmowej Komisji Samorządu Terytorialnego i Polityki Regionalnej	21.07.2006 r. GI-DP-024/928/06	Wystąpienie w sprawie podjęcia inicjatywy legislacyjnej mającej na celu uregulowanie w przepisach prawa uprawnień komisji rewizyjnej w związku z dokonywaniem przez nią czynności kontrolnych, w których to przepisach będzie wyraźnie określone jej prawo dostępu do związanej z przedmiotem kontroli dokumentacji osób fizycznych.
14.	Minister Nauki i Szkolnictwa Wyższego	17.08.2006 r. GI-DRZDO-400/19/06	Wystąpienie w sprawie podjęcia działań mających na celu dopełnienie obowiązku zgłoszenia do rejestracji, prowadzonych przez uczelnie wyższe, zbiorów danych osobowych kandydatów na studia.
15.	Minister Spraw Wewnętrznych i Administracji	05.09.2006 r. DRZDO-400-20/06	Wystąpienie w sprawie zakresu danych osobowych gromadzonych w zbiorach meldunkowych prowadzonych przez gminy i wojewodów.
16.	Minister Sprawiedliwości	25.10.2006 r. GI-DP-023/205/06	Wystąpienie w sprawie braku konieczności określania w projekcie ustawy o dostępie do nieodpłatnej pomocy prawnej dodatkowych standardów ochrony danych osobowych osób, które są klientami punktów pomocy prawnej.
17.	Główny Geodeta Kraju, Minister Budownictwa	31.10.2006 r. GI-DP-024/1037/06	Wystąpienie w sprawie legalności przetwarzania danych w ramach Integrującej Platformy Elektronicznej.
18.	Minister Spraw Wewnętrznych i Administracji	14.11.2006 r. GI-DP-024/1677/06	Wystąpienie w sprawie usunięcia nieprawidłowości legislacyjnych w art. 34 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. Nr 74, poz. 676 ze zm.), który odwoływał się do treści nieobowiązujących już przepisów ustawy o ochronie danych osobowych.

Załącznik nr 2 Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2006 do podmiotów prywatnych.

I.p.	Podmiot, do którego wystąpienie było skierowane	Data i sygnatura sprawy	Przedmiot
1.	Prezes Zarządu Canal+ Cyfrowy Sp. z o.o.	03.02.2006 r. GI-DS-430/527/05	Wystąpienie o zmianę stosowanej przez Spółkę praktyki umieszczania w proponowanych klientom drukach „polecenie zapłaty” danych o rachunkach bankowych pozyskiwanych nie bezpośrednio od abonentów.
2.	Prezes Zarządu Banku Millenium S.A.	01.03.2006 r. GI-DS-430/789/05	Wystąpienie w sprawie zaprzestania stosowania przez bank praktyki przetwarzania danych osobowych byłych klientów w celach związanych z marketingiem własnych produktów i usług.
3.	Prezes Zarządu Wólczanki S.A.	31.03.2006 r. GI-DS-430/847/05	Wystąpienie o zmianę treści stosowanych przez spółkę kuponów konkursowych, z których spółka pozyskuje dane osobowe, celem umożliwienia uczestnikom konkursu prowadzonego przez spółkę wyrażenia odrębnej zgody na udostępnienie danych osobowych innym podmiotom oraz na wykorzystywanie danych osobowych w celach marketingowych innych podmiotów.
4.	Prezes Zarządu Spółdzielni Mieszkaniowej „Kaszuby”	06.04.2006 r. GI-DP-024/475/06	Wystąpienie w sprawie zamieszczania na tablicach ogłoszeń na klatkach schodowych podziękowań dla członków spółdzielni terminowo regulujących należne opłaty wraz z wyszczególnieniem numerów ich mieszkań.
5.	Właściciel Apteki Avena	19.04.2006 r. GI-DP-024/635/06	Wystąpienie w sprawie niedopełniania przez aptekę Avena obowiązku informacyjnego, o którym mowa w art. 24 ustawy o ochronie danych osobowych, wobec osób, których dane apteka gromadzi w związku z organizowanym konkursem.

6.	Prezes Zarządu Wspólnoty Mieszkaniowej nieruchomości warszawskiej przy ul. Grochowskiej 237 i Prezes Zarządu Biura Administracji Nieruchomości „POSIADŁOŚĆ” Sp. z o.o.	17.05.2006 r. GI-DS-430/823/05	Wystąpienie o niezwłoczne podjęcie czynności mających na celu powstrzymanie się w przyszłości od działań polegających na udostępnieniu w miejscu powszechnie dostępnym pisma kierowanego do prokuratury rejonowej, stanowiącego zawiadomienie o podejrzeniu popełnienia przestępstwa i zawierającego w swej treści dane osobowe członków wspólnoty mieszkaniowej.
7.	Prezes Zarządu Learning System Polska	31.05.2006 r. GI-DP-024/634/06	Wystąpienie w sprawie dostosowania procesu przetwarzania danych osobowych gromadzonych za pomocą formularza umieszczonego na stronie internetowej www.orangeschool.pl/kontakt.php do wymogów ustawy o ochronie danych osobowych.
8.	Prezes Zarządu Commercial Union Polska – Towarzystwo Ubezpieczeń na Życie S.A.	31.05.2006 r. GI-DS-430/155/06	Wystąpienie o częściową zmianę formularza pt. ”Deklaracja uczestnictwa i zmian w Grupowym Ubezpieczeniu na Życie z Ubezpieczeniowym Funduszem Kapitałowym ZESPÓŁ” w zakresie klauzul odnoszących się do przetwarzania danych osobowych Uczestników, pozyskiwanych przez Towarzystwo.
9.	Dom Ferie Pośrednictwo Wynajmu	01.06.2006 r. GI-DP-024/1014/06	Wystąpienie w sprawie dostosowania procesu przetwarzania danych osobowych gromadzonych za pomocą formularza umieszczonego na stronie internetowej www.domferie.com.pl do zasad określonych w przepisach o ochronie danych osobowych.
10.	Prezes Zarządu Grupy Żywiec S.A.	20.06.2006 r. GI-DP-024/1048/06	Wystąpienie w sprawie dostosowania procesu przetwarzania danych osobowych gromadzonych za pomocą programów stażowych przez Dział Personalny Grupy Żywiec S.A. do wymogów ustawy o ochronie danych osobowych.
11.	Prezes Zarządu Canal + Cyfrowy Sp. z o.o.	23.06.2006 r. GI-DP-024/1107/06	Wystąpienie w sprawie uzależniania uczestnictwa w programie o nazwie Złoty Plus od wyrażenia zgody na przetwarzanie danych przez operatora Cyfry + w celach marketingowych innych podmiotów.
12.	Prezes Fundacji Wielka Orkiestra Świątecznej Pomocy	27.06.2006 r. GI-DP-024/1213/06	Wystąpienie w sprawie naruszania przez Fundację zasad ochrony danych osobowych przy gromadzeniu danych przez formularz zgłoszeniowy do Programu „Ratujemy i uczymy ratować”.
13.	Prezes Zarządu Banku Millenium S.A.	28.06.2006 r. GI-DS-430/29/06	Wystąpienie o zapewnienie respektowania przez bank oświadczeń dotyczących dopuszczalności przekazywania bankom informacji o produktach i usługach banku drogą telefoniczną odbieranych przez bank od klientów.
14.	Pełnomocnik Skarbnicy Narodowej Sp. z o.o.	10.07.2006 r. GI-DS-430/250/06	Wystąpienie o zapewnienie opcjonalności klauzuli zgody osób dokonujących zamówienia produktów Spółki na przetwarzanie ich danych, pozyskiwanych za pomocą karty rezerwacyjnej, w celach marketingowych oraz na ewentualne udostępnianie przedmiotowych danych innym podmiotom, a także o wypełnienie wobec klientów Spółki obowiązku informacyjnego określonego w art. 24 ust. 1 pkt 1 ustawy o ochronie danych osobowych.
15.	Prezes Zarządu Żabka Polska S.A.	12.07.2006 r. GI-DS-430/170/06	Wystąpienie o wypełnienie wobec klientów spółki obowiązku informacyjnego określonego w art. 24 ust. 1 pkt 3 i 4 ustawy o ochronie danych osobowych poprzez poinformowanie o prawie dostępu do treści danych, prawie ich poprawiania oraz dobrowolności podania danych.
16.	Prezes Zarządu Grupy Żywiec S.A.	24.07.2006 r. GI-DP-024/1300/06	Wystąpienie w sprawie dostosowania procesu przetwarzania danych osobowych gromadzonych za pomocą formularza rejestracyjnego dostępnego na stronie internetowej www.heinekenmusic.pl do wymogów ustawy o ochronie danych osobowych.
17.	Prezes Zarządu BRE Banku S.A.	11.10.2006 r. GI-DS-430/129/06	Wystąpienie o stosowanie formuły zgody umieszczonej na stronie internetowej mBanku do wymogów ustawy o ochronie danych osobowych, w sytuacji, gdy przekazywanie danych nie dotyczyło odbiorcy danych, ale podmiotu, którym był przedstawiciel mBanku.
18.	Dariusz Tauchert Firma Handlowa Tadar	19.10.2006 r. GI-DP-024/1744/06	Wystąpienie w sprawie wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych gromadzonych za pomocą formularza rejestracyjnego umieszczonego na stronie internetowej

			www.tadar.com.pl.
19.	Prezes Zarządu Beverly Hills Video S.A.	07.11.2006 r. GI-DS- 430/451/06	Wystąpienie o zapewnienie opcjonalności klauzuli zgody osób korzystających z usług Spółki na przetwarzanie ich danych, pozyskiwanych za pomocą deklaracji członkowskiej, w celach marketingowych oraz na ewentualne udostępnianie przedmiotowych danych innym podmiotom, a także o wypełnienie wobec klientów Spółki obowiązku informacyjnego określonego w art. 24 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Załącznik nr 3 Wykaz kontroli przeprowadzonych w 2006 roku

l.p.	Data i sygnatura kontroli	Podmiot kontrolowany i miejsce kontroli	Inicjatywa kontroli	Rozstrzygnięcie oraz/lub data i sygnatura decyzji.
1.	09-11.01.2006 GI-DIS-K- 411/1/06	Pierwszy Urząd Skarbowy Warszawa Śródmieście, Warszawa, ul. Lindleya 14	Departament Skarg	wnioski przekazano do Departamentu Skarg
2.	09-13.01.2006 GI-DIS-K- 411/2/06	Komendant Straży Miejskiej Miasta Stołecznego Warszawy, Warszawa, ul. Czerniakowska 130/132	z urzędu	02.06.2006, decyzja GI-DEC-DIS-181/06
3.	17-18.01.2006 GI-DIS-K- 411/3/06	Marcin Wolniewicz prowadzący działalność gospodarczą pod nazwą „Londoner”, Warszawa, ul. Kopernika 30/209	Departament Prawny	19.06.2006, decyzja GI-DEC-DIS-196/06
4.	23-27.01.2006 GI-DIS-K- 411/4/06	Metro Warszawskie Sp. z o.o., Warszawa, ul. Wilczy Dół 5	Departament Prawny	02.06.2006, decyzja GI-DEC-DIS-180/06
5.	23-27.01.2006 GI-DIS-K- 411/5/06	Trader.com (Polska) Sp. z o.o., Warszawa, ul. Towarowa 22	Departament Skarg	06.10.2006, decyzja GI-DEC-DIS-386/06
6.	23-26.01.2006 GI-DIS-K- 411/6/06	Telekomunikacja Polska S.A. Warszawa, ul. Twarda 18	Departament Skarg	wnioski przekazano do Departamentu Skarg
7.	06-09.02.2006 GI-DIS-K- 411/7/06	Cegedim Poland Sp. z o.o., Warszawa, ul. Pileckiego 63	z urzędu	08.06.2006, decyzja GI-DEC-DIS-186/06
8.	06-07.02.2006 GI-DIS-K- 411/8/06	Mineral Midrange Sp. z o.o., Warszawa, ul. Jana III Sobieskiego 110	Departament Prawny	19.05.2006, decyzja GI-DEC-DIS-165/06
9.	06-09.02.2006 GI-DIS-K- 411/9/06	Masterlink Express Sp. z o.o., Warszawa, ul. Mineralna 15	Departament Skarg	12.07.2006, decyzja GI-DEC-DIS-256/06
10.	20-23.02.2006 GI-DIS-K- 411/10/06	Lukas Bank S.A., Wrocław, Pl. Orłąt Lwowskich 1	Departament Skarg	07.07.2006, decyzja GI-DEC-DIS-250/06
11.	20-24.02.2006 GI-DIS-K- 411/11/06	Polski Związek Piłki Nożnej, Warszawa, ul. Miodowa 1	z urzędu	15.09.2006, decyzja GI-DEC-DIS-359/06
12.	20-24.02.2006 GI-DIS-K- 411/12/06	Uniwersytet Rzeszowski, Rzeszów, Al. Rejtana 16C	Prokuratura Rejonowa w Rzeszowie	25.08.2006, decyzja GI-DEC-DIS-323/06
13.	27.02-03.03.2006 GI-DIS-K- 411/13/06	GE Money Bank S.A., Gdańsk, ul. Elżbietańska 2	Departament Skarg	26.07.2006, decyzja GI-DEC-DIS-277/06,
14.	06-08.03.2006 GI-DIS-K- 411/14/06	Roman Raczyński prowadzący działalność gospodarczą pod nazwą „Ośrodek Pomocy Profesjonalnej Biuro Elite”,	Departament Prawny	23.06.2006, decyzja GI-DEC-DIS-208/06

		Bielsko – Biała, ul. Piłsudskiego 7		
15.	13-14.03.2006 GI-DIS-K- 411/15/06	Magda Grzesiak prowadząca działalność gospodarczą pod nazwą „Ogólnopolski Ośrodek Wychodzenia z Samotności Czandra”, Warszawa, ul. Żurawia 2/43	Departament Prawny	23.06.2006, decyzja GI-DEC-DIS-207/06
16.	06-10.03.2006 GI-DIS-K- 411/16/06	Europejska Szkoła Kształcenia Korespondencyjnego Sp. z o.o., Poznań, ul. Forteczna 17a	Departament Prawny	25.07.2006, decyzja GI-DEC-DIS-276/06
17.	13-15.03.2006 GI-DIS-K- 411/17/06	Państwowy Powiatowy Inspektor Sanitarny w Szydłowie – Powiatowa Stacja Sanitarno – Epidemiologiczna w Szydłowie, Szydłowiec, ul. Metalowa 7	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
18.	20-22.03.2006 GI-DIS-K- 411/18/06	Apollo Sp. z o.o., Kraków, ul. Budryka 7	Departament Prawny	23.06.2006, decyzja GI-DEC-DIS-206/06
19.	20-24.03.2006 GI-DIS-K- 411/19/06	Centralna Wojskowa Przychodnia Lekarska „CePeLek” Samodzielny Publiczny Zakład Opieki Zdrowotnej, Warszawa, ul. Koszykowa 78	Departament Skarg	12.07.2006, decyzja GI-DEC-DIS-254/06
20.	28-29.03.2006 GI-DIS-K- 411/20/06	Project Support Sp. z o.o., Warszawa, ul. Poleczki 21	Departament Rejestracji Zbiorów Danych Osobowych	11.05.2006, decyzja GI-DEC-DIS-153/06
21.	10-11.04.2006 GI-DIS-K- 411/21/06	e-Bay Sp. z o.o., Warszawa, Al. Jerozolimskie 148	Departament Prawny	nie stwierdzono uchybień
22.	10-12.04.2006 GI-DIS-K- 411/22/06	Forin Sp. z o.o., Warszawa, Al. Jerozolimskie 133A	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
23.	10-11.04.2006 GI-DIS-K- 411/23/06	Biuro Usług Specjalistycznych „Rokada” Sp. z o.o., Warszawa, ul. Ciołka 13	Departament Rejestracji Zbiorów Danych Osobowych	27.11.2006, decyzja GI-DEC-DIS-435/06
24.	24-28.04.2006 GI-DIS-K- 411/24/06	Websky Sp. z o.o., Białystok, ul. Legionowa 28 lok. 1001	Departament Prawny	13.09.2006, decyzja GI-DEC-DIS-354/06
25.	19-22.04.2006 GI-DIS-K- 411/25/06	Konsul Generalny RP we Lwowie – Konsulat Generalny we Lwowie, Lwów, ul. Iwana Franki 110	z urzędu	pismo z informacją o stwierdzonych uchybieniach
26.	19-20.04.2006 GI-DIS-K- 411/26/06	Prominent – Antoni Michał Minchberg Sp. k., Warszawa, ul. H. Junkiewicz 2B lok. 5	Departament Rejestracji Zbiorów Danych Osobowych	26.07.2006, decyzja GI-DEC-DIS-278/06
27.	22-31.05.2006 GI-DIS-K- 411/27/06	Polska Telefonii Cyfrowa Sp. z o.o., Warszawa, Al. Jerozolimskie 181	z urzędu	nie stwierdzono uchybień
28.	24-28.04.2006 GI-DIS-K- 411/28/06	General Logistics Systems Poland Sp. z o.o., Gądk, ul. Poznańska 71	Departament Skarg	21.09.2006, decyzja GI-DEC-DIS-362/06
29.	24-28.04.2006	Centralny Ośrodek Sportu	Prokuratura	31.07.2006, decyzja GI-DEC-DIS-282/06

	GI-DIS-K-411/29/06	w Warszawie – Ośrodek Przygotowań Olimpijskich, Zakopane, ul. Bronisława Czecha 1	Okręgowa w Nowym Sączu	
30.	10-12.05.2006 GI-DIS-K-411/30/06	Bank Millennium S.A., Warszawa, Al. Jerozolimskie 123A	z urzędu	nie stwierdzono uchybień
31.	15-17.05.2006 GI-DIS-K-411/31/06	Witold Jędraszewski prowadzący działalność gospodarczą pod nazwą „Centrum – Biuro Obrotu Nieruchomościami”, Warszawa, ul. Pańska 61	Departament Skarg	wnioski przekazano do Departamentu Skarg
32.	16.05.2006 GI-DIS-K-411/32/06	Sitel Polska Sp. z o.o., Warszawa, ul. Domaniewska 41	z urzędu	26.07.2006, decyzja GI-DEC-DIS-279/06
33.	22-25.05.2006 GI-DIS-K-411/33/06	Auchan Polska Sp. z o.o. – Hipermarket Auchan Gdańsk, ul. Szczęśliwa 3	z urzędu	30.03.2007, decyzja GI-DEC-DIS-13/07
34.	28.05-02.06.2006 GI-DIS-K-411/34/06	Wydział Konsularny Ambasady RP w Federacji Rosyjskiej, Moskwa, ul. Klimaszkińska 4	z urzędu	pismo z informacją o stwierdzonych uchybieniach
35.	31.05.2006 GI-DIS-K-411/36/06	Wspólnota Mieszkaniowa Zielone Zacisze II, Warszawa, ul. Św. Wincentego 112	Departament Skarg	wnioski przekazano do Departamentu Skarg
36.	01-02.06.2006 GI-DIS-K-411/37/06	Prezes Głównego Urzędu Statystycznego – Centralny Ośrodek Informatyki Statystycznej, Warszawa, Al. Niepodległości 208	z urzędu	zaplanowana kontrola kompleksowa
37.	05-09.06.2006 GI-DIS-K-411/38/06	IT Polpager S.A., Warszawa, ul. Pawia 55	Departament Rejestracji Zbiorów Danych Osobowych	06.03.2007, decyzja GI-DEC-DIS-10/07
38.	05-09.06.2006 GI-DIS-K-411/39/06	Niepubliczny Zakład Opieki Zdrowotnej „Medmax”, Andrespol, ul. Rokicińska 125	Departament Skarg	08.02.2007, wystąpienie do Ministra Zdrowia
39.	19-21.06.2006 GI-DIS-K-411/40/06	GE Money Bank S.A. – Departament Zarządzania Siecią Agentów „Chrobry”, Gniezno, ul. Żwirki i Wigury 7	z urzędu	26.07.2006, decyzja GI-DEC-DIS-277/06
40.	26-30.06.2006 GI-DIS-K-411/41/06	PZU Życie S.A., Warszawa, Al. Jana Pawła II 24	z urzędu	nie stwierdzono uchybień
41.	26-30.06.2006 GI-DIS-K-411/42/06	Signal Iduna Polska Towarzystwo Ubezpieczeń S.A., Warszawa, ul. Jasna 14/16A	z urzędu	08.05.2007, decyzja GI-DEC-DIS-15/07
42.	26-30.06.2006 GI-DIS-K-411/43/06	Towarzystwo Ubezpieczeń i Reasekuracji Cigna Stu S.A., Warszawa, ul. Noakowskiego 22	z urzędu	24.10.2006, decyzja GI-DEC-DIS-403/06
43.	26-29.06.2006 GI-DIS-K-411/44/06	Gerling Polska Towarzystwo Ubezpieczeń na Życie S.A., Warszawa, ul. Hrubieszowska 2	z urzędu	25.10.2006, decyzja GI-DEC-DIS-406/06
44.	10-14.07.2006 GI-DIS-K-	Kujawsko – Pomorski Oddział Regionalny Agencji	Prokuratura Rejonowa Toruń	nie stwierdzono uchybień

	411/45/06	Restrukturyzacji i Modernizacji Rolnictwa, Toruń, ul. Dąbrowskiego 4	Centrum - Zachód	
45.	10-12.07.2006 GI-DIS-K-411/46/06	Telekomunikacja Polska S.A., Warszawa, ul. Twarda 18	Departament Prawny	wnioski przekazano do Departamentu Prawnego
46.	24-27.07.2006 GI-DIS-K-411/47/06	Ośrodek Rehabilitacyjno – Edukacyjny dla Dzieci i Młodzieży Niepełnosprawnej, Rusinowice, ul. Zielona 23	Departament Skarg	nie stwierdzono uchybień
47.	24-29.07.2006 GI-DIS-K-411/48/06	Samodzielny Publiczny Zakład Opieki Zdrowotnej – Zespół Ośrodków Zdrowia Gminy Szczecinek, Szczecinek, ul. Piłska 3	Departament Skarg	08.11.2006, decyzja GI-DEC-DIS-418/06
48.	24-29.07.2006 GI-DIS-K-411/49/06	Samodzielny Publiczny Zakład Opieki Zdrowotnej – Zespół Ośrodków Zdrowia Gminy Szczecinek – Ośrodek Zdrowia w Wierzchowie 65	Departament Skarg	08.11.2006, decyzja GI-DEC-DIS-418/06
49.	24-28.07.2006 GI-DIS-K-411/50/06	Home.pl Sp. j., Szczecin, Pl. Rodła 9	Departament Skarg	22.11.2006, decyzja GI-DEC-DIS-427/06
50.	26-28.07.2006 GI-DIS-K-411/51/06	Związek Kynologiczny w Polsce, Warszawa, ul. Nowy Świat 35	Departament Skarg	24.05.2007, decyzja GI-DEC-DIS-18/07
51.	02-04.08.2006 07-08.08.2006 GI-DIS-K-411/52/06	EMPiK Sp. z o.o., Warszawa, ul. Marszałkowska 116/122	Departament Skarg	14.05.2007, decyzja GI-DEC-DIS-16/07
52.	07-11.08.2006 GI-DIS-K-411/53/06	Zakład Ubezpieczeń Społecznych Oddział w Kielcach, Kielce, ul. Piotrkowska 27	z urzędu	wszczęto postępowanie administracyjne
53.	07-11.08.2006 GI-DIS-K-411/54/06	Zakład Ubezpieczeń Społecznych Oddział w Częstochowie, Częstochowa, ul. Dąbrowskiego 43/45	z urzędu	wszczęto postępowanie administracyjne
54.	07-28.08.2006 GI-DIS-K-411/55/06	Zakład Ubezpieczeń Społecznych, Warszawa, ul. Czerniakowska 16	Departament Skarg	wszczęto postępowanie administracyjne
55.	21-25.08.2006 GI-DIS-K-411/56/06	Zakład Ubezpieczeń Społecznych Oddział w Olsztynie, Olsztyn, Pl. Konsulatu Polskiego 4	z urzędu	wszczęto postępowanie administracyjne
56.	21-25.08.2006 GI-DIS-K-411/57/06	Zakład Ubezpieczeń Społecznych Oddział w Lublinie, Lublin, ul. T. Zana 36-38C	z urzędu	wszczęto postępowanie administracyjne
57.	21-25.08.2006 GI-DIS-K-411/58/06	Bank BPH S.A., Kraków, Al. Pokoju 1	Departament Skarg	usunięto uchybienia
58.	28.08.2006 GI-DIS-K-411/59/06	Sebastian Surzyn prowadzący działalność gospodarczą pod nazwą „Luna”, Warszawa, ul. Targowa 11/13	Departament Skarg	27.11.2006, decyzja GI-DEC-DIS-434/06
59.	04-08.09.2006 GI-DIS-K-411/60/06	Komenda Główna Straży Granicznej – Morski Oddział Straży Granicznej, Gdańsk, ul. Oliwska 35	z urzędu	nie stwierdzono uchybień

60.	06-08.09.2006 GI-DIS-K- 411/61/06	EuroCross International Polska Sp. z o.o., Warszawa, ul. Hrubieszowska 2	z urzędu	usunięto uchybienia
61.	11-15.09.2006 GI-DIS-K- 411/62/06	Komenda Główna Straży Granicznej – Karpacki Oddział Straży Granicznej – Lotnicze Przejście Graniczne w Krakowie Balicach	z urzędu	nie stwierdzono uchybień
62.	11-15.09.2006 GI-DIS-K- 411/63/06	Komenda Główna Straży Granicznej – Warmińsko – Mazurski Oddział Straży Granicznej – Placówka Straży Granicznej w Gołdapi	z urzędu	nie stwierdzono uchybień
63.	18-22.09.2006 GI-DIS-K- 411/64/06	Komenda Główna Straży Granicznej – Podlaski Oddział Straży Granicznej – Placówka Straży Granicznej w Bobrownikach	z urzędu	nie stwierdzono uchybień
64.	18-22.09.2006 GI-DIS-K- 411/65/06	Komenda Główna Straży Granicznej – Podlaski Oddział Straży Granicznej – Placówka Straży Granicznej w Budzisku	z urzędu	nie stwierdzono uchybień
65.	19-22.09.2006 GI-DIS-K- 411/66/06	Ministerstwo Finansów, Warszawa, ul. Świętokrzyska 12	z urzędu	nie stwierdzono uchybień
66.	25-29.09.2006 GI-DIS-K- 411/67/06	Komenda Główna Straży Granicznej – Nadbużański Oddział Straży Granicznej – Placówka Straży Granicznej w Dorohusku	z urzędu	nie stwierdzono uchybień
67.	25-27.09.2006 GI-DIS-K- 411/68/06	Guard Systems Polska S.A., Warszawa, ul. Modlińska 223A	Departament Skarg	nie stwierdzono uchybień
68.	02-05.10.2006 GI-DIS-K- 411/69/06	Związek Kynologiczny w Polsce Oddział w Warszawie, ul. Lubelska 5/7	z urzędu	wnioski wykorzystano w postępowaniu prowadzonym po kontroli GI-DIS-K- 411/51/06
69.	09-13.10.2006 GI-DIS-K- 411/70/06	Zakład Ubezpieczeń Społecznych Oddział w Gdańsku, Gdańsk, ul. Chmielna 27/33	z urzędu	wszczęto postępowanie administracyjne
70.	09-13.10.2006 GI-DIS-K- 411/71/06	Zakład Ubezpieczeń Społecznych Oddział we Wrocławiu, Wrocław, ul. Pretficza 11	z urzędu	wszczęto postępowanie administracyjne
71.	09-13.10.2006 18.10.2006 GI- DIS-K-411/72/06	Mędzyresortowe Centrum ds. Zwalczania Przestępczości Zorganizowanej i Międzynarodowego Terroryzmu, Warszawa, ul. Batorego 5	z urzędu	likwidacja podmiotu
72.	05-06.10.2006 GI-DIS-K- 411/73/06	Komenda Główna Straży Granicznej, Warszawa, Al. Niepodległości 100	z urzędu	nie stwierdzono uchybień
73.	09-13.10.2006 GI-DIS-K- 411/74/06	Zakład Ubezpieczeń Społecznych Oddział w Krakowie, Kraków, ul. Pędzichów 27	z urzędu	wszczęto postępowanie administracyjne
74.	11-13.10.2006 GI-DIS-K-	Stowarzyszenie Rodziców i Przyjaciół Dzieci	z urzędu	16.03.2007, decyzja GI-DEC-DIS-11/07

	411/75/06	Niewidomych i Słabowidzących „Tęcza”, Warszawa, ul. Kopińska 6/10		
75.	18-20.10.2006 GI-DIS-K-411/76/06	Izba Celna w Warszawie, Warszawa, ul. Modlińska 4	z urzędu	nie stwierdzono uchybień
76.	23-27.10.2006 GI-DIS-K-411/77/06	Izba Celna w Poznaniu, Poznań, ul. Krańcowa 28	z urzędu	nie stwierdzono uchybień
77.	23-27.10.2006 GI-DIS-K-411/78/06	Zakład Ubezpieczeń Społecznych Oddział w Toruniu, Toruń, ul. Mickiewicza 10/16	z urzędu	wszczęto postępowanie administracyjne
78.	23-27.10.2006 GI-DIS-K-411/79/06	Zakład Ubezpieczeń Społecznych Oddział w Białymstoku, Białystok, ul. Młynowa 29	z urzędu	wszczęto postępowanie administracyjne
79.	23-25.10.2006 GI-DIS-K-411/80/06	2A Sp. z o.o., Warszawa, ul. Piękna 22	z urzędu	31.01.2007, zawiadomienie o przestępstwie
80.	23-25.10.2006 GI-DIS-K-411/81/06	2A Sp. z o.o. i Partnerzy Sp. j., Warszawa, ul. Domaniewska 7	z urzędu	31.01.2007, zawiadomienie o przestępstwie
81.	30.10.2006 GI-DIS-K-411/82/06	Agencja Restrukturyzacji i Modernizacji Rolnictwa, Warszawa, ul. Żelazna 59	z urzędu	nie stwierdzono uchybień
82.	06-10.11.2006 GI-DIS-K-411/83/06	Zakład Ubezpieczeń Społecznych Inspektorat w Częstochowie, Częstochowa, ul. Okólna 17/19	z urzędu	nie stwierdzono uchybień
83.	06-10.11.2006 GI-DIS-K-411/84/06	Zakład Ubezpieczeń Społecznych Inspektorat w Krakowie Łagiewnikach, Kraków, ul. Zakopiańska 33	z urzędu	wszczęto postępowanie administracyjne
84.	06.11.2006 GI-DIS-K-411/85/06	EuroCross International Polska Sp. z o.o., Warszawa, ul. Hrubieszowska 2	z urzędu	usunięto uchybienia
85.	06-10.11.2006 GI-DIS-K-411/86/06	Poznańskie Zakłady Sprzętu Ortopedycznego Sp. z o.o., Poznań, ul. Przemysłowa 15/17	Departament Rejestracji Zbiorów Danych Osobowych	20.04.2007, decyzja GI-DEC-DIS-14/07
86.	08-10.11.2006 GI-DIS-K-411/87/06	Miejskie Przedsiębiorstwo Komunikacyjne w Poznaniu Sp. z o.o., Poznań, ul. Głogowska 131/133	z urzędu	wykonano decyzję GI-DEC-DIS-122/04
87.	07-08.11.2006 GI-DIS-K-411/88/06	Naczelna Izba Lekarska, Warszawa, ul. Sobieskiego 110	z urzędu	wykonano decyzję GI-DEC-DIS-118/06
88.	09-10.11.2006 GI-DIS-K-411/89/06	Mineral Midrange Sp. z o.o., Warszawa, ul. Sobieskiego 110	z urzędu	wykonano decyzję GI-DEC-DIS-165/06
89.	09.11.2006 GI-DIS-K-411/90/06	EMPiK Sp. z o.o., Warszawa, ul. Marszałkowska 116/122	z urzędu	14.05.2007, decyzja GI-DEC-DIS-16/07
90.	13-17.11.2006 GI-DIS-K-411/91/06	Zakład Ubezpieczeń Społecznych Inspektorat we Włocławku, Włocławek, Pl. Wolności 18/19	z urzędu	wszczęto postępowanie administracyjne
91.	13.11.2006 GI-DIS-K-411/92/06	Cegedim Poland Sp. z o.o., Warszawa, ul. Pileckiego 63	z urzędu	wykonano decyzję GI-DEC-DIS-186/06

92.	15.11.2006 GI-DIS-K-411/93/06	Ferrero Polska Sp. z o.o., Warszawa, ul. Wiertnicza 126	z urzędu	wykonano decyzję GI-DEC-DIS-45/06
93.	17.11.2006 GI-DIS-K-411/94/06	Sitel Polska Sp. z o.o., Warszawa, ul. Domaniewska 41	z urzędu	wykonano decyzję GI-DEC-DIS-279/06
94.	15.11.2006 GI-DIS-K-411/95/06	Sygma Banque Societe Anonyme S.A. Oddział w Polsce, Warszawa, Al. Jerozolimskie 92	z urzędu	wykonano decyzję GI-DEC-DIS-155/06
95.	16.11.2006 GI-DIS-K-411/96/06	Kredyt Bank S.A., Warszawa, ul. Kasprzaka 2/8	z urzędu	wykonano decyzję GI-DEC-DIS-334/05
96.	17.11.2006 GI-DIS-K-411/97/06	Okręgowa Izba Lekarska, Warszawa, ul. Grójecka 65A	z urzędu	wykonano decyzję GI-DEC-DIS-77/06
97.	17.11.2006 GI-DIS-K-411/98/06	Triada Biuro Podróży Sp. z o.o., Warszawa, ul. Nowogrodzka 42	z urzędu	wykonano decyzję GI-DEC-DIS-144/05
98.	20-24.11.2006 GI-DIS-K-411/99/06	Zakład Ubezpieczeń Społecznych Inspektorat w Białej Podlaskiej, Biała Podlaska, ul. Sadowa 23	z urzędu	wszczęto postępowanie administracyjne
99.	23.11.2006 GI-DIS-K-411/100/06	Marek Niesiołkowski prowadzący działalność gospodarczą pod nazwą „Marksoft – Marek Niesiołkowski”, Warszawa, ul. Perzyńskiego 2	z urzędu	wykonano decyzję GI-DEC-DIS-376/05
100.	23.11.2006 GI-DIS-K-411/101/06	Agencja Nieruchomości Rolnych, Warszawa, ul. Dolańskiego 2	z urzędu	wykonano decyzję GI-DEC-DIS-82/06
101.	22.11.2006 GI-DIS-K-411/102/06	Krajowy Samorządowy Fundusz Pożyczkowy „Karbona” – Polska Grupa Spółdzielni Pożyczkowych – Spółdzielnia Osób Prawnych, Warszawa, ul. Miodowa 14	z urzędu	wniosek o kontrolę w podmiocie współpracującym z jednostką kontrolowaną
102.	27-28.11.2006 GI-DIS-K-411/103/06	Ray & Berndtson Polska Sp. o.o., Warszawa, ul. Puławska 15	z urzędu	wykonano decyzję GI-DEC-DIS-16/05
103.	27.11.2006 GI-DIS-K-411/104/06	Maciej Kierzkowski prowadzący działalność gospodarczą pod nazwą „Maciej Kierzkowski – Wydawnictwo Translegis”, Warszawa, ul. Krasińskiego 16 lok. 134	z urzędu	wykonano decyzję GI-DEC-DIS-173/04
104.	27-28.11.2006 GI-DIS-K-411/105/06	Carrefour Polska Sp. z o.o., Warszawa, ul. Targowa 72	z urzędu	wykonano decyzję GI-DEC-DIS-393/05
105.	29.11.2006 GI-DIS-K-411/106/06	Carrefour Polska Sp. z o.o., Warszawa, ul. Targowa 72	z urzędu	wykonano decyzję GI-DEC-DIS-381/05
106.	29-30.11.2006 GI-DIS-K-411/107/06	Przedsiębiorstwo Państwowej Komunikacji Samochodowej, Piaseczno, ul. Gen. Okulickiego 4	z urzędu	wykonano decyzję GI-DEC-DIS-89/05
107.	24.11.2006 GI-DIS-K-411/108/06	Netmaniak s.c. Paweł Kubalski, Paweł Ołtarzewski, Legionowo, ul. Jagiellońska 10	z urzędu	zmiana administratora danych

108.	05.12.2006 GI-DIS-K-411/109/06	PKO BP S.A., Warszawa, ul. Puławska 15	z urzędu	wykonano decyzję GI-DEC-DIS-192/04
109.	28.11.2006 GI-DIS-K-411/110/06	Bank Pekao S.A., Warszawa, ul. Grzybowska 53/57	z urzędu	wykonano decyzję GI-DEC-DIS-193/04
110.	05-06.12.2006 GI-DIS-K-411/111/06	Centralna Wojskowa Przychodnia Lekarska „CePeLek” Samodzielny Publiczny Zakład Opieki Zdrowotnej, Warszawa, ul. Koszykowa 78	z urzędu	wykonano decyzję GI-DEC-DIS-254/06
111.	05.12.2006 GI-DIS-K-411/112/06	Masterlink Express Sp. z o.o., Warszawa, ul. Mineralna 15	z urzędu	wykonano decyzję GI-DEC-DIS-256/06
112.	05.12.2006 GI-DIS-K-411/113/06	Klub Piłkarski Legia Warszawa Sportowa Spółka Akcyjna, Warszawa, ul. Łazienkowska 3	z urzędu	wykonano decyzję GI-DEC-DIS-183/06
113.	06.12.2006 GI-DIS-K-411/114/06	Prominent – Minchberg Sp. k., Warszawa, ul. Heleny Junkiewicz 2B/5	z urzędu	wykonano decyzję GI-DEC-DIS-278/06
114.	11-15.12.2006 GI-DIS-K-411/115/06	Batimex Corporation Sp. z o.o., Poznań, ul. Głogowska 170A	z urzędu	09.02.2007, zawiadomienie o przestępstwie
115.	11.12.2006 GI-DIS-K-411/117/06	Axel Springer Kontakt Sp. z o.o., Warszawa, ul. Jagiellońska 74	z urzędu	wykonano decyzję GI-DEC-DIS-259/05
116.	12.12.2006 GI-DIS-K-411/118/06	Axel Springer Polska Sp. z o.o., Warszawa, ul. Domaniewska 52	z urzędu	wykonano decyzję GI-DEC-DIS-98/06
117.	11-15.12.2006 GI-DIS-K-411/119/06	Polskie Media Amer.com S.A., Poznań, ul. Grochowe Łąki 6	z urzędu	wykonano decyzję GI-DEC-DIS-282/06
118.	12.12.2006 GI-DIS-K-411/120/06	Tomasz Broniecki i Grzegorz Broniecki Wspólnicy s.c. – Przedsiębiorstwo Produkcyjno – Handlowo – Usługowe Tomsoft, Warszawa, ul. Krzywa 4	z urzędu	wykonano decyzję GI-DEC-DIS-229/04
119.	11.12.2006 GI-DIS-K-411/121/06	Spencer Stuart Poland Sp. z o.o., Warszawa, ul. Mysia 5	z urzędu	wykonano decyzję GI-DEC-DIS-195/06
120.	11.12.2006 GI-DIS-K-411/122/06	Polsko – Japońska Wyższa Szkoła Technik Komputerowych, Warszawa, ul. Koszykowa 86	z urzędu	wykonano decyzję GI-DEC-DIS-133/04
121.	11.12.2006 GI-DIS-K-411/123/06	Oficyna Wydawnicza „Oikos” Sp. z o.o., Warszawa, ul. Kaliska 1/7	z urzędu	wykonano decyzję GI-DRZDO/401/DEC/001142/01-77/06
122.	12.12.2006 GI-DIS-K-411/125/06	Główny Inspektor Jakości Handlowej Artykułów Rolno – Spożywczych, Warszawa, ul. Wspólna 30	z urzędu	wykonano decyzję GI-DRZDO/401/DEC/004799/05-649/06
123.	12.12.2006 GI-DIS-K-411/126/06	Bawaria Motors Sp. z o.o., Warszawa, ul. Czerniakowska 47	z urzędu	wykonano decyzję GI-DRZDO/401/DEC/002151/05-541/06
124.	14.12.2006 GI-DIS-K-411/127/06	Brother International Austria GmbH Sp. z o.o. Przedstawicielstwo w Polsce, Warszawa, ul. Garażowa 7	z urzędu	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
125.	15.12.2006	Fundacja Rozwoju,	z urzędu	wykonano decyzję

	GI-DIS-K-411/128/06	Warszawa, ul. Ciołka 15		GI-DRZDO/401/DEC/001962/05-520/06
126.	18.12.2006 GI-DIS-K-411/129/06	PZ Cussons Polska S.A., Warszawa, ul. Kolska 3	z urzędu	wykonano decyzję GI-DRZDO/401/DEC/003168/05-512/06
127.	18-19.12.2006 GI-DIS-K-411/130/06	Przedsiębiorstwo Handlu Usługowego Jubiler Sp. z o.o., Warszawa, ul. Szyszkowa 35/37	z urzędu	nie stwierdzono uchybień
128.	18-19.12.2006 GI-DIS-K-411/131/06	Anyro & Co Sp. z o.o., Warszawa, ul. Szyszkowa 35/37	z urzędu	nie stwierdzono uchybień
129.	19.12.2006 GI-DIS-K-411/132/06	Fundacja „Poznaj Swoją Ojczyznę”, Warszawa, ul. Bernardyńska 1A	z urzędu	wykonano decyzję GI-DEC-DIS-59/06
130.	21.12.2006 GI-DIS-K-411/133/06	Imperial – Tatry Sp. z o.o., Warszawa, ul. Jagiellońska 15	z urzędu	wykonano decyzję GI-DEC-DIS-35/05
131.	22.12.2006 GI-DIS-K-411/134/06	Fundacja „Ad Rem”, Warszawa, ul. Bałuckiego 20/3	z urzędu	wykonano decyzję GI-DRZDO/401/DEC/002022/05-628/06
132.	19.12.2006 GI-DIS-K-411/135/06	Novartis Poland Sp. z o.o., Warszawa, Al. Witosa 31	z urzędu	wykonano decyzję GI-DEC-DIS-88/06

Załącznik nr 4 Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2006 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych.

I.p.	Data, sygnatura orzeczenia WSA w Warszawie lub NSA	Sygnatury decyzji Generalnego Inspektora Ochrony Danych Osobowych	Przedmiot sprawy	Rozstrzygnięcie Wojewódzkiego Sądu Administracyjnego w Warszawie lub Naczelnego Sądu Administracyjnego
1.	26.01.2006 r. II SA/Wa 1700/05	GI-DEC-DIS-147/05 GI-DEC-DIS-207/05	Odmowa stwierdzenia nieważności decyzji GI-DEC-DIS-35/05	Oddalenie skargi
2.	27.01.2006 r. II SA/Wa 2077/05	GI-DEC-DS-191/03 GI-DEC-DS-251/03	Udostępnienie przez Aster City Cable sp. z o.o. danych osobowych skarżącej w związku z przelewem wierzytelności	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej
3.	24.02.2006 r. II SA/Wa 1939/05	GI-DEC-DS-268/05	Przetwarzanie danych osobowych skarżącego przez Syndyka Masy Upadłości Banku Spółdzielczego – Bank Gospodarki Żywnościowej S.A. bez podstawy prawnej	Oddalenie skargi
4.	08.03.2006 r. II SAB/Wa 12/05	GI-DEC-DS-159/05 GI-DEC-DS-265/05	Skarga na bezczynność Generalnego Inspektora Ochrony Danych Osobowych	Umorzenie postępowania
5.	29.03.2006 r.	GI-DS-430/799/05	Naruszenie przepisów	Odrzucenie skargi

	II SA/Wa 373/06		Kodeksu postępowania administracyjnego.	
6.	30.03.2006 r. II SA/Wa 1719/05	GI-DEC-DS-51/05 GI-DEC-DS-215/05	Udostępnienie przez Bank Handlowy w Warszawie S.A. danych osobowych skarżącego Kancelarii Prawnej „Lexus” Spółka Komandytowa	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej
7.	30.03.2006 r. I OSK 628/05	GI-DEC-DS/89/04	Udostępnienie przez Regionalną Sieć Telekomunikacyjną El-Net S.A. danych osobowych skarżącej w związku z przelewem wierzytelności. Wojewódzki Sąd Administracyjny oddalił skargę GIODO	Oddalenie skargi kasacyjnej GIODO
8.	31.03.2006 r. II SA/Wa 2395/04	GI-DEC-DS-132/04 GI-DEC-DS-202/04	Udostępnienie przez Polkomtel S.A. danych osobowych skarżącego w związku z przelewem wierzytelności	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej
9.	31.03.2006 r. II SA/Wa 2396/04	GI-DEC-DS-132/04 GI-DEC-DS-202/04	Przetwarzanie przez P.R.E.S.C.O. Sp. z o.o. danych osobowych skarżącego pozyskanych w związku z przelewem wierzytelności	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej
10.	11.04.2006 r. II SA/Wa 316/06	GI-DIS-K-411/71/05/789	Odmowa przywrócenia terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy	Oddalenie skargi
11.	20.04.2006 r. II SA/Wa 29/06	GI-DS-430/216/05	Odmowa GIODO udostępnienie kserokopii dokumentów	Oddalenie skargi
12.	21.04.2006 r. I OSK 726/05	GI-DEC-DIS-31/04 GI-DEC-DIS-109/04	Nie zgłoszenie do rejestracji Generalnemu Inspektorowi prowadzonego zbioru danych osobowych	Oddalenie skargi kasacyjnej
13.	27.04.2006 r. I OSK 711/05	GI-DEC-DS/42/03	Przetwarzanie przez P.R.E.S.C.O. Sp. z o.o. danych osobowych skarżącego pozyskanych w związku z przelewem wierzytelności. Wojewódzki Sąd Administracyjny oddalił skargę P.R.E.S.C.O. Sp. z o.o.	Uchylenie zaskarżonego wyroku WSA i przekazanie WSA sprawy do ponownego rozpoznania
14.	12.05.2006 r. II SA/Wa 156/06	GI-DEC-DS-419/05	Odmowa udostępnienia informacji publicznej	Umożliwienie postępowania
15.	12.05.2006 r. II SA/Wa 15/06	GI-DEC-DS-133/05 GI-DEC-DS-350/05	Odmowa udostępnienia przez Prezydenta Miasta Szczecina skarżącemu danych osobowych osoby, która zainicjowała przeciw niemu postępowanie przed Urzędem miasta	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej

			Szczecina	
16.	15.05.2006 r. II SA/Wa 726/06	GI-DEC-DIS- 90/06	Odmowa stwierdzenia nieważności decyzji GI-DEC-DIS-55/06	Odrzucenie skargi
17.	16.05.2006 r. II S.A./Wa 1850/04	GI-DEC-DS- 143/04	Przetwarzanie przez P.R.E.S.C.O. Sp. z o.o. danych osobowych skarżącego pozyskanych w związku z przelewem wierzytelności	Umorzenie postępowania
18.	22.05.2006 r. II SA/Wa 2139/05	GI-DEC-DS- 217/05 GI-DEC-DS- 346/06	Nakazanie Narodowemu Funduszowi Zdrowia udostępnienie skarżącemu danych osobowych	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej
19.	24.05.2006 r. I OSK 727/05	GI-DEC-DIS- 81/04 GI-DEC-DIS- 165/04	Przechowywanie danych osobowych w postaci umożliwiającej identyfikację osób, których dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania	Uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania
20.	30.05.2006 r. II SA/Wa 1894/05	GI-DEC-DIS- 191/05 GI-DEC-DIS- 266/05	Udostępnianie danych osobom nieupoważnionym, nie zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym, nie zapewnienie kontroli nad tym, kto, kiedy i jakie dane wprowadził do zbioru oraz komu są przekazywane, brak ewidencji osób upoważnionych do przetwarzania danych, nie zgłoszenie prowadzonych zbiorów do rejestracji, brak spełnienia niektórych wymogów rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych	Uchylenie decyzji
21.	06.06.2006 r. II SA/Wa 2226/05	GI-DEC-DS- 344/05	Przetwarzanie danych osobowych skarżącego i jego małoletniej córki przez Stowarzyszenie Charytatywne „Dobromir”	Oddalenie skargi
22.	30.06.2006 r.	GI-DEC-DS-	Udostępnienie przez	Oddalenie skargi

	II SAWa 14/06	347/05	Sąd Rejonowy w Goleniowie danych o stanie zdrowia skarżącego osobom nieupoważnionym.	
23.	07.07.2006 r. II SA/Wa 176/06	GI-DS-430/279/05	Odmowa sporządzenia wykazu akt. Wojewódzki Sąd Administracyjny oddalił skargę.	Odrzucenie skargi kasacyjnej
24.	10.07.2006 r. II SA/Wa 955/06	GI-DEC-DS/5/03 GI-DEC-DS/42/03	Przetwarzanie przez P.R.E.S.C.O. Sp. z o.o. danych osobowych skarżącego pozyskanych w związku z przelewem wierzytelności	Stwierdzenie nieważności zaskarżonej decyzji i decyzji ją poprzedzającej
25.	13.07.2006 r. I OSK 1083/06	GI-DEC-DIS-105/04, GI-DEC-DIS-147/04	Zbieranie danych osobowych potencjalnych klientów w zakresie szerszym niż jest to niezbędne dla realizacji celów przetwarzania danych, przetwarzanie danych osób, z którymi nie została zawarta umowa	Uchylenie wyroku w części, w pozostałym zakresie oddalenie skargi kasacyjnej
26.	13.07.2006 r. I OSK 1084/05	GI-DEC-DIS-95/04 GI-DEC-DIS-118/04	Odmowa stwierdzenia nieważności decyzji GI-DEC-DIS-150/03	Oddalenie skargi kasacyjnej
27.	19.07.2006 r. II SA/Wa 738/06	GI-DEC-DS-377/05 GI-DEC-DS-48/06	Odmowa udostępnienia przez lekarza weterynarii Fundacji „Azyl pod Psim Aniołem” danych osób, którym ww. przekazał zwierzęta w trybie tzw. adopcji	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej
28.	30.08.2006. II SA/Wa 809/05	GI-DEC-DS-270/04 GI-DEC-DS-31/05	Odmowa udostępnienia Straży Miejskiej przez Polską Telefonię Cyfrową S.A. danych osobowych abonentów telefonów komórkowych użytkowników tej sieci	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej
29.	11.09.2006 r. II SA/Wa 14/06	GI-DEC-DS-347/05	Udostępnienie przez Sąd Rejonowy w Goleniowie danych o stanie zdrowia skarżącego osobom nieupoważnionym. Wojewódzki Sąd Administracyjny oddalił skargę	Odrzucenie skarg kasacyjnych (2 skargi)
30.	19.09.2006 r. II SA/Wa 260/06	GI-DEC-DS-412/05	Udostępnienie przez Polkomtel S.A. danych osobowych skarżącego P.R.E.S.C.O. Sp. z o.o. w związku z przelewem wierzytelności	Stwierdzenie nieważności zaskarżonej decyzji
31.	22.09.2006 r.	GI-DEC-DS/1/06	Nakazanie Zakładowi	Oddalenie skargi

	II SA/Wa 382/06		Ubezpieczeń Społecznych udostępnienia akt emerytalno-rentowych, zawierających dane osobowe skarżącego na potrzeby badań naukowych	
32.	28.09.2006 r. II SA/Wa 898/06	GI-DEC-DS-80/06	Odmowa udostępnienia przez Fundację „Centrum Ochrony Środowiska”, prowadzącą schronisko dla bezdomnych zwierząt Fundacji „Azyl pod Psim Aniołem” danych osób, którym przekazane zostały zwierzęta w trybie tzw. adopcji	Oddalenie skargi
33.	03.10.2006 r. II SA/Wa 871/06	GI-DEC-DS/74/06	Udostępnienie przez Bank Millennium S.A. danych skarżącej BIK S.A. oraz w związku z przelewem wierzytelności PTF Bankowi S.A.	Częściowe uchylenie zaskarżonej decyzji, oddalenie skargi w pozostałym zakresie
34.	05.10.2006 r. I OSK 1365/06	GI-DEC-DIS-191/05 GI-DEC-DIS-266/05	Udostępnianie danych osobom nieupoważnionym, nie zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym, nie zapewnienie kontroli nad tym, kto, kiedy i jakie dane wprowadził do zbioru oraz komu są przekazywane, brak ewidencji osób upoważnionych do przetwarzania danych, nie zgłoszenie prowadzonych zbiorów do rejestracji, brak spełnienia niektórych wymogów rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych	Umorzenie postępowania
35.	10.10.2006 r. II SA/Wa 642/05	GI-DEC-DS-208/04 GI-DEC-DS/7/05	Odmowa udostępnienia Straży Miejskiej przez Polkomtel S.A. danych osobowych abonenta	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej

			telefonu komórkowego użytkownika tej sieci	
36.	10.10.2006 r. I OSK 1353/05	GI-DRZDO/ 401/DEC/010304/ 99-388/04	Odmowa rejestracji zbioru danych.	Oddała skargę kasacyjną
37.	26.10.2006 r. II SA/Wa 1337/06	GI-DEC-DS- 152/06	Wstrzymanie wykonania decyzji Generalnego Inspektora Ochrony Danych Osobowych	Odmowa wstrzymania wykonania decyzji
38.	07.11.2006 r. II SA/Wa 1289/06	GI-DEC-DIS- 81/04 GI-DEC-DIS- 165/04	Przechowywanie danych osobowych w postaci umożliwiającej identyfikację osób, których dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania	Uchylenie decyzji
39.	09.11.2006 r. II SA/Wa 1781/06	GI-DS-430/757/05	Odmowa wydania uwierzytelnionych odpisów dokumentów z akt sprawy	Odrzucenie skargi
40.	10.11.2006 r. II SA/Wa 4/06	GI-DEC-DS- 337/05	Udostępnienie Przez Telekomunikację Polską S.A. danych osobowych skarżącego Intrum Justitia Debt Finance AD i Intrum Justitia Sp. z o.o. w związku z przelewem wierzytelności	Oddalenie skargi
41.	15.11.2006 r. II SA/Wa 1612/06	GI-DEC-DIS- 105/04 GI-DEC-DIS- 147/04	Zbieranie danych osobowych potencjalnych klientów w zakresie szerszym niż jest to niezbędne dla realizacji celów przetwarzania danych, przetwarzanie danych osób, z którymi nie została zawarta umowa	Oddalenie skargi
42.	21.11.2006 r. II SA/Wa 1472/06	GI-DS-430/184/06	Przekazanie podania według właściwości	Odrzucenie skargi
43.	30.11.2006 r. II SA/Wa 1552/06	GI-DEC-DS- 228/06	Odmowa udostępnienia przez Polską Telefonię Cyfrową Sp. z o.o. danych osobowych Komendantowi Straży Miejskiej	Wstrzymanie wykonania zaskarżonej decyzji

Załącznik nr 5 Informacje przekazane przez organy ścigania w sprawach skierowanych w 2006 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa.

Informacja	Rok 2004	Rok 2005	Rok 2006
Umorzenie dochodzenia	4	13	2
Umorzenie dochodzenia w części	-	-	
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	12	13	
Umorzenie dochodzenia i odmowa podjęcia go na nowo	5	7	
Wszczęcie dochodzenia	9	8	
Odmowa wszczęcia dochodzenia	3	21	1
Wszczęcie śledztwa i jego umorzenie	15	15	
Zawieszenie dochodzenia	11	1	
Skierowanie sprawy do sądu	21	12	
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	6	5	
Brak informacji	10	13	

Załącznik nr 6 Dokumenty Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych przyjęte w 2006 r.

Lp	Dokumenty Grupy Roboczej Artykułu 29 (2006)
1	Opinia 1/2006 w sprawie zastosowania unijnych zasad ochrony danych do wewnętrznych systemów informowania o nieprawidłowościach w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych (WP 117)
2	Opinia nr 2/2006 dotyczącą kwestii prywatności w związku ze świadczeniem usług skanowania wiadomości elektronicznych (WP 118)
3	Opinia nr 3/2006 w sprawie dyrektywy Parlamentu Europejskiego i Rady nr 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE, przyjętej przez Radę dnia 21 lutego 2006 r. (WP 119)
4	Program prac na lata 2006-2007 (WP 120)
5	Opinia nr 4/2006 w sprawie Powiadomienia dotyczącego wniosku legislacyjnego Departamentu Zdrowia i Opieki Społecznej Stanów Zjednoczonych w sprawie kontroli chorób zakaźnych i zbierania informacji o pasażerach z dnia 20 listopada 2005 r. (Wniosek w sprawie kontroli chorób zakaźnych 42 CFR część 70 i 71) (WP 121)
6	Opinia nr 5/2006 w sprawie wyroku Europejskiego Trybunału Sprawiedliwości z dnia 30 maja 2006 r. w połączonych sprawach C-317/04 i C-318/04 dotyczących przekazywania danych dotyczących pasażerów (PNR) do Stanów Zjednoczonych Ameryki (WP 122)
7	Opinia nr 6/2006 dotyczącą projektu rozporządzenia Rady w sprawie jurysdykcji, obowiązującego prawa, uznawania i wykonywania decyzji oraz współpracy w zakresie obowiązków alimentacyjnych (WP 123)
8	Opinia nr 7/2006 w sprawie wyroku Europejskiego Trybunału Sprawiedliwości z dnia 30 maja 2006 r. w połączonych sprawach C-317/04 i C-318/04 w sprawie przekazywania danych przechowywanych w imiennym rejestrze pasażerów (PNR) do Stanów Zjednoczonych Ameryki i pilnej konieczności przygotowania nowej umowy (WP 124)
9	Dokument roboczy w sprawie ochrony danych i wpływu na prywatność w kontekście inicjatywy eCall (WP 125)
10	Opinia nr 8/2006 dotyczącą przeglądu ram regulacyjnych dotyczących sieci i usług łączności elektronicznej, ze szczególnym uwzględnieniem dyrektywy o prywatności i łączności elektronicznej (WP 126)
11	Opinia nr 9/2006 dotyczącą wdrożenia dyrektywy 2004/82/WE Rady w sprawie zobowiązania przewoźników do przekazywania z wyprzedzeniem danych pasażerów (WP 127)
12	Opinia nr 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT), (WP 128)