

**Generalny Inspektor
Ochrony Danych Osobowych**

**SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH
W ROKU 2007**

Sprawozdanie stanowi wykonanie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. 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 1 stycznia 2007 r do 31 grudnia 2007 r.

SPIS TREŚCI

I.	Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych	4
II.	Biuro Generalnego Inspektora Ochrony Danych Osobowych	5
	1. Struktura organizacyjna	5
	2. Pracownicy Biura GIODO	5
	3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2007 rok	6
Część I.	Stan wiedzy i przestrzegania przepisów o ochronie danych osobowych	7
1.	Informacje ogólne	7
2.	Kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych	8
2.1.	Czynności kontrolne	8
2.2.	Kontrola przetwarzania danych osobowych w wybranych obszarach	10
	1) Administracja publiczna	10
	2) Bezpieczeństwo publiczne	12
	3) Banki i inne instytucje finansowe	12
	4) Służba zdrowia	14
	5) Ubezpieczenia społeczne, majątkowe i osobowe	16
	6) Archiwa	18
	7) Inne	19
3.	Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych	22
	1) Administracja publiczna	25
	2) Bezpieczeństwo publiczne	29
	3) Banki i inne instytucje finansowe	31
	4) Sądy, organy prokuratury, komornicy	34
	5) Marketing	36
	6) Sektor mieszkalnictwa	39
	7) Ubezpieczenia społeczne, majątkowe i osobowe	41
	8) Telekomunikacja	44
	9) Sektor zatrudnienia	48
	10) Inne....	51
4.	Prowadzenie rejestru zbiorów danych osobowych oraz udzielanie informacji o zarejestrowanych zbiorach	54

5.	Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych	61
6.	Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych	76
. 6.1.	Interpretacja przepisów	77
6.2.	Działalność informacyjna	101
7.	Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych	112
Część II.	Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2007 roku	115
Część III.	Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych	130
Załączniki		
Załącznik nr 1	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2007 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego.....	136
Załącznik nr 2	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2007 do podmiotów prywatnych	139
Załącznik nr 3	Wykaz kontroli przeprowadzonych w 2007 roku	141
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	155
Załącznik nr 5	Informacje przekazane przez organy ścigania w sprawach skierowanych w 2007 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa	161
Załącznik nr 6	Wykaz szkoleń przeprowadzonych przez GODO w 2007 r.	162

SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2007

I. 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) – wydane na podstawie art. 39a ustawy - które określa:
 - sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
 - podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
 - wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.
- 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) – wydane na podstawie art. 46a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia,
- 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) – wydane na podstawie art. 22a ustawy – określa wzory, o których mówi to rozporządzenie.

Na system ochrony danych osobowych składają się też przepisy szczególne innych ustaw, które regulują kwestie wykorzystywania danych osobowych. Podmioty publiczne, w myśl zasady praworządności wyrażonej w art. 7 Konstytucji Rzeczypospolitej Polskiej, działają wyłącznie na

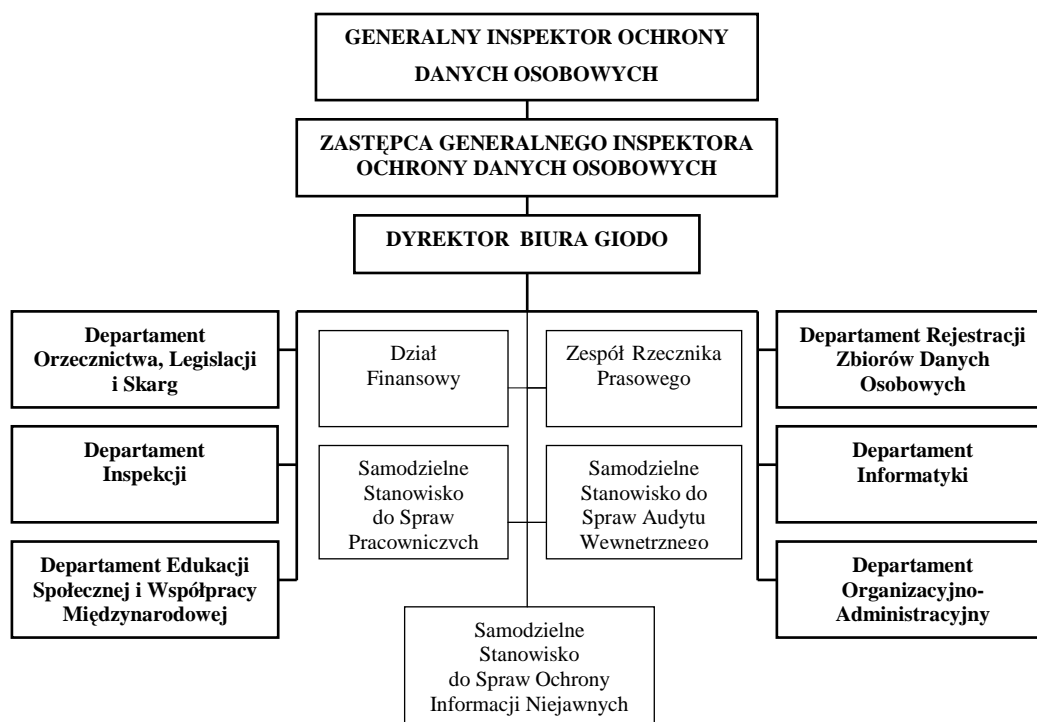
podstawie i w granicach prawa. Oznacza to, że mogą one przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu określonych prawem zadań, obowiązków i upoważnień.

II. 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.

Strukturę organizacyjną Biura Generalnego Inspektora Ochrony Danych Osobowych przedstawia poniższy schemat:



Generalny Inspektor wykonuje swoje zadania bezpośrednio lub przy pomocy Dyrektora Biura, dyrektorów jednostek organizacyjnych Biura, osób wskazanych w Regulaminie Biura.

2. Pracownicy Biura GODO

Stan zatrudnienia w Biurze GODO na dzień 31 grudnia 2007 r. wyniósł 117 etatów. Na stanowiskach merytorycznych zatrudnione były 103 osoby, a na stanowiskach pomocniczych 17 osób. Wyższe wykształcenie posiadało 97 pracowników, w tym 67 legitymowało się wykształceniem wyższym prawniczym.

Zatrudnienie w poszczególnych jednostkach organizacyjnych Biura GIODO w przeliczeniu **na pełny etat** na koniec 2007 r. przedstawia się następująco:

- GIODO – 1 osoba,
- Zastępca GIODO – 1 osoba,
- Asystent GIODO – 1 osoba,
- Dyrektor Biura – 1 osoba,
- Zespół Rzecznika Prasowego – 5 osób,
- Departament Edukacji Społecznej i Współpracy Międzynarodowej [dalej: DESiWM] – 10 osób,
- Departament Informatyki [dalej: DIF] – 14 osób,
- Departament Inspekcji [dalej: DIS] – 20 osób,
- Departament Orzecznictwa, Legislacji i Skarg [dalej: DOLiS] – 25 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 – 2 osoby,

3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2007 rok

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2007 r. wynosił: 12 391 tys. zł, w tym:

wynagrodzenia	8 152 tys. zł
pochodne od wynagrodzeń	1 483 tys. zł
wydatki majątkowe	182 tys. zł
pozostałe wydatki	2 574 tys. zł

Wydatki zrealizowane przez GIODO wynosiły 12 139 tys. zł, w tym:

wynagrodzenia	8 052 tys. zł
pochodne od wynagrodzeń	1 350 tys. zł
wydatki majątkowe	182 tys. zł
pozostałe wydatki	2 555 tys. zł

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

1. Informacje ogólne

Ustawa o ochronie danych osobowych [dalej: ustawa] 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 bez większego wysiłku na określenie tożsamości tej osoby. Danymi osobowymi nie będą jednak pojedyncze informacje o dużym stopniu ogólności. Dopiero z chwilą zestawienia ich z innymi, dodatkowymi informacjami, które w konsekwencji pozwolą na odniesienie ich do konkretnej osoby, takie informacje stają się danymi osobowymi.

Możliwa do zidentyfikowania jest więc taka osoba, której tożsamość można określić bezpośrednio lub pośrednio, zwłaszcza poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 26 ust. 1 ustawy, ujmując je w formę podstawowych obowiązków administratora danych.² Z jego treści wynika, że administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie, ma on przestrzegać wskazanych poniżej zasad:

- 1) legalności – dane mogą być przetwarzane tylko na podstawie przepisów prawa,
- 2) celowości – dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, jeśli jest to niezgodne z tymi celami,
- 3) merytorycznej poprawności – dane powinny być merytorycznie poprawne,
- 4) adekwatności – dane powinny być adekwatne w stosunku do celów, w jakich są przetwarzane,
- 5) ograniczenia czasowego – dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie mogą być przechowywane dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania.

Jako obywatele mamy możliwość skorzystania z przysługującego nam prawa do formalnej kontroli przetwarzania dotyczących nas danych, które ustanowione 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

² Administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych (art. 7 pkt 4 ustawy o ochronie danych osobowych). Między innymi może to być organ państwowy, organ samorządu terytorialnego lub państwowa albo komunalna jednostka organizacyjna.

informacji o źródle, z którego pochodzą, żądania uzupełnienia, uaktualnienia, sprostowania, a nawet 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 dane 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 obywateli do ochrony ich danych osobowych. Ponadto ustanawia instrumenty umożliwiające realizację tego prawa.

Nad przestrzeganiem prawa obywateli do ochrony dotyczących ich danych osobowych czuwa niezależny organ – Generalny Inspektor Ochrony Danych Osobowych. Postępowanie w sprawach uregulowanych w ustawie o ochronie danych osobowych Generalny Inspektor prowadzi według zasad określonych w przepisach Kodeksu postępowania administracyjnego [dalej: K.p.a.], o ile przepisy ustawy o ochronie danych osobowych nie stanowią inaczej (art. 22 ustawy).

Zgodnie z brzmieniem art. 12 ustawy, Generalny Inspektor w szczególności:

- 1) kontroluje zgodność przetwarzania danych z przepisami o ochronie danych osobowych,
- 2) wydaje decyzje administracyjne i rozpatruje skargi w sprawach wykonania przepisów o ochronie danych osobowych,
- 3) prowadzi ogólnokrajowy, jawny rejestr zbiorów danych oraz udziela informacji o zarejestrowanych zbiorach,
- 4) opiniuje projekty ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- 5) inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych,
- 6) uczestniczy w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

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

2.1. Czynności kontrolne

Czynności kontrolne, których celem jest ustalenie, czy jednostka kontrolowana przetwarza dane zgodnie z przepisami o ochronie danych osobowych, przeprowadzane są na podstawie art. 12 pkt 1 i art. 14 ustawy o ochronie danych osobowych. W art. 14 ustawy wymienione zostały uprawnienia przysługujące Generalnemu Inspektorowi Ochrony Danych Osobowych, Zastępcy Generalnego

Inspektora Ochrony Danych Osobowych oraz upoważnionym inspektorom w związku z realizacją zadania określonego w art. 12 pkt 1 powołanej ustawy.

Uprawnienia te obejmują przede wszystkim:

- prawo wstępu do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
- żądania złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwanie osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
- wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
- przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

Wymienionym uprawnieniom towarzyszy obowiązek kierownika jednostki kontrolowanej umożliwienia inspektorom dokonania tych czynności (art. 15 ust. 1 ustawy o ochronie danych osobowych).

Czynności wykonywane podczas kontroli (odbieranie wyjaśnień od kierownictwa i pracowników kontrolowanej jednostki, oględziny) są dokumentowane w formie:

- protokołów przyjęcia ustnych wyjaśnień,
- protokołów przesłuchania świadka,
- protokołów oględzin miejsca, pomieszczeń, dokumentów, urządzeń, nośników, systemów informatycznych służących do przetwarzania danych osobowych.

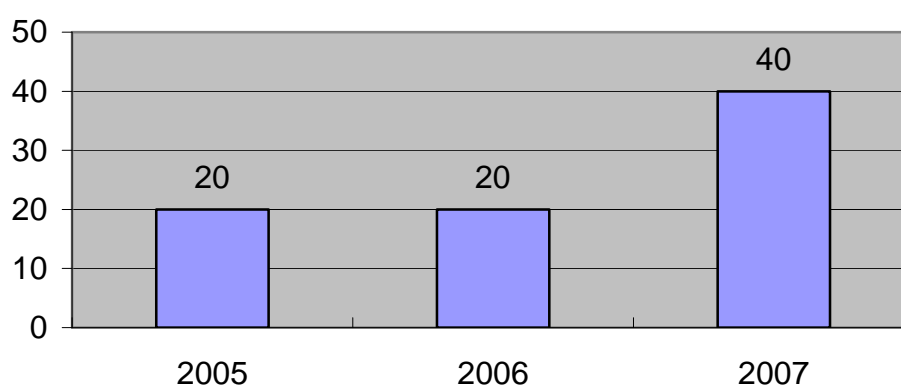
Na podstawie ustaleń zawartych w ww. protokołach, kserokopii dokumentów przedłożonych w toku kontroli oraz wydruków z systemów informatycznych służących do przetwarzania danych osobowych sporządzany jest protokół kontroli. Podpisują go inspektorzy, którzy kontrolę przeprowadzili. Protokół przedstawiany jest następnie do podpisu kierownikowi jednostki kontrolowanej, który, zgodnie z art. 16 ust. 2 ustawy o ochronie danych osobowych, może wnieść do niego umotywowane zastrzeżenia i uwagi. W zależności od ustaleń poczynionych w toku kontroli, tzn. tego, czy w procesie przetwarzania danych osobowych stwierdzone zostały nieprawidłowości, czy nie, wszczynane jest postępowanie administracyjne albo do jednostki kontrolowanej kierowane jest pismo z informacją, że w zakresie objętym kontrolą nie stwierdzono uchybień. Ponadto w przypadku stwierdzenia, że działanie lub zaniechanie kierownika jednostki kontrolowanej lub jej pracownika wyczerpuje znamiona przestępstwa określonego w ustawie o ochronie danych osobowych, do organu powołanego do ścigania przestępstw kierowane jest zawiadomienie o popełnieniu

przestępstwa. Ustalenia kontrolne mogą także uzasadnić żądanie wszczęcia postępowania dyscyplinarnego przeciwko osobom winnym dopuszczenia do uchybień.

2.2. Kontrola przetwarzania danych osobowych w wybranych obszarach

1) Administracja publiczna

W okresie sprawozdawczym, na ogólną liczbę 167 kontroli, w **podmiotach wykonujących zadania publiczne** przeprowadzono 40 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych³.



Wykres 1: *Porównanie liczby kontroli przeprowadzonych w podmiotach należących do sektora administracji publicznej w latach 2005–2007.*

W tej kategorii podmiotów kontrole przeprowadzono m.in. w jednostkach samorządu terytorialnego, tj. urzędach marszałkowskich, starostwach powiatowych i urzędach gmin (25 kontroli). Objęto nimi zabezpieczenie danych osobowych przetwarzanych przez te podmioty.

Na podstawie ustaleń kontrolnych należy krytycznie ocenić poziom spełnienia przez organy administracji samorządowej wymogów określonych w przepisach o ochronie danych osobowych – uchybień w procesie przetwarzania danych osobowych nie stwierdzono tylko w czasie jednej kontroli. Ww. podmioty najwięcej problemów miały z właściwym zabezpieczeniem danych osobowych. Stosowane w tym zakresie przez jednostki samorządu terytorialnego rozwiązania techniczne i organizacyjne nie zapewniały ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną. Nie dbano należycie zwłaszcza o zabezpieczenie danych przed: ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

³ Np. kontrole GI-DIS-K-411/48/07, GI-DIS-K-411/50/07, GI-DIS-K-411/58/07, DIS-K-421/147/07, DIS-K-421/163/07

Uchybienia polegały przede wszystkim na przechowywaniu dokumentacji zawierającej dane osobowe na odkrytych regałach oraz w szafach niewyposażonych w zamki, a także w pomieszczeniach, w których przyjmowane były osoby postronne.

Kontrole wykazały również inne uchybienia w procesie przetwarzania danych osobowych, zwłaszcza dotyczące dokumentacji opisującej sposób przetwarzania danych osobowych oraz przetwarzania danych osobowych przy użyciu systemów informatycznych. Stwierdzone w tym zakresie nieprawidłowości polegały m.in. na niezawarciu w polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wszystkich wymaganych informacji określonych w przepisach o ochronie danych osobowych. Natomiast uchybienia w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych dotyczyły przede wszystkim niespełniania przez te systemy wszystkich wymogów o charakterze technicznym (m.in. nie zapewniały one każdej osobie, której dane były przetwarzane w systemie informatycznym, odnotowania daty ich pierwszego wprowadzenia do systemu, identyfikatora użytkownika je wprowadzającego; hasła dostępu zmienianie były rzadziej niż co 30 dni). W pojedynczych przypadkach stwierdzono także nieprawidłowości polegające na niezabezpieczeniu systemu informatycznego służącego do przetwarzania danych osobowych przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, niewykonywaniu kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

Niektóre uchybienia w procesie przetwarzania danych osobowych były konsekwencją wykorzystywania w jednostkach administracji publicznej do przetwarzania danych osobowych systemów informatycznych oferowanych przez producentów oprogramowania istniejących na rynkach lokalnych. Systemy lokalne najczęściej nie były dostosowane do wymogów wynikających z przepisów o ochronie danych osobowych, m.in. z powodu zastosowania przestarzałych narzędzi informatycznych oraz zaprzestania ich rozwijania przez autorów systemu. Jednocześnie w toku kontroli zaobserwowano tendencje do łączenia lub zastępowania odrębnych systemów informatycznych zintegrowanymi systemami służącymi do całościowej obsługi informatycznej jednostek samorządowych. Systemy te charakteryzowały się konstrukcją modułową – dane osobowe przetwarzane były w jednej centralnej bazie z dostępem do odpowiednich kategorii danych, regulowanym poprzez nadawanie odpowiednich uprawnień użytkownikom tych systemów.

W związku ze stwierdzonymi w czasie kontroli uchybieniami wydane zostały decyzje nakazujące ich usunięcie oraz decyzje umarzające postępowanie w zakresie nieprawidłowości na bieżąco usuniętych przez jednostki kontrolowane w toku postępowania⁴. W wydanych decyzjach Generalny Inspektor nakazał m.in. zastosowanie środków technicznych i organizacyjnych

⁴ Np. decyzje: z dnia 26 czerwca 2007 r. o sygn. GI-DEC-DIS-25/07, z dnia 10 lipca 2007 r. o sygn. GI-DEC-DIS-41/07, z dnia 1 sierpnia 2007 r. o sygn. GI-DEC-DIS-55/07

zapewniających ochronę przetwarzanych danych osobowych, uzupełnienie polityki bezpieczeństwa o opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także, aby dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten każdorazowo odnotowywał datę pierwszego wprowadzenia jej danych do systemu.

2) Bezpieczeństwo publiczne

W okresie sprawozdawczym, w związku z wejściem Polski do strefy Schengen, Generalny Inspektor Ochrony Danych Osobowych przeprowadził kontrolę Centralnego Organu Technicznego Krajowego Systemu Informatycznego [dalej: KSI]⁵ w celu sprawdzenia, czy System ten, służący do przekazywania oraz dostępu do danych gromadzonych w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, spełnia wymogi określone w art. 36 – 39 ustawy o ochronie danych osobowych i 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 osobowych⁶. Kontrola ta została przeprowadzona na podstawie przepisów ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz w Systemie Informacji Wizowej i na skutek złożonego przez Komendanta Głównego Policji wniosku o przeprowadzenie kontroli⁷.

Kontrola wykazała, że KSI spełnia określone przepisami prawa wymogi, wobec czego Generalny Inspektor wydał stosowną opinię w tej sprawie, co było jednym z warunków niezbędnych do uruchomienia Krajowego Systemu Informatycznego⁸.

3) Banki i inne instytucje finansowe

W 2007 r. 29 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych przeprowadzono **w bankach oraz innych instytucjach finansowych**⁹, a najwięcej w towarzystwach zarządzających funduszami inwestycyjnymi (10) oraz w podmiotach prowadzących rejestry uczestników funduszy inwestycyjnych (6).

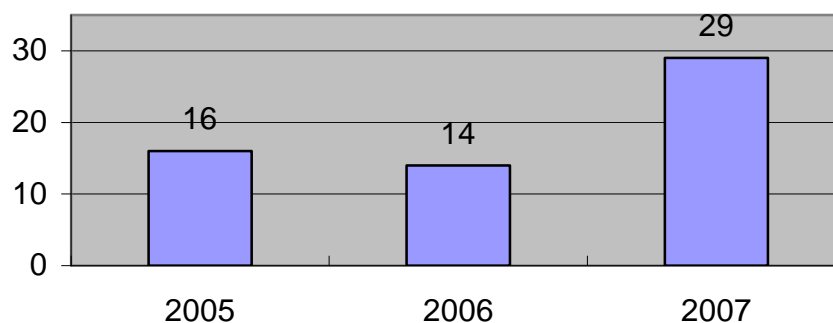
⁵ Centralnym Organem Technicznym KSI jest Komendant Główny Policji.

⁶ Kontrola DIS-K-421/168/07

⁷ Wniosek z dnia 17 grudnia 2007 r. złożony na podstawie art. 30 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz w Systemie Informacji Wizowej, zgodnie z którym Centralny Organ Techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego, jest obowiązany do wystąpienia do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o przeprowadzenie kontroli w zakresie spełniania przez Krajowy System Informatyczny wymogów określonych w art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz w przepisach wydanych na podstawie art. 39a tej ustawy.

⁸ Opinia z dnia 19 grudnia 2007 r. o sygn. DIS-K-421/168/07/966

⁹ Np. kontrole GI-DIS-K-411/2/07, GI-DIS-K-411/15/07 i GI-DIS-K-411/21/07



Wykres 2: Porównanie liczby kontroli przeprowadzonych w sektorze banków i innych instytucji finansowych w latach 2005–2007.

W związku z kontrolami przeprowadzanymi w omawianym sektorze powstał problem dotyczący określenia, czy administratorami danych osobowych uczestników funduszy inwestycyjnych są poszczególne fundusze inwestycyjne, czy towarzystwa zarządzające tymi funduszami.

Na podstawie analizy obowiązującego stanu prawnego uznano, że administratorami danych uczestników funduszy inwestycyjnych są poszczególne fundusze inwestycyjne. Natomiast towarzystwa są administratorami danych przetwarzanych w celach marketingowych, np. gdy prowadzą zbiory danych osobowych obejmujące dane tych uczestników funduszy inwestycyjnych, którzy wypełnili kupon akcji promocyjnej i wyrazili zgodę na przetwarzanie przez towarzystwo swoich danych osobowych w celach marketingowych. W toku kontroli przeprowadzonych w towarzystwach funduszy inwestycyjnych stwierdzono, że każde z nich zarządzało od kilku do kilkunastoma funduszami inwestycyjnymi, z czego większość stanowiły fundusze otwarte (liczba zamkniętych funduszy jest mniejsza). Nadmienić przy tym należy, że uczestnikami funduszy mogą być zarówno osoby fizyczne (w niektórych funduszach dostosowanych do potrzeb wąskiej grupy inwestorów może być nawet tylko jeden uczestnik), jak i osoby prawne.

Na podstawie wyników kontroli Generalny Inspektor ustalił, że większość towarzystw funduszy inwestycyjnych miała problemy dotyczące przestrzegania przepisów o ochronie danych osobowych – uchybień nie stwierdzono tylko w toku trzech kontroli. Stwierdzone nieprawidłowości dotyczyły m.in.: niewyznaczenia administratora bezpieczeństwa informacji, nienadania upoważnień osobom dopuszczonym do przetwarzania danych osobowych, nieprowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, niezgłoszenia do rejestracji zbioru danych osobowych uczestników funduszu, formułowania klauzul zgody zawierających oświadczenia na przetwarzanie danych osobowych w sposób wprowadzający w błąd osoby, które składają takie oświadczenie.

Na podstawie art. 87 ust. 1 ustawy o funduszach inwestycyjnych, fundusz inwestycyjny otwarty prowadzi rejestr swoich uczestników, który zawiera w szczególności dane identyfikujące każdego uczestnika. Możliwość powierzenia innemu podmiotowi prowadzenia rejestru uczestników funduszy inwestycyjnych wynika pośrednio z art. 31 ust. 2 pkt 3 wspomnianej ustawy¹⁰. Umowę z podmiotem prowadzącym rejestr uczestników funduszu inwestycyjnego, o której mowa w powołanym wyżej przepisie, należy zakwalifikować jako umowę powierzenia przetwarzania danych osobowych. W toku kontroli ustalono, że większość funduszy zawarło umowy o prowadzenie rejestru uczestników, a tylko nieliczne prowadziły je samodzielnie.

Podsumowując, w toku kontroli podmiotów prowadzących rejestr uczestników funduszu inwestycyjnego stwierdzono m.in. takie uchybienia w zakresie przestrzegania przepisów o ochronie danych osobowych, jak: pozyskiwanie danych uczestników funduszy inwestycyjnych w zakresie nieadekwatnym w stosunku do celów, w jakich są przetwarzane, niezawarcie w ewidencji osób upoważnionych do przetwarzania danych osobowych daty nadania i ustania oraz zakresu upoważnienia do przetwarzania danych osobowych, zmienianie haseł do systemów informatycznych, w których są przetwarzane dane osobowe uczestników funduszy inwestycyjnych, rzadziej niż co 30 dni.

W związku z tym, że w toku postępowania administracyjnego kontrolowane jednostki przywróciły stan zgodny z prawem, wydane zostały decyzje umarzające postępowanie¹¹.

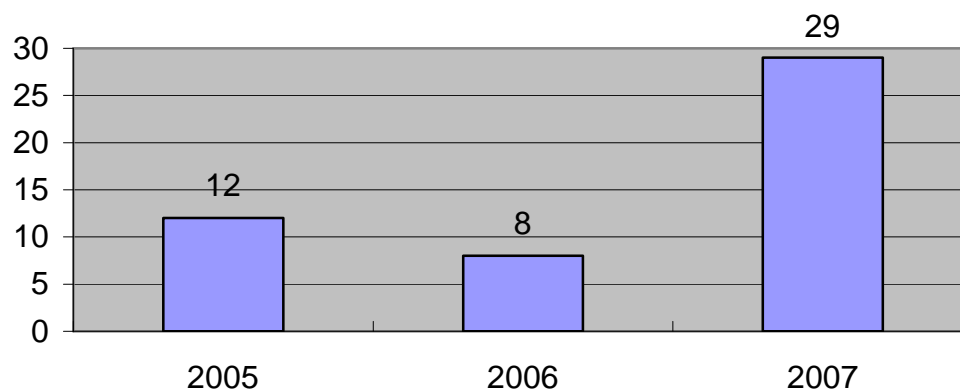
4) Służba zdrowia

W okresie sprawozdawczym w **podmiotach udzielających świadczeń zdrowotnych, aptekach oraz jednostkach organizacyjnych samorządu lekarzy** przeprowadzono 29 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych¹². Zakresem kontroli objęto zabezpieczenia danych osobowych przetwarzanych przez te podmioty.

¹⁰ Art. 31 ust. 2 pkt 3: Z chwilą wpisania funduszu inwestycyjnego do rejestru fundusz inwestycyjny wstępuje w prawa i obowiązki z tytułu umowy z podmiotem prowadzącym rejestr uczestników funduszu inwestycyjnego.

¹¹ Np. decyzje: z dnia 15 maja 2007 r. o sygn. GI-DEC-DIS-17/07, z dnia 29 czerwca 2007 r. o sygn. GI-DEC-DIS-30/07, z dnia 10 lipca 2007 r. o sygn. GI-DEC-DIS-43/07

¹² Np. kontrole GI-DIS-K-411/96/07, GI-DIS-K-411/97/07, GI-DIS-K-411/98/07



Wykres 3: ***Porównanie liczby kontroli przeprowadzonych w sektorze służby zdrowia w latach 2005–2007.***

Na podstawie ustaleń kontrolnych krytycznie należy ocenić poziom spełnienia przez kontrolowane jednostki wymogów określonych w przepisach o ochronie danych osobowych. Uchybień w procesie przetwarzania danych osobowych nie stwierdzono tylko w dziewięciu przypadkach. Negatywna ocena dotyczy zwłaszcza stosowania przez podmioty udzielające świadczeń zdrowotnych środków technicznych i organizacyjnych mających na celu zapewnienie ochrony przetwarzanych danych w niepełnym zakresie. Kontrole wykazały, że zastosowane przez administratorów danych środki nie zabezpieczają danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Nieprawidłowości w tym zakresie stwierdzono w dziesięciu kontrolowanych jednostkach.

Podkreślić należy, że 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 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 niewyposażonych w zamki, a także w pomieszczeniach, do których dostęp miały osoby trzecie.

Przeprowadzone kontrole wykazały ponadto, że podmioty udzielające świadczeń zdrowotnych miały również problemy z prawidłowym wypełnieniem innych obowiązków administratora danych określonych w ustawie o ochronie danych osobowych, tj. z:

- zapewnieniem kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu były przekazywane,
- opracowaniem ewidencji osób upoważnionych do przetwarzania danych osobowych,

- opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń i kategorii danych objętych ochroną.

W toku kontroli wymienionych podmiotów stwierdzono także liczne uchybienia w procesie przetwarzania danych osobowych w systemach informatycznych. Polegały one m.in. na: niezapewnianiu 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 te dane, niezabezpieczeniu systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, niewykonywaniu kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych oraz zmienianiu haseł dostępu rzadziej niż co 30 dni. Pozytywnie natomiast należy ocenić sposób zabezpieczenia danych osobowych przetwarzanych przy użyciu systemów informatycznych służących do rozliczeń z Narodowym Funduszem Zdrowia. Jednak w tym przypadku o bezpieczeństwo przesyłanych danych pacjentów oraz o bezpieczeństwo danych potrzebnych do uwierzytelnienia użytkownika zadbał Narodowy Fundusz Zdrowia jako właściciel ww. systemów.

W pojedynczych przypadkach przeprowadzone kontrole wykazały także inne naruszenia przepisów o ochronie danych osobowych. Wskazane nieprawidłowości dotyczyły dopuszczenia do przetwarzania danych osób nieposiadających upoważnienia nadanego przez administratora danych oraz niewyznaczenia administratora bezpieczeństwa informacji.

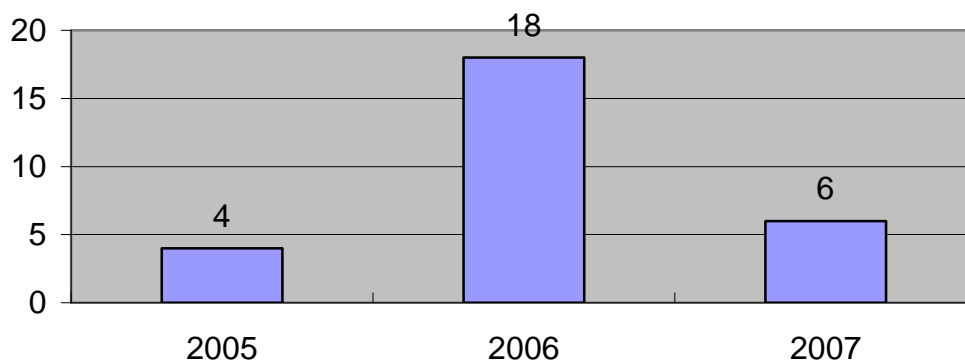
W związku ze stwierdzonymi w toku kontroli uchybieniami wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych przez jednostki kontrolowane w toku postępowania¹³.

5) Ubezpieczenia społeczne, majątkowe i osobowe

W 2007 r. w jednostkach organizacyjnych Zakładu Ubezpieczeń Społecznych, podmiotach prowadzących działalność w zakresie ubezpieczeń majątkowych i osobowych oraz towarzystwach emerytalnych przeprowadzonych zostało 6 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych¹⁴.

¹³ Np. decyzje: z dnia 12 listopada 2007 r. o sygn. DIS-DEC-111/421/07, z dnia 5 lipca 2007 r. o sygn. DIS-DEC-109/421/07, z dnia 5 października 2007 r. o sygn. DIS-DEC-108/421/07

¹⁴ Np. kontrole GI-DIS-K-411/66/07 i DIS-K-421/136/07



Wykres 4: ***Porównanie liczby kontroli przeprowadzonych w sektorze ubezpieczenia społeczne, majątkowe i osobowe w latach 2005–2007.***

Jedna z nich odbyła się w Zakładzie Ubezpieczeń Społecznych¹⁵. Jej celem było ustalenie zasad i legalności udostępniania danych osobowych Centralnemu Biuru Antykorupcyjnemu [dalej: CBA]. Kontrola wykazała, że na gruncie obowiązujących przepisów określających uprawnienia Centralnego Biura Antykorupcyjnego, Zakład Ubezpieczeń Społecznych ma obowiązek udostępnić wszelkie gromadzone i przetwarzane przez siebie informacje (w szczególności z Centralnego Rejestru Ubezpieczonych i Centralnego Rejestru Płatników Składek)¹⁶. Zakres, warunki i tryb przekazywania Centralnemu Biuru Antykorupcyjnemu ww. informacji zostały określone w przepisach rozporządzenia Prezesa Rady Ministrów z dnia 27 września 2006 r. w sprawie zakresu, warunków i trybu przekazywania Centralnemu Biuru Antykorupcyjnemu informacji przez organy, służby i instytucje państwowe (Dz. U. Nr 177, poz. 1310). Przepisy powołanego aktu wykonawczego wskazują zwłaszcza na możliwość przekazania danych na podstawie wniosków pisemnych lub przesłanych przez urządzenia i systemy informatyczne. Przy czym sposób udostępniania danych powinien wynikać z odrębnych porozumień zawartych z Centralnym Biurem Antykorupcyjnym.

W toku kontroli ustalono, że w dniu 3 września 2007 r., w trybie § 3 ww. rozporządzenia¹⁷, między Szefem Centralnego Biura Antykorupcyjnego a Prezesem Zakładu Ubezpieczeń Społecznych zawarte zostało porozumienie w sprawie określenia szczegółowych zasad przetwarzania przez Centralne Biuro Antykorupcyjne informacji, w tym danych osobowych stanowiących zawartość Kompleksowego Systemu Informatycznego. Porozumienie to dotyczyło sposobu udostępniania danych za pomocą systemu teleinformatycznego i odnosiło się tylko do kwestii udostępnienia stacji roboczych

¹⁵ Kontrola DIS-K-421/136/07

¹⁶ Patrz art. 22 ust. 2 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 z późn. zm.).

¹⁷ § 3: Podmioty, o których mowa w art. 22 ust. 2 ustawy, udostępniają za pomocą systemu teleinformatycznego zbiory, dane lub informacje jednostkom organizacyjnym CBA uprawnionym do wykonywania czynności operacyjno-rozpoznawczych lub ewidencyjnych lub archiwalnych w sposób określony w zawartych z CBA odrębnych porozumieniach.

wraz z oprogramowaniem i licencją w celu realizacji zadań związanych z bezpośrednim dostępem do zasobów Zakładu Ubezpieczeń Społecznych.

Z tego względu uznano, że wymienione porozumienie nie jest realizacją przepisu § 6 ust. 1 powołanego rozporządzenia.¹⁸ Oznacza to, że na jego mocy nie można przyjąć, iż została wyrażona zgoda na udostępnienia danych za pomocą urządzeń i systemów informatycznych bez konieczności każdorazowego składania wniosków.

6) Archiwa

W okresie sprawozdawczym w **archiwach państwowych** przeprowadzono 8 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych¹⁹. Ich zakresem objęto zabezpieczenie danych osobowych przetwarzanych przez te podmioty. W poprzednich latach kontrole w tej kategorii podmiotów nie były przeprowadzane.

Na osiem skontrolowanych jednostek archiwów państwowych uchybienia w procesie przetwarzania danych osobowych stwierdzono w czterech przypadkach. Najwięcej problemów przysparzało przetwarzanie danych osobowych przy użyciu systemów informatycznych. Uchybienia w tym zakresie dotyczyły m.in.:

- niezapewniania przez te systemy dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
- niezastosowania mechanizmów kontroli dostępu do danych,
- niezabezpieczenia systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

W pojedynczych przypadkach stwierdzono także nieprawidłowości polegające m.in. na niezawarceniu w polityce bezpieczeństwa wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, oraz na niezastosowaniu środków zabezpieczających dane przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Kontrole wykazały, że niektóre systemy informatyczne używane w archiwach państwowych zostały opracowane przez Centralny Ośrodek Informacji Archiwalnej przy Naczelnej Dyrekcji

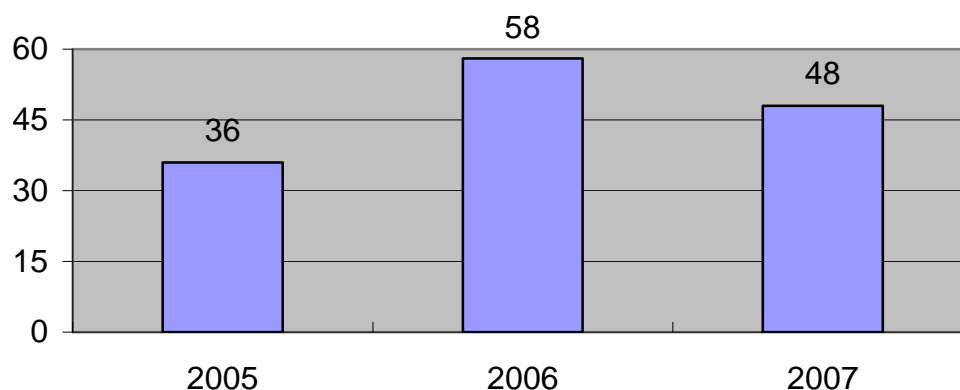
¹⁸ § 6 ust. 1: Podmioty, o których mowa w art. 22 ust. 2 ustawy, mogą, w drodze decyzji lub na mocy odrębnych porozumień, wyrazić zgodę na udostępnianie jednostkom organizacyjnym CBA zgromadzonych zbiorów, danych lub informacji za pomocą urządzeń i systemów informatycznych, bez konieczności każdorazowego składania pisemnych wniosków.

¹⁹ Np. kontrole DIS-K-421/147/07, DIS-K-421/162/07, DIS-K-421/163/07

Archiwów Państwowych, a ich stosowanie zostało nakazane wszystkim archiwom państwowym w Polsce, w tym m.in. system zawierający informacje o narodowym zasobie archiwalnym przechowywanym w archiwach państwowych oraz system służący do rejestracji osób, którym zostały udostępnione materiały archiwalne. Obsługa informatyczna tych ogólnopolskich systemów należy do zadań Centralnego Ośrodka Informacji Archiwalnej. Na podstawie ustaleń kontrolnych zaobserwowana została również tendencja do wymiany lub zastępowania przestarzałych systemów informatycznych nowymi zintegrowanymi platformami systemowymi, podwyższającymi poziom zabezpieczenia danych osobowych.

7) Inne

W okresie sprawozdawczym w podmiotach nienależących do sektorów omówionych w poprzednich rozdziałach przeprowadzono 48 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych²⁰. Grupa tych podmiotów była bardzo zróżnicowana i obejmowała m.in. podmioty wykonujące działalność gospodarczą w zakresie transportu drogowego oraz podmioty zajmujące się produkcją i handlem.



Wykres 5: *Porównanie liczby kontroli przeprowadzonych w podmiotach należących do sektora inne w latach 2005–2007.*

Analizując wyniki kontroli należy stwierdzić, że jednostki kontrolowane najwięcej problemów miały z prawidłowym wykonaniem podstawowych obowiązków wynikających z przepisów o ochronie danych osobowych. Uchybienia w tym zakresie dotyczyły zwłaszcza: niedopełnienia wobec osób, których dane dotyczą, obowiązku informacyjnego wynikającego z art. 24 ust. 1 ustawy o ochronie danych osobowych²¹, niezgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych

²⁰ Np. kontrole GI-DIS-K-411/1/07, GI-DIS-K-411/31/07 i GI-DIS-K-411/57/07

²¹ Art. 24. 1: W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców

Osobowych prowadzonych zbiorów danych osobowych (np. zbioru danych osobowych klientów) oraz zbierania w szerszym zakresie danych osobowych pracowników (m.in. o nazwisko rodowe matki) niż wynikało to z przepisów art. 22¹ § 1, § 2 i § 4 Kodeksu pracy²². Kontrole wykazały również inne nieprawidłowości w procesie przetwarzania danych osobowych, takie jak brak ewidencji osób upoważnionych do przetwarzania danych osobowych oraz polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych lub niezawarcie w ww. dokumentach wszystkich wymaganych informacji, określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych²³ oraz § 4 i § 5 rozporządzenia ministra spraw wewnętrznych i administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych²⁴.

Krytycznie należy ocenić także sposób wykonania obowiązków związanych z przetwarzaniem danych przy użyciu systemów informatycznych. Nieprawidłowości dotyczyły przede wszystkim niespełniania przez te systemy wszystkich wymogów o charakterze technicznym.

danych, 3) prawie dostępu do treści swoich danych oraz ich poprawiania, 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

²² Art. 22¹ § 1: 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. § 2. 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). § 4. Pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

²³ 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.

²⁴ § 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 Generalny Inspektor Ochrony Danych Osobowych wydał stosowne decyzje nakazujące ich usunięcie, bądź umarzające postępowanie w zakresie nieprawidłowości usuniętych w toku postępowania.²⁵

Jedną z bardziej interesujących była kontrola podmiotu zajmującego się badaniem rynku i opinii publicznej²⁶. W czasie jej trwania ustalono, że kontrolowany podmiot w związku z wykonywaniem swojej działalności zawierał umowy ramowe lub jednorazowe z administratorami danych dotyczące przeprowadzania badań rynku i opinii publicznej. W zależności od metody przeprowadzanego badania, administrator danych przekazywał posiadane przez siebie zbiory danych osobowych respondentów, tj. swoich klientów lub pracowników, a kontrolowana jednostka przetwarzała je na podstawie umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 ustawy o ochronie danych osobowych²⁷. Ustalono jednak, że wskazany podmiot przekazywał bazy danych przesłane przez administratorów danych do działu realizacji badań znajdującego się w podmiocie trzecim współpracującym z jednostką kontrolowaną na podstawie umowy o współpracy. Podmiot ten po przeprowadzeniu badań zwracał bazy danych do kontrolowanej jednostki, gdzie były one niszczone lub przekazywane administratorowi danych.

Analiza umów powierzenia przetwarzania danych zawartych między kontrolowaną jednostką a administratorami danych wykazała, że podmiot ten nie miał uprawnienia do udostępniania danych osobowych klientów administratorów danych podmiotom trzecim. Jednocześnie na podstawie ustaleń poczynionych w toku kontroli przeprowadzonych u wybranych administratorów danych współpracujących z poddanym kontroli podmiotem stwierdzono, że nie posiadali oni wiedzy na temat współpracy, jaką podejmuje kontrolowana jednostka z podmiotem trzecim – dysponowali jedynie wiedzą ogólną, że podmiot ten współpracuje z podmiotami zależnymi w zakresie przeprowadzania badań rynku i opinii publicznej. W związku z tym uznano, że poddany kontroli podmiot zajmujący się badaniem rynku i opinii publicznej, przekazując dane osobowe do podmiotu trzeciego bez zgody administratorów danych, udostępnił je osobom nieupoważnionym. Ponadto ustalono, iż administratorzy danych, mimo, iż wiedzieli, że kontrolowana jednostka współpracuje z podmiotami zależnymi, nie podjęli działań zmierzających do ustalenia komu, kiedy, na jakich zasadach i na jakiej podstawie prawnej dane są udostępniane i nie dołożyli szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, np. poprzez uregulowanie ww. kwestii w umowie powierzenia przetwarzania danych osobowych.

²⁵ Np. decyzje: z dnia 20 lipca 2007 r. o sygn. GI-DEC-DIS-48/07 i z dnia 23 listopada 2007 r. o sygn. DIS-DEC-122/421/07

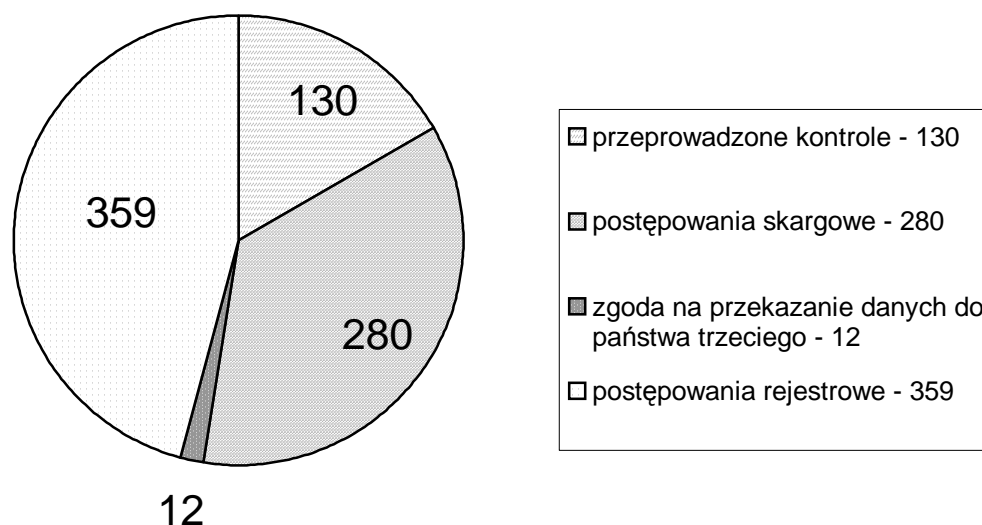
²⁶ kontrola GI-DIS-K-411/22/07

²⁷ Art. 31 ust. 1: W drodze umowy zawartej na piśmie administrator danych może powierzyć innemu podmiotowi przetwarzanie danych.

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 poprzez usunięcie uchybień, uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie albo usunięcie danych osobowych, zastosowanie dodatkowych środków zabezpieczających zgromadzone dane, wstrzymanie przekazania ich za granicę, zabezpieczenie danych lub przekazanie ich innym podmiotom.

W 2007 r. Generalny Inspektor wydał 781 decyzji administracyjnych, w tym 359 dotyczyło postępowań rejestrowych, 130 zostało wydanych w związku z przeprowadzonymi kontrolami, 280 wydano na skutek postępowania zainicjowanego skargą, zaś 12 dotyczyło zgody na przekazanie danych do państwa trzeciego.



Wykres 6: Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2007 r.

W analizowanym roku sprawozdawczym 2007 Generalny Inspektor Ochrony Danych Osobowych skierował do organu powołanego do ścigania przestępstw 18 zawiadomień o popełnieniu przestępstwa.

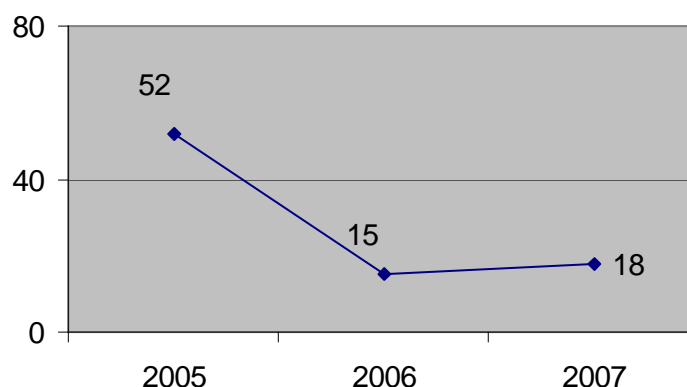
Jak co roku, najwięcej zawiadomień o popełnieniu przestępstwa złożonych zostało w związku z postępowaniami prowadzonymi na skutek skarg wniesionych do Generalnego Inspektora (15).

Najwięcej z nich (8) dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego, zagrożonego karą określoną w art. 49 ust. 1 ustawy o ochronie danych osobowych, przestępstwa przetwarzania danych osobowych bez podstawy prawnej. Ponadto GODO stwierdził 5 przypadków udostępnienia danych osobowych podmiotom nieuprawnionym. W związku z tym do organów ścigania skierowano zawiadomienia o podejrzeniu popełnienia przestępstwa z art. 51 ust. 1 ustawy. Podobnie jak w latach ubiegłych przeważająca część zawiadomień dotyczyła przetwarzania danych osobowych przez podmioty prowadzące sprzedaż produktów i usług w tzw. systemie wysyłkowym. Podmioty takie, bądź to w sposób nieuprawniony (bez spełnienia jednej z przesłanek z art. 23 ust. 1 ustawy) udostępniały dane osobowe innym podmiotom również prowadzącym tego typu działalność, bądź nie potrafiły w sposób wiarygodny i jednoznaczny udowodnić przed GODO legalności źródła, z którego dane pozyskano. W pozostałych przypadkach przedmiotem zawiadomień uczyniono podejrzenie popełnienia przestępstwa niezgłoszenia do rejestracji zbioru danych osobowych (art. 53 ustawy) oraz niedopełnienia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej ustawą o ochronie danych osobowych (art. 54 ustawy).

Natomiast przedmiotem pozostałych 3 zawiadomień o popełnieniu przestępstwa było naruszenie przez podmioty kontrolowane przepisów art. 40, art. 36 ust. 3, art. 37, art. 39 ust. 1 ustawy, a także §§ 4 i 5 rozporządzenia 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 oraz pkt IV ust. 2, pkt VIII załącznika do tego rozporządzenia, co stanowiło wypełnienie znamion przestępstw określonych w art. 51 i art. 53 ustawy o ochronie danych osobowych. W zawiadomieniach wskazano m.in., iż podmioty poddane kontroli uporczywie uniemożliwiały prawidłowe przeprowadzenie czynności kontrolnych. W dwóch przypadkach prokuratura wszczęła śledztwo, a następnie umorzyła je wobec braku znamion przestępstwa. W pozostałym przypadku dochodzenie zostało umorzone ze względu na brak znamion czynu zabronionego.

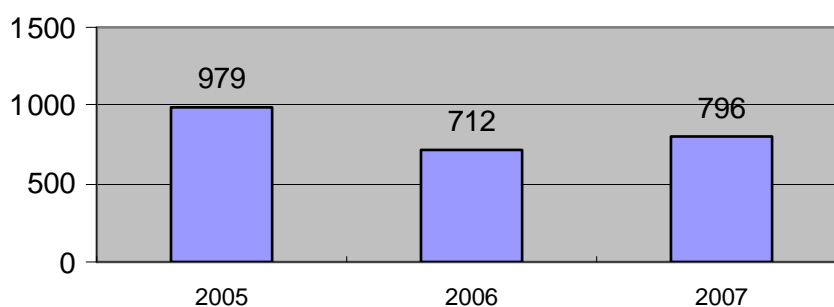
Nadmienić zarazem należy, że w porównaniu z rokiem 2006 liczba spraw, w których organ skierował zawiadomienia o podejrzeniu popełnienia przestępstwa, utrzymuje się prawie na tym samym poziomie. Potwierdza to niewątpliwie skuteczność dotychczasowych działań organu w zakresie propagowania przestrzegania przepisów o ochronie danych osobowych.

Liczbę **zawiadomień o popełnieniu przestępstwa** składanych przez Generalnego Inspektora w latach 2005–2007 obrazuje Wykres 7:



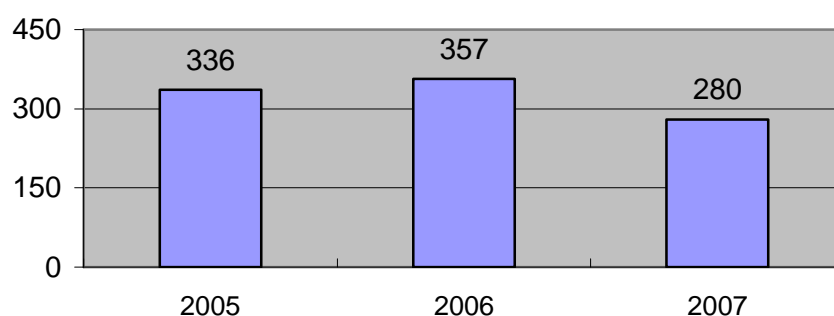
Wykres 7: *Porównanie liczby zawiadomień o popełnieniu przestępstwa składanych przez GIODO w latach 2005–2007.*

W 2007 r. do Departamentu Orzecznictwa, Legislacji i Skarg wpłynęło **796 skarg** dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2006, liczba ta uległa zwiększeniu, co przedstawia Wykres 8.



Wykres 8: *Liczbowe zestawienie skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2005–2007.*

W postępowaniach zainicjowanych tymi skargami wydanych zostało 280 decyzji administracyjnych; z których 58 zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie [dalej: WSA] (zob. Wykres 9).



Wykres 9: Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2005–2007 w związku z rozpatrywanymi skargami.

Każda z wpływających do Biura Generalnego Inspektora Ochrony Danych Osobowych skarg analizowana była na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego. W przypadku tych, które je spełniały, GODO inicjował postępowania administracyjne. Jeżeli w ich toku stwierdzał naruszenie przepisów ustawy o ochronie danych osobowych, wydawał decyzje administracyjne i zgodnie z art. 18 ustawy nakazywał przywrócenie stanu zgodnego z prawem, a w szczególności – zgodnie z ww. artykułem: 1) usunięcie uchybień, 2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych, 3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe, 4) wstrzymanie przekazywania danych osobowych do państwa trzeciego, 5) zabezpieczenie danych lub przekazanie ich innym podmiotom, 6) usunięcie danych osobowych.

Zakres podmiotowy skarg kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w 2007 roku obejmował następujące obszary: 1) administracja publiczna, 2) bezpieczeństwo publiczne, 3) banki i inne instytucje finansowe, 4) sądy, organy prokuratury, komornicy, 5) marketing, 6) sektor mieszkalnictwa, 7) sektor ubezpieczeń, 8) telekomunikacja, 9) sektor zatrudnienia i 10) inne.

1) Administracja publiczna

Wśród skarg dotyczących organów administracji publicznej, które GODO rozpatrzył w 2007 r., najczęściej odnotowywane były zarzuty udostępnienia danych osobowych osobom (podmiotom) nieuprawnionym oraz wykorzystywanie danych osobowych pozyskanych w toku prowadzonego postępowania administracyjnego w innych celach niż na jego potrzeby²⁸. Nadmienić jednak należy, że w analizowanym okresie sprawozdawczym w tym sektorze odnotowano znaczny spadek skarg zasadnych.

GODO badał, np. sprawę upublicznienia na stronach internetowych urzędu gminy, bez zgody osoby, której dane dotyczą, informacji o zwolnieniu jej z podatku od nieruchomości wraz z takimi danymi, jak: imię, nazwisko oraz adres zamieszkania. Organ ds. ochrony danych uznał w tym przypadku, że upublicznienie było zgodne z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

²⁸ Np.: GI-DOLiS-430/43/07; GI-DOLiS-430/88/07; GI-DOLiS-430/245/07; GI-DOLiS-430/357/07; GI-DOLiS-430/364/07, GI-DOLiS-430/357/07

Podstawą prawną takiego działania był bowiem art. 14 pkt 2 lit. e w zw. z art. 15 ust. 2 ustawy o finansach publicznych²⁹.

Generalny Inspektor analizował również sprawę upublicznienia na stronie internetowej Biuletynu Informacji Publicznej [dalej: BIP] jednego z urzędów publicznych informacji o treści uchwały rady gminy zawierającej takie dane osobowe, jak: imię, nazwisko oraz adres zamieszkania osoby, której ta uchwała dotyczyła. W tym przypadku³⁰ organ ds. ochrony danych osobowych uznał, iż samo upublicznianie na stronie BIP danych osobowych w związku z informowaniem o podjętej uchwale jest dopuszczalne jako realizacja prawa obywateli dostępu do informacji publicznej, jednak tylko w zakresie imienia i nazwiska. Ujawnianie dodatkowo adresu zamieszkania jest sprzeczne z zasadą adekwatności wynikającą z ustawy o ochronie danych osobowych³¹ oraz prowadzi do naruszenia prywatności tej osoby, i jako takie może stanowić naruszenie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej³². W związku z tym GODO nakazał usunięcie danych osobowych ze strony internetowej BIP w zakresie adresu zamieszkania osoby skarżącej³³.

Z kolei w sprawie, w której przedmiotem było żądanie usunięcia z treści uzasadnienia decyzji administracyjnej wydanej przez Prezydenta Miasta W. (a więc z konkretnego aktu administracyjnego) usunięcia imienia i nazwiska osoby skarżącej, GODO uznał, że jako organ ds. ochrony danych nie ma ustawowych kompetencji do tego typu ingerencji. Powyższe stanowisko znalazło potwierdzenie w orzeczeniu WSA w Warszawie, w którym wskazano, że „organ (...) zasadnie uznał, iż nie jest uprawniony do ingerencji w rozstrzygnięcie innego organu, a takim byłoby zobowiązanie go do usunięcia danych osobowych skarżącego z uzasadnienia decyzji Prezydenta Miasta W.”³⁴.

Wspomnieć tu należy również o sprawie dotyczącej przetwarzania danych osobowych uczniów pochodzenia romskiego przez Prezydenta Miasta L.³⁵. Podmiot ten gromadził dane osobowe uczniów tamtejszych szkół pochodzenia romskiego w zakresie imienia, nazwiska, klasy, rodzaju sytuacji problemowej oraz formy udzielonej pomocy. Pozyskane informacje miały służyć realizacji przygotowanego przez Ministerstwo Spraw Wewnętrznych i Administracji „Programu na rzecz

²⁹ Zgodnie z art. 14 pkt 2 lit. e ustawy z dnia 30 czerwca 2005 r. o finansach publicznych (Dz. U. Nr 249, poz. 2104 z późn. zm.), zarząd jednostki samorządu terytorialnego podaje do publicznej wiadomości w terminie, o którym mowa w art. 15 ust. 2, informację obejmującą wykaz osób prawnych i fizycznych oraz jednostek organizacyjnych nieposiadających osobowości prawnej, którym w zakresie podatków lub opłat udzielono ulg, odroczeń, umorzeń lub rozłożono spłatę na raty w kwocie przewyższającej 500 zł, wraz ze wskazaniem wysokości umorzonych kwot i przyczyn umorzenia.

³⁰ GI-DOLiS-430/22/06

³¹ Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dolożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

³² Zgodnie z art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2001. Nr 112, poz. 1198 z późn. zm.), prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

³³ Decyzja z dnia 10 sierpnia 2007 r. o sygn. GI-DEC-DOLiS-174/07/4607,4608

³⁴ Wyrok z dnia 22 sierpnia 2007 r. (sygn. akt II SA/Wa 793/07)

społeczności romskiej w Polsce”, zaś podstawą prawną takiego pozyskiwania danych miał być § 1 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 3 grudnia 2002 r. w sprawie warunków i sposobu wykonywania przez szkoły i placówki publiczne zadań umożliwiających podtrzymywanie poczucia tożsamości narodowej, etnicznej, językowej i religijnej uczniów należących do mniejszości narodowych i grup etnicznych³⁶ oraz art. 34a ust. 3 w zw. z art. 33 ust. 3 pkt 2 ustawy o systemie oświaty³⁷. GODO uznał, że w tym przypadku, po pierwsze, żaden z przywołanych przepisów nie daje Prezydentowi Miasta L. prawa gromadzenia takich danych szczególnie chronionych, a po drugie – odnośnie do powoływania się na przepisy ww. rozporządzenia – stosownie do art. 27 ust. 2 pkt 2 ustawy³⁸ - niezbędna do przetwarzania takich danych jest podstawa prawna rangi ustawowej, a nie przepisy aktów wykonawczych do ustaw. W związku z tym GODO nakazał ww. organowi usunięcie z posiadanych zbiorów danych osobowych uczniów pochodzenia romskiego pozyskanych w związku z realizacją przygotowanego przez Ministerstwo Spraw Wewnętrznych i Administracji „Programu na rzecz społeczności romskiej w Polsce”³⁹.

Co do przetwarzania danych szczególnie chronionych warto również wspomnieć, że w 2007 r. Generalny Inspektor Ochrony Danych Osobowych interweniował w sprawie przetwarzania (gromadzenia) w celach statystycznych przez Ministerstwo Spraw Wewnętrznych i Administracji danych osobowych ujawniających pochodzenie etniczne kandydatów w wyborach samorządowych przeprowadzonych w listopadzie 2006 r. Kandydaci związani byli ze środowiskiem mniejszości narodowych, etnicznych oraz mniejszości posługujących się językiem regionalnym i ubiegali się o mandaty z list komitetów wyborczych. Przedstawiciel MSWiA wskazał, że pozyskiwano jedynie ogólnie dostępne dane osobowe ujawniające pochodzenie etniczne, a jawność tych informacji miała wynikać z publicznej wiedzy o tym, że poszczególni kandydaci są zgłoszeni przez komitety wyborcze zarejestrowane przez organizacje mniejszości narodowych i etnicznych oraz społeczności posługujące się językiem regionalnym. GODO ustalił jednak, że MSWiA pozyskiwało nie tylko dane osobowe kandydatów zgłoszonych przez takie komitety – które to dane niewątpliwie mają charakter jawny - ale również informacje o kandydatach związanych, co prawda, że

³⁵ GI-DOLiS-430/41/07

³⁶ Zgodnie z § 1 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 3 grudnia 2002 r. w sprawie warunków i sposobu wykonywania przez szkoły i placówki publiczne zadań umożliwiających podtrzymywanie poczucia tożsamości narodowej, etnicznej, językowej i religijnej uczniów należących do mniejszości narodowych i grup etnicznych (Dz. U. Nr 220, poz. 1853), szkoły i placówki publiczne umożliwiają uczniom należącym do mniejszości narodowych i grup etnicznych podtrzymywanie i rozwijanie poczucia tożsamości narodowej, etnicznej, językowej i religijnej oraz własnej historii i kultury poprzez: 1) naukę języka mniejszości narodowej lub grupy etnicznej; 2) naukę historii, geografii i kultury kraju pochodzenia mniejszości narodowej; 3) prowadzenie zajęć artystycznych lub innych dodatkowych zajęć.

³⁷ Zgodnie z art. 33 ust. 3 pkt 2 ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.), nauczyciele, o których mowa w art. 35 ust. 5, wykonujący czynności z zakresu nadzoru pedagogicznego mają prawo wglądu do prowadzonej przez szkołę lub placówkę dokumentacji dotyczącej przebiegu nauczania, wychowania i opieki oraz organizacji pracy.

³⁸ Zgodnie z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych, o których mowa w ust. 1 (szczególnie chronionych), jest dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

³⁹ Decyzja z dnia 12 października 2007 r. o sygn. GI-DEC-DOLiS-218/07/5787, 5788

środowiskami mniejszościowymi, ale ubiegających się o mandaty z list zgłoszonych przez inne komitety, tj. niezarejestrowane przez organizacje mniejszości narodowych i etnicznych oraz społeczności posługujące się językiem regionalnym. GODO stwierdził w tej sprawie, że gromadzenie tych szczególnie chronionych danych osobowych nie znajduje uzasadnienia w art. 27 ustawy i w związku z tym zwrócił się do Ministra Spraw Wewnętrznych i Administracji o podjęcie działań mających na celu zaprzestanie ich przetwarzania⁴⁰.

W innej z badanych spraw pracownik jednostki organizacyjnej gminy zakwestionował legalność udostępnienia jego danych osobowych przez dyrektora tej jednostki radcy prawnemu, który nie był pracownikiem tej jednostki i nie był – zdaniem osoby kierującej do GODO skargę – osobą upoważnioną do dostępu do dokumentów zawierających jej dane⁴¹. Dokumentacja z danymi osobowymi miała być przekazana w celu dokonania przez wspomnianego radcę prawnego opinii prawnej. Po przeprowadzeniu postępowania wyjaśniającego organ uznał, że nie doszło do naruszenia ustawy o ochronie danych osobowych. Ustalono, że dyrektor jednostki - stanowiącej jednostkę organizacyjną gminy - po zapoznaniu się z dokumentami z akt osobowych osoby skarżącej, dotyczących jej uprawnienia do otrzymania nagrody jubileuszowej, powziął wątpliwości w tym zakresie i dlatego zwrócił się do komórki prawnej urzędu o wydanie w tej sprawie opinii prawnej. W tym celu udostępnił dokumentację z danymi osobowymi osoby skarżącej radcy prawnemu, który był zatrudniony w tym urzędzie. GODO ocenił powyższe działanie pracodawcy jako nierozważnie związane ze świadczeniem przez osobę skarżącą pracy i znajdujące uzasadnienie zarówno w przepisach Kodeksu pracy⁴², jak i ustawy o samorządzie gminnym⁴³, a w konsekwencji, jako zgodne z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Ocenie organu poddany był również przypadek udostępnienia przez Burmistrza Miasta B. danych osobowych osoby małoletniej jej ojcu, który nie pozostawał już w związku małżeńskim z matką dziecka. W ten sposób osoba ta pozyskała informację o aktualnym adresie zamieszkania zarówno dziecka, jak i byłej żony, czego ta ostatnia sobie nie życzyła. GODO ustalił, że udostępnienie wspomnianych danych ze zbioru meldunkowego odbyło się bez zgody matki, tj. przedstawiciela ustawowego osoby, której dane dotyczyły⁴⁴. W tym przypadku, udostępniając te dane, nie wzięto pod uwagę treści art. 44h ust. 2 pkt 4 ustawy o ewidencji ludności i dowodach osobistych⁴⁵, z którego wynika, że przesłanką decydującą o udostępnieniu danych jest zgoda osoby, której dane dotyczą (w

⁴⁰ Pismo z dnia 23 listopada 2007 r. o sygn. GI-DOLiS-430/103/07/6592

⁴¹ GI-DOLiS-430/167/07

⁴² Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.)

⁴³ Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.)

⁴⁴ GI-DOLiS-430/21/06

⁴⁵ Zgodnie z art. 44h ust. 2 pkt 4 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.), dane ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych, mogą być udostępnione osobom i podmiotom – jeżeli uwiarygodnią one interes faktyczny w otrzymaniu danych i za zgodą osób, których dane dotyczą.

tym przypadku przedstawiciela ustawowego, którym była matka). W badanej sprawie Burmistrz Miasta B. taką zgodą nie dysponował. Wobec tych okoliczności GODO zwrócił się do niego o podjęcie odpowiednich działań techniczno–organizacyjnych przy weryfikowaniu wniosków o udostępnienie danych osobowych ze zbiorów meldunkowych Urzędu Miasta w B., mających na celu wyeliminowanie tego typu przypadków w przyszłości⁴⁶. W odpowiedzi na to wystąpienie GODO został poinformowany przez Burmistrza Miasta B., iż w przypadku wniosku o udostępnienie danych pochodzącego od osoby fizycznej będzie wymagał zgody osoby, której dane dotyczą, bądź zgody sądu⁴⁷.

Podsumowując analizę działalności organu ochrony danych osobowych w sektorze „**administracja publiczna**”, należy podkreślić, że treść skarg kierowanych do GODO świadczy o tym, iż główną przyczyną inicjowania postępowania skargowego było błędne przekonanie po stronie osób skarżących, iż brak ich zgody na przetwarzanie danych osobowych jest okolicznością wykluczającą legalność takiego przetwarzania. Często w toku postępowań okazywało się, że podstawą prawną przetwarzania konkretnych danych były inne, aniżeli zgoda osoby zainteresowanej, przesłanki legalnego przetwarzania danych z art. 23 ust. 1 ustawy o ochronie danych osobowych⁴⁸. Dodać również trzeba, że na podstawie analizy treści skarg rozpatrywanych w 2007 r. odnotowano nie tylko systematyczny wzrost wśród pracowników administracji publicznej świadomości obowiązywania w porządku prawnym ustawy o ochronie danych osobowych, ale również jej właściwe stosowanie oraz jednocześnie zanik przypadków nieuzasadnionego wykorzystywania tych uregulowań jako przeszkody w bezzwłocznym załatwieniu konkretnej sprawy administracyjnej.

2) Bezpieczeństwo publiczne

W 2007 r. Generalny Inspektor Ochrony Danych Osobowych rozpatrywał kilka spraw dotyczących tego sektora. Zarzuty dotyczące nieprawidłowości w procesie przetwarzania danych osobowych przez **Policję** dotyczyły głównie bezprawnego – zdaniem osób skarżących – udostępnienia ich danych osobowych z akt prowadzonego postępowania osobom nieuprawnionym⁴⁹. W prowadzonych w tym zakresie postępowaniach organ nie stwierdzał jednak podstaw do wydania rozstrzygnięcia, w którym musiałby nakazywać przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych. W każdym z analizowanych przypadków przetwarzanie danych osobowych przez Policję znajdowało uzasadnienie w przepisach prawa i tym samym wypełniało przesłankę z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Zarówno pozyskiwanie przez Policję danych osobowych, jak i ich udostępnianie przez ten

⁴⁶ Pismo z dnia 16 kwietnia 2007 r. o sygn. GI-DOLiS-430/21/06/2290/07

⁴⁷ Pismo z dnia 27 kwietnia 2007 r. o sygn. OP.0517-86/06

⁴⁸ Najczęściej przesłanką znajdującą zastosowanie w działaniach organów administracji publicznej był art. 23 ust. 1 pkt 2 ustawy (realizacja uprawnień lub spełnienie obowiązku wynikającego z przepisu prawa).

⁴⁹ Np. GI-DOLiS-430/136/07

podmiot, dokonywane było na potrzeby prowadzonych przez Policję postępowań i na podstawie odpowiednich przepisów prawa, tj. Kodeksu postępowania karnego⁵⁰ oraz ustawy o Policji⁵¹.

Omawiając sprawy dotyczące tego sektora, warto również wskazać badaną przez GODO skargę na odmowę udostępnienia przez Policję dokumentów zawartych w aktach prowadzonego przez nią postępowania pełnomocnikowi pokrzywdzonego, dla którego były one niezbędne w celu sporządzenia prywatnego aktu oskarżenia⁵². W tej sprawie GODO zwrócił uwagę osobie skarżącej, że pojęcie przetwarzania danych obejmuje wszelkie czynności mające za przedmiot dane osobowe, nie zaś nośniki, na których dane te zostały utrwalone (w tym dokumenty, ich kserokopie itp.)⁵³. GODO powołał się tu zwłaszcza na art. 29 ustawy o ochronie danych osobowych⁵⁴, który określa warunki pozyskania danych osobowych (a nie ich nośników) w celach innych, niż włączenie ich do zbioru. Zasadniczym warunkiem pozyskania danych w tym trybie jest złożenie odpowiedniego, umotywowanego wniosku zawierającego elementy określone w art. 29 ust. 3 ustawy. Dopiero po złożeniu takiego wniosku i ewentualnej negatywnej odpowiedzi administratora danych (w tej sprawie był nim Komendant Miejski Policji), takie działanie może zostać poddane kontroli GODO. W związku z tym, że w omawianej sprawie osoba skarżąca nie wykazała, że chodzi jej o pozyskanie jedynie danych osobowych, a nie ich nośników (dokumentów) oraz nie wskazała, że zwróciła się o udostępnienie danych w trybie przewidzianym w art. 29 ustawy o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych ustosunkował się do wspomnianej skargi negatywnie.

W analizowanym okresie GODO badał również sprawę pozyskania przez Centralne Biuro Antykorupcyjne danych osobowych zawartych w dokumentacji medycznej pacjentów Centralnego Szpitala Klinicznego MSWiA w Warszawie⁵⁵. Dokonawszy analizy prawnej tej sprawy, organ stwierdził, iż zabezpieczenie przez CBA dokumentacji medycznej nastąpiło na podstawie art. 217 Kodeksu postępowania karnego⁵⁶, na mocy postanowienia Prokuratora Prokuratury Okręgowej w Warszawie⁵⁷ oraz

⁵⁰ Zgodnie z 15 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89, poz. 555 z późn. zm.), wszystkie instytucje państwowe i samorządowe są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne w terminie wyznaczonym przez te organy.

⁵¹ Zgodnie z art. 14 ust. 1 pkt 4 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.), Policja w celu realizacji ustawowych zadań może korzystać z danych o osobie, w tym również w formie zapisu elektronicznego, uzyskanych przez inne organy, służby i instytucje państwowe w wyniku wykonywania czynności operacyjno-rozpoznawczych oraz przetwarzać je w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), bez wiedzy i zgody osoby, której dane te dotyczą.

⁵² GI-DOLiS-430/430/07

⁵³ Pismo z dnia 26 lipca 2007 r. o sygn. GI-DOLiS-43-/430/07/4268

⁵⁴ Zgodnie z art. 29 ustawy o ochronie danych osobowych, dane osobowe z wyłączeniem danych, o których mowa w art. 27 ust. 1, mogą być udostępnione, jeżeli w sposób wiarygodny wnioskodawca uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

⁵⁵ GI-DOLiS-430/388/07

⁵⁶ Zgodnie z art. 217 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.), rzeczy mogące stanowić dowód w sprawie lub podlegające zajęciu w celu zabezpieczenia kar majątkowych, środków karnych o charakterze majątkowym albo roszczeń o naprawienie szkody, należy wydać na żądanie sądu lub prokuratora, a w wypadkach niecierpiących zwłoki - także na żądanie Policji lub innego uprawnionego organu.

w trybie odrębnych przepisów, tj. na podstawie ustawy o Centralnym Biurze Antykorupcyjnym⁵⁸ i w związku z tym nie stwierdzono naruszenia ustawy o ochronie danych osobowych.

W jednej z otrzymanych przez organ skarg zakwestionowano zakres danych osobowych pozyskiwanych przez **Straż Miejską** za pomocą formularza - oświadczenia o wyrażeniu zgody na przyjęcie grzywny w drodze mandatu karnego za popełnienie wykroczenia polegającego na przekroczeniu dozwolonej prędkości. Osoba skarżąca wskazała, że pozyskanie danych osobowych wychodzących poza informacje o imieniu i nazwisku oraz adresie zamieszkania, tj. nazwiska rodzowego, imion rodziców, numeru telefonu kontaktowego i informacji o dokumencie uprawniającym do kierowania pojazdu, stanowi naruszenie przepisów ustawy o ochronie danych osobowych⁵⁹. Po dokonaniu analizy stanu prawnego dotyczącego przedmiotowej sprawy organ uznał jednak, iż zarzuty nielegalnego przetwarzania (pozyskiwania) danych osobowych przez ten podmiot są bezpodstawne. Prawo do przetwarzania danych osobowych przez Straże Miejskie w powyższym zakresie, wynika bowiem z przepisów ustawy o strażach gminnych⁶⁰.

Podsumowując ten wątek sprawozdania należy podkreślić, że Generalny Inspektor Ochrony Danych Osobowych odnotowuje systematyczny spadek zasadnych skarg odnoszących się do sektora „**bezpieczeństwo publiczne**”. Przyczyn tego zjawiska należy upatrywać – z jednej strony – w ścisłej współpracy GIODO z Komendą Główną Policji w zakresie propagowania zasad przetwarzania danych osobowych w działalności tej instytucji, z drugiej zaś – w często spotykanej w analizowanych sprawach błędnej interpretacji przez strony postępowań, obowiązujących procedur regulujących te postępowania, na podstawie których działają administratorzy z tego sektora.

3) Banki i inne instytucje finansowe

Przedmiotem skarg rozpatrywanych przez Generalnego Inspektora Ochrony Danych Osobowych w tej dziedzinie była głównie kwestia legalności udostępnienia przez banki bądź inne instytucje upoważnione do udzielania kredytów danych osobowych byłych kredytobiorców (będących osobami fizycznymi) do Biura Informacji Kredytowej S.A. [dalej: BIK S.A.] oraz do Związku Banków Polskich [dalej: ZBP] bez zgody zainteresowanego i przetwarzania danych bez tejże zgody po wygaśnięciu zobowiązania kredytowego⁶¹. W tego rodzaju sprawach GIODO reprezentował stanowisko, iż dane

⁵⁷ Postanowienie z dnia 11 lutego 2007 r. (sygn. akt VI Ds. 185/06)

⁵⁸ Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 z późn. zm.)

⁵⁹ GI-DOLiS-430/76/07

⁶⁰ Zgodnie z art. 10a pkt 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779 z późn. zm.), straż w celu realizacji ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia.

⁶¹ Np.: GI-DOLiS-430/10/07, GI-DOLiS-430/75/07

osobowe kredytobiorcy, który nie przekroczył 60-dniowego terminu w spełnieniu zobowiązania wobec banku bądź instytucji finansowej upoważnionej do udzielania kredytów, i który nie udzielił zgody na przekazanie swoich danych osobowych do BIK S.A. bądź ZBP, nie powinny być udostępniane tym instytucjom. Natomiast dane już figurujące w bazach danych tych podmiotów powinny zostać usunięte⁶². Nie zachodzą bowiem w takim przypadku przesłanki do zastosowania regulującego tę kwestię przepisu art. 105a ust. 2 i 3 Prawa bankowego⁶³. Odmienne organ oceniał sprawy, w których doszło do nieterminowego spełnienia świadczenia (opóźnienia powyżej 60 dni). W takim przypadku, biorąc pod uwagę wspomniane regulacje Prawa bankowego, GODO stwierdzał, iż nawet mimo braku zgody osoby, której dane dotyczyły, udostępnienie danych do BIK S.A. bądź ZBP było zgodne z ustawą o ochronie danych osobowych, jako dokonane na podstawie art. 105a ust. 3 Prawa bankowego. Zasadność stanowiska organu w tym zakresie potwierdzane było w orzecznictwie WSA w Warszawie⁶⁴. Nadmienić przy tym należy, że przetwarzanie danych przez banki bądź inne instytucje upoważnione do udzielania kredytów oraz BIK S.A. i ZBP, zgodnie z art. 105a ust. 5 Prawa bankowego, ograniczone zostało przez ustawodawcę do lat 5, licząc od chwili wygaśnięcia zobowiązania.

Warto dodać, że przy rozpatrywaniu tego typu spraw pojawiał się - odnotowany również w poprzednim roku sprawozdawczym - problem interpretacji ustawowego okresu przejściowego⁶⁵ dla zastosowania wprowadzonych w życie nowych przepisów Prawa bankowego. Nakładają one na banki obowiązek spełnienia ściśle określonych przesłanek w przypadku przetwarzania danych osobowych rzetelnych i nierzetelnych klientów po wygaśnięciu łączących ich z bankami zobowiązań. W 2007 r. Generalny Inspektor Ochrony Danych Osobowych w dalszym ciągu reprezentował wobec administratorów danych z tego sektora stanowisko potwierdzone przez WSA w Warszawie⁶⁶, iż przepis ten nie może być traktowany jako regulacja dająca prawo do przetwarzania danych osobowych osób terminowo

⁶² Decyzja z dnia 20 lipca 2007 r. o sygn. GI-DEC-DOLiS-162/07

⁶³ Zgodnie z art. 105a ust. 2 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. 2002 r. Nr 72, poz. 665 z późn. zm.), 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. 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 ustawowo upoważnioną do udzielania kredytów o zamiarze przetwarzania dotyczących jej informacji stanowiących tajemnicę bankową, bez jej zgody.

⁶⁴ Wyrok z dnia 15 lutego 2007 r. (sygn. akt II SA/Wa 2064/06)

⁶⁵ 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.

⁶⁶ Wyrok z dnia 3 października 2006 r. (sygn. akt II SA/Wa 871/06); wyrok WSA w Warszawie z dnia 30 listopada 2006 r. (sygn. akt SA/Wa 1734/06)

wywiązujących się z zaciągniętych wobec banków zobowiązań w terminie 3 lat, bez ich zgody, w momencie, gdy osoby takie występują z żądaniem usunięcia ich danych z bazy BIK.

Inną kategorią spraw analizowanych w ramach omawianego działu były kwestie przekazania przez banki, w związku z przelewem wierzytelności, danych osobowych klientów funduszm sekurytyzacyjnym.⁶⁷ GODO reprezentował tu pogląd, że bank, dokonując takiego przelewu i w konsekwencji przekazując dane osobowe funduszm sekurytyzacyjnemu nawet bez zgody osoby, której dane dotyczą, nie naruszał przepisów ustawy o ochronie danych osobowych. Bank działał bowiem na podstawie odpowiednich przepisów prawa pozwalających na taką zmianę wierzyciela i tym samym udostępnienia danych osobowych⁶⁸.

W omawianym okresie badany był również problem spełniania przez BIK S.A. obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych⁶⁹. Otóż BIK S.A. wobec osoby, która zwracała się w trybie z art. 33 ust. 1 ustawy⁷⁰ o zrealizowanie wobec niej obowiązku informacyjnego, żądał złożenia wniosku o informację w trybie określonym w „Regulaminie udostępniania informacji dotyczących danych osobowych przetwarzanych w zbiorze Biura Informacji Kredytowej S.A.”. Stosownie natomiast do tego regulaminu, od osób domagających się udzielenia informacji BIK S.A. żąda uiszczenia opłaty w wysokości 10 zł jako „zryczałtowany koszt wysłania przesyłki”. GODO uznał, iż uzależnianie spełnienia owego obowiązku od uiszczenia określonej kwoty pieniężnej jest sprzeczne z postanowieniami ustawy o ochronie danych osobowych i, wskazując na jednoznaczną treść

⁶⁷ Np.: GI-DOLiS-430/50/07

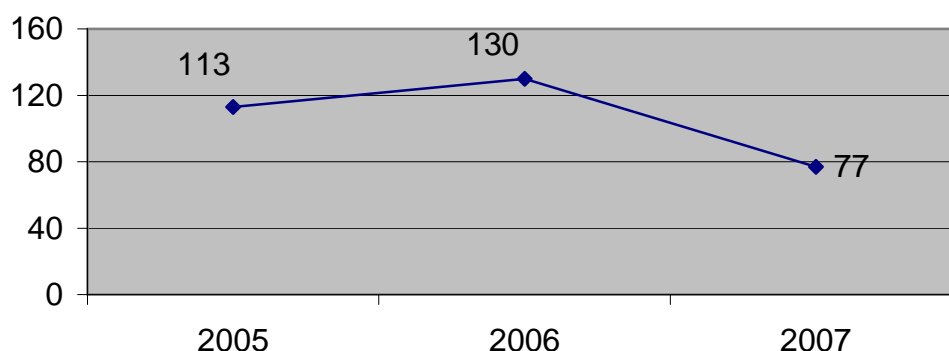
⁶⁸ Zgodnie z art. 326 ust. 1 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych (Dz. U. Nr 146, poz. 1546 z późn. zm.), do przelewu wierzytelności banku na fundusz sekurytyzacyjny, z tytułu umów zawartych przed dniem wejścia w życie ustawy (tj. przed dniem 1 lipca 2004 r.) stosuje się przepisy art. 92 – 92c ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.) z zastrzeżeniem ust. 2-4. Art. 92a ust. 1 Prawa bankowego dopuszcza wprost zawarcie pomiędzy bankiem a towarzystwem funduszy inwestycyjnych tworzącym fundusz sekurytyzacyjny, albo funduszem sekurytyzacyjnym umowy przelewu wierzytelności. Art. 326 ust. 2 ustawy o funduszach inwestycyjnych stanowi, iż bank nie jest zobowiązany do uzyskania zgody dłużnika banku na przelew wierzytelności z banku z tytułu umów kredytu, w przypadku niedotrzymania przez kredytobiorcę warunków udzielenia kredytu określonych w umowie. Jednocześnie art. 104 ust. 2 pkt 4 Prawa bankowego zwalnia bank, osoby w nim zatrudnione oraz osoby, za pośrednictwem których bank wykonuje czynności bankowe, z obowiązku zachowania tajemnicy bankowej (obejmującej wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje) w przypadku, w którym udzielenie informacji objętych tajemnicą bankową jest niezbędne do zawarcia i wykonywania umów sprzedaży wierzytelności zakwalifikowanych zgodnie z odrębnymi przepisami do kategorii straconych. Stosownie do brzmienia art. 193 ustawy o funduszach inwestycyjnych, fundusz sekurytyzacyjny oraz podmiot, z którym fundusz zawarł umowę o obsługę sekurytyzowanych wierzytelności, mogą zbierać i przetwarzać dane osobowe dłużników sekurytyzowanych wierzytelności jedynie dla celów związanych z administrowaniem wierzytelnościami sekurytyzowanymi i ich obrotem.

⁶⁹ GI-DOLiS-43065/07

⁷⁰ Zgodnie z art. 33, na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1 – 5a, a w szczególności podać w formie zrozumiałej: 1) jakie dane osobowe zawiera zbiór, 2) w jaki sposób zebrano dane, 3) w jakim celu i zakresie dane są przetwarzane, 4) w jakim zakresie oraz komu dane zostały udostępnione. Na wniosek osoby, której dane dotyczą, informacji, o których mowa powyżej, udziela się na piśmie – art. 33 ust. 2 ustawy.

wspomnianego art. 33 oraz prawo gwarantowane art. 32 ust. 1 tej ustawy⁷¹, nakazał spełnienie obowiązku informacyjnego⁷².

Mimo spadku w 2007 r. liczby skarg z tego sektora, podobnie jak w latach ubiegłych stanowiły one jedną z liczniejszych grup spraw rozpoznawanych przez GODO.



Wykres 10: *Zestawienie porównawcze liczby skarg dotyczących sektora bankowości, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w latach 2005-2007.*

W stosunku do poprzednich lat spadła liczba skarg dotyczących nieprawidłowego zabezpieczenia danych osobowych oraz bezpodstawnego ich przetwarzania przez banki w celach marketingowych⁷³. Ponadto do GODO nie wpływały w omawianym okresie, dosyć liczne w poprzednich latach, skargi na niedopełnienie przez administratorów z tego sektora obowiązku informacyjnego.

4) Sądy, organy prokuratury, komornicy

W skargach dotyczących analizowanego sektora najczęściej pojawiały się zarzuty dotyczące pozyskiwania danych osobowych przez prokuratury bądź sądy bez podstawy prawnej. GODO analizował też sprawy dotyczące bezpodstawnego – zdaniem osób skarżących – udostępniania danych

⁷¹ Zgodnie z art. 32 ust. 1 ustawy o ochronie danych osobowych, każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do: 1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska, 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze, 3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych, 4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej, 5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane, 5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2.

⁷² Decyzja nieprawomocna z dnia 17 września 2007 r. (sygn. GI-DEC-DOLiS-198/07/5293,5294,5295)

⁷³ Np.: GI-DOLiS-430/190/07, GI-DOLiS-430-363/07

osobowych zawartych w aktach postępowań sądowych podmiotom nieuprawnionym. GODO w takich przypadkach ustalał, że tymi podmiotami były inne strony tego samego postępowania, które, korzystając z zasady jawności wewnętrznej postępowania sądowego, mogły mieć dostęp do treści akt sądowych, a więc również zawartych w nich danych osobowych⁷⁴.

Generalny Inspektor badał również kwestię naruszenia ustawy o ochronie danych osobowych wskutek dołączania do akt sprawy sądowej - jako dowodu - pism (dokumentów) zawierających dane osobowe. W konkretnym przypadku, w postępowaniu sądowym dotyczącym sprawy cywilnej, pełnomocnik strony przedłożył - jako dowód w sprawie - kopię aktu oskarżenia skierowanego do sądu w innej sprawie zainicjowanej zawiadomieniem tejże strony o popełnieniu przestępstwa⁷⁵. GODO ustalił, że dopuszczając wspomniany dowód, sąd działał na podstawie przepisów prawa, o których wspomina art. 23 ust. 1 pkt 2 ustawy. Zarówno złożenie określonego dowodu, jak i włączenie go do materiału dowodowego znajdowało bowiem uzasadnienie w przepisach Kodeksu postępowania cywilnego⁷⁶. GODO uwzględnił tu treść art. 217 § 1, art. 232, art. 233 § 1 oraz art. 244 K.p.c.⁷⁷ Zaznaczyć przy tym należy, że w takich sprawach nie oceniał merytorycznie rozstrzygnięć sądowych wydanych w toku postępowania z wykorzystaniem takiej dokumentacji, gdyż nie mieściło się to w zakresie jego kompetencji⁷⁸.

W analizowanym okresie sprawozdawczym pojawiło się również zagadnienie ujawnienia przez komornika sądowego osobom nieuprawnionym danych osobowych osób, wobec których prowadzone było postępowanie egzekucyjne.⁷⁹ W konkretnym przypadku rozpowszechniono w gazecie codziennej ogłoszenie o licytacji zajętej nieruchomości zawierające imiona i nazwiska osób, wobec których prowadzone jest właśnie takie postępowanie egzekucyjne. Zdaniem GODO, ujawnienie informacji o imionach i nazwiskach dłużników odbyło się niezgodnie z przywoływanym przez komornika jako

⁷⁴ Np.: GI-DOLiS-430/221/07; GI-DOLiS-430/284/07; GI-DOLiS-430/249/07

⁷⁵ GI-DOLiS-430/198/07

⁷⁶ Ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.)

⁷⁷ Zgodnie z art. 217 § 1 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 1964 Nr 43, poz. 296 z późn. zm.), strona może aż do zamknięcia rozprawy przytaczać okoliczności faktyczne i dowody na uzasadnienie swych wniosków lub dla odparcia wniosków i twierdzeń strony przeciwnej, z zastrzeżeniem niekorzystnych skutków, jakie według przepisów niniejszego kodeksu mogą dla niej wynikać z działania na zwłokę lub niezastosowania się do zarządzeń przewodniczącego i postanowień sądu. Zgodnie z art. 232 K.p.c., strony są obowiązane wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne. Sąd może dopuścić dowód niewskazany przez stronę. Zgodnie z art. 233 § 1, sąd ocenia wiarygodność i moc dowodów według własnego przekonania, na podstawie wszechstronnego rozważenia zebranego materiału. Zgodnie z art. 244 § 1 i 2, dokumenty urzędowe, sporządzone w przepisanej formie przez powołane do tego organy władzy publicznej i inne organy państwowe w zakresie ich działania, stanowią dowód tego, co zostało w nich urzędowo zaświadczone. Przepisy te stosuje się odpowiednio do dokumentów urzędowych sporządzonych przez organizacje zawodowe, samorządowe, spółdzielcze i inne organizacje społeczne w zakresie zleconych im przez ustawę spraw z dziedziny administracji publicznej.

⁷⁸ Podobnie NSA w wyroku z dnia 2 marca 2001 r. (sygn. akt II SA 401/00), w którym stwierdził, że „(...) Generalny Inspektor (...) nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji, czy w inny sposób określony odpowiednimi procedurami”.

⁷⁹ GI-DOLiS-430/142/07

podstawa prawna takiego działania art. 955 K.p.c.⁸⁰ W konsekwencji, uznając to za sprzeczne z ustawą o ochronie danych osobowych, GODO zwrócił się do komornika z pismem o zaprzestanie tego typu praktyk. W odpowiedzi został poinformowany, iż uwagi w nim zawarte zostały przez komornika uwzględnione⁸¹.

Podsumowując należy wskazać, że w 2007 r. - w porównaniu do lat poprzednich - odnotowano spadek skarg dotyczących przetwarzania danych osobowych przez sądy, prokuratury i komorników sądowych. Przyczyn tego zjawiska należy upatrywać m.in. w rozszerzeniu przez GODO w latach ubiegłych działalności informacyjno-edukacyjnej (przeprowadzane w szerokim zakresie szkolenia pracowników instytucji z tego sektora, artykuły i wywiady prasowe, rozbudowana strona internetowa organu) oraz w konsekwentnym sygnalizowaniu organom nadzoru nad konkretnymi administratorami danych uchybień stwierdzonych przy przetwarzaniu danych i sposobów ich usuwania.

5) Marketing

W niniejszym sektorze odniesiono się zarówno do spraw dotyczących podmiotów, które przetwarzały dane osobowe w celu realizacji ich głównego celu, jakim było prowadzenie marketingu (najczęściej na rzecz innych podmiotów), jak i podmiotów, które przetwarzały dane w celach marketingowych jedynie obok swojej głównej działalności, np. towarzystwa ubezpieczeniowe, banki, operatorzy telekomunikacyjni.

Głównym z zarzutów pod adresem administratorów było przetwarzanie danych osobowych w celach marketingowych bez zgody osoby, której dane dotyczą, oraz nierespektowanie złożonych już pisemnych sprzeciwów wobec takiego przetwarzania⁸².

Jeśli chodzi o pierwszą ze wskazanych grup skarg należy zauważyć, że ich autorzy nie mieli w zdecydowanej przewadze świadomości, iż podstawę legalnego przetwarzania danych osobowych w celach marketingowych stanowi nie tylko zgoda, o której mowa w art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych⁸³, ale również art. 23 ust. 1 pkt 5 ustawy, w myśl którego marketing własnych produktów i usług administratora danych jest dopuszczalny, gdy przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą. Tę przesłankę przetwarzania danych ustawodawca określił jako prawnie usprawiedliwiony cel administratora danych. Zgoda osoby, której dane dotyczą, na przetwarzanie danych w celach marketingowych wymagana jest natomiast, gdy marketing dotyczy produktów innych podmiotów niż administrator danych. Wobec powyższych okoliczności prawnych część zarzutów

⁸⁰ Zgodnie z art. 955 K.p.c., obwieszczenie o licytacji należy co najmniej dwa tygodnie przed jej terminem ogłosić publicznie w budynku sądowym i w lokalu organu gminy oraz w dzienniku poczytnym w danej miejscowości (§ 1). Na wniosek i koszt strony komornik może zarządzić ogłoszenie również w inny wskazany przez nią sposób (§ 2). W ogłoszeniu w dzienniku wystarczy oznaczenie nieruchomości, czasu i miejsca licytacji, sumy oszacowania i ceny wywołania oraz wysokości rękojmi, jaką licytant powinien złożyć (§ 3).

⁸¹ Pismo z dnia 25 października 2007 r.

⁸² Np.: GI-DOLiS-430/64/07, GI-DOLiS-430/26/07

⁸³ Zgodnie z art. 23 ust. 1 pkt 1, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę.

przedstawionych w skargach do organu ochrony danych osobowych w analizowanym okresie nie znalazła potwierdzenia. Zauważyć przy tym należy, że w większości spraw osoby kierujące skargi do GODO nie korzystały wcześniej z uprawnienia z art. 32 ust. 1 pkt 8 ustawy polegającego na możliwości wniesienia sprzeciwu do administratora danych wobec przetwarzania danych w przypadkach wymienionych w art. 23 ust. 1 pkt. 4 i 5 ustawy. W takich przypadkach GODO, kierując się treścią art. 35 ust. 2 ustawy o ochronie danych osobowych⁸⁴, informował osoby skarżące o przysługującym im prawie wniesienia wspomnianego sprzeciwu oraz możliwości wniesienia skargi do organu dopiero w przypadku nierespektowania przez konkretnego administratora danych wniesionego sprzeciwu.

W jednej z tego typu spraw osoba skarżąca wskazała, że administrator danych przetwarza jej dane osobowe w celach marketingowych, mimo pisemnego niewyrażenia na to zgody. GODO stwierdził, iż administrator przetwarzał dane bez podstawy prawnej. Uznawszy, że powyższa nieprawidłowość wynika z całą pewnością z zaniedbania po stronie administratora danych, korzystając ze swoich ustawowych kompetencji (art. 17 ust. 2 ustawy o ochronie danych osobowych), skierował wniosek o wszczęcie postępowania dyscyplinarnego⁸⁵, wskutek którego już w toku postępowania administrator danych zaprzestał wadliwego przetwarzania (wykorzystywania) danych do celów marketingowych.

W omawianym okresie badana była również kwestia przetwarzania przez jeden z banków danych osobowych w celach marketingowych, mimo uprzedniego sprzeciwu osoby, której dane dotyczyły⁸⁶. GODO ustalił, że osoba skarżąca (klient banku) otrzymywała zestawienie operacji dokonywanych na drukach rachunków, które „opatrzone są tekstem zawierającym istotne użyteczne informacje dotyczące poszczególnych rachunków (...) oraz powiązanych z nimi usług”. Informacje te miały dotyczyć m.in. ubezpieczeń na życie oraz funduszy inwestycyjnych. GODO uznał, że bank, umieszczając tego typu informacje na kierowanych do swojego klienta zestawieniach operacji dokonywanych na rachunkach bankowych, w rzeczywistości przetwarzał dane osoby skarżącej w celach marketingowych, choć było to niedopuszczalne. Wobec tego, organ nakazał bankowi przywrócenie stanu zgodnego z prawem poprzez zaprzestanie przetwarzania danych osobowych jego klienta w celach marketingowych⁸⁷.

GODO badał również treść stosowanych przez administratorów danych formularzy obejmujących tzw. klauzule zgody na przetwarzanie danych osobowych⁸⁸. Podobnie jak to było w

⁸⁴ Zgodnie z art. 35 ust. 2 ustawy o ochronie danych osobowych, w razie niedopełnienia przez administratora danych obowiązku, o którym mowa w ust. 1, osoba, której dane dotyczą, może się zwrócić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku.

⁸⁵ Pismo z dnia 9 marca 2007 r. o sygn. GI-DOLiS-430/26/07/1528

⁸⁶ GI-DOLiS-430/252/07

⁸⁷ Decyzja z dnia 19 października 2007 r. o sygn. GI-DEC-DOLiS-226/07/5960,5961

⁸⁸ GI-DOLiS-430/120/07, GI-DOLiS-430/81/07

poprzednich latach, większość z badanych klauzul wprowadzała osoby zainteresowane w błąd co do tego, na jakie przetwarzanie swoich danych się godzą i jaki jest konkretny cel tego przetwarzania. Na takich formularzach brakowało ponadto podstawowych informacji, do jakich osoba zainteresowana ma prawo, wskazanych w art. 24 i 25 ustawy⁸⁹. W takich przypadkach GODO z urzędu podejmował czynności mające na celu doprowadzenie do takich zmian w treści formularzy, aby nie budziły wątpliwości, co do ich zgodności z przepisami ustawy o ochronie danych osobowych⁹⁰.

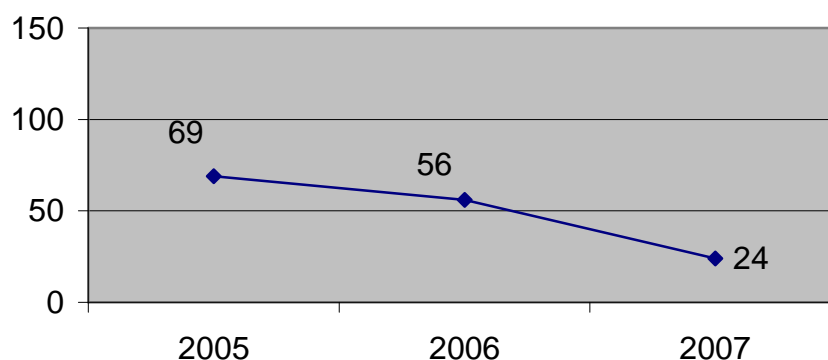
W jednej z takich spraw GODO wystąpił do firmy, która pozyskiwała dane osobowe za pomocą tzw. karty zamówienia, zawierającej jedną formułę obejmującą zgodę nie tylko na przetwarzanie danych osobowych przez administratora danych, ale również zgodę na „udostępnienie (...) danych innym podmiotom w celach marketingowych”. Jak wyżej wskazano, w świetle przepisów ustawy o ochronie danych osobowych, dane osobowe mogłyby być pozyskiwane w takim celu jedynie wówczas, gdyby administrator danych legitymował się odrębną zgodą osoby, której dane dotyczą. W tym przypadku organ wskazał administratorowi danych, że we wspomnianym formularzu zamówienia powinien sformułować całkowicie niezależną klauzulę zgody, gwarantującą możliwość wyrażenia przez osobę składającą zamówienie świadomej decyzji co do wyrażenia, bądź niewyrażenia, zgody na udostępnienie danych innym podmiotom niezależnie od zgody na przetwarzanie danych przez samego administratora⁹¹.

W omawianym okresie sprawozdawczym, w porównaniu do lat ubiegłych, odnotowano spadek liczby skarg dotyczących tego sektora.

⁸⁹ Zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, 3) prawie dostępu do treści swoich danych oraz ich poprawiania, 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Zgodnie z art. 25 ust. 1 w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, 3) źródle danych, 4) prawie dostępu do treści swoich danych oraz ich poprawiania, 5) uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8

⁹⁰ Np. GI-DOLiS-430/127/07

⁹¹ Pismo z dnia 13 lipca 2007 r. o sygn. GI-DOLiS-430/137/07/4035



Wykres 11: *Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych w celach marketingowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2005-2007.*

Niewątpliwie w znacznym stopniu jest to efekt nie tylko działalności edukacyjnej organu ochrony danych osobowych w poprzednich latach, rygorystycznego stosowania przepisów tej ustawy w odniesieniu do firm, które w poprzednich latach na skalę masową, z naruszeniem zasad określonych w ustawie, przetwarzały dane w celu rozsyłania niezamawianej korespondencji o treści marketingowej, ale również konsekwencji w dążeniu do wyegzekwowania odpowiedzialności karnej osób za to odpowiedzialnych. Przykładem takiego działania może być wystąpienie GODO z dnia 10 października 2007 r.⁹² do Ministra Sprawiedliwości, Prokuratora Generalnego, wskazujące sprawy, w których organ składał zawiadomienie o podejrzeniu popełnienia przestępstwa, a w których – zdaniem GODO – prokuratury bezzasadnie odmawiały wszczęcia postępowania albo pochopnie kończyły je postanowieniem o umorzeniu. Reakcją na to wystąpienie było poinformowanie GODO przez Prokuratora Krajowego, Zastępcę Prokuratora Generalnego, iż wskutek przeprowadzenia badania wskazanych przez organ spraw za konieczne uznano ponowne podjęcie umorzonych postępowań i rozważenie poddania ocenie sądu czynów będących ich przedmiotem⁹³.

6) Sektor mieszkalnictwa

Skargi z tej kategorii dotyczyły zagadnień przetwarzania danych osobowych przez spółdzielnie mieszkaniowe, wspólnoty mieszkaniowe oraz zarządców nieruchomości.

Obok dotychczasowych skarg na udostępnianie danych podmiotom trzecim oraz ich bezprawne upublicznianie pojawił się problem pozyskiwania przez spółdzielnie danych osobowych jej członków za pomocą różnego rodzaju formularzy. Jak tłumaczono, dane te były zbierane w celu

⁹² Pismo z dnia 10 października 2007 r. o sygn. GI-DOLiS 430/768/04/5724/07

wykorzystania ich w przyszłym ewentualnym postępowaniu egzekucyjnym dotyczącym należności czynszowych⁹⁴. W takich sprawach organ przyjmował, iż zbieranie danych osobowych w celu bliżej niesprecyzowanym i odległym w czasie, stanowi naruszenie art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych⁹⁵. W związku z tym zwrócono się do spółdzielni o przywrócenie stanu zgodnego z prawem⁹⁶.

Wśród skarg dotyczących udostępnienia przez administratorów z opisywanego sektora danych osobowych podmiotom trzecim najczęściej pojawiał się problem przekazywania ich organom procesowym (prokuratury, sądy) oraz różnego rodzaju podmiotom świadczącym usługi na rzecz spółdzielni i wspólnot. Skargi w tym zakresie – podobnie jak w poprzednich latach – okazywały się najczęściej niezasadne. Kwestionowane operacje na danych podejmowane były bowiem, bądź w usprawiedliwionym celu administratora danych, bądź w celu zrealizowania obowiązków wynikających z przepisów prawa, np. w celu realizacji kontroli instalacji gazowej, wentylacyjnej czy grzewczej⁹⁷.

Nie zniknęły również przypadki nieuprawnionego upublicznienia danych osobowych członków spółdzielni i wspólnot⁹⁸. Najczęściej działanie to przybierało postać wywieszania na terenie danej spółdzielni czy wspólnoty, w miejscach powszechnie dostępnych (gabloty, tablice ogłoszeń), informacji o osobach zadłużonych, traktując takie działania jako skuteczną metodę egzekwowania zadłużenia. Istotne jest jednak, że każdy z podmiotów przetwarzających w ten sposób dane osobowe, niezwłocznie po pozyskaniu informacji o zainteresowaniu się przez GODO tą kwestią, bądź wskutek formalnego wystąpienia organu z pismem sygnalizacyjnym⁹⁹, zaprzestawał tego typu praktyk.

W analizowanym roku 2007, w porównaniu z latami ubiegłymi, odnotowano spadek liczby skarg na przetwarzanie danych przez ww. podmioty¹⁰⁰.

⁹³ Pismo z dnia 18 grudnia 2007 r. (PR III Ko 1120/05)

⁹⁴ Np. GI-DOLiS-430/55/07

⁹⁵ Zgodnie z art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

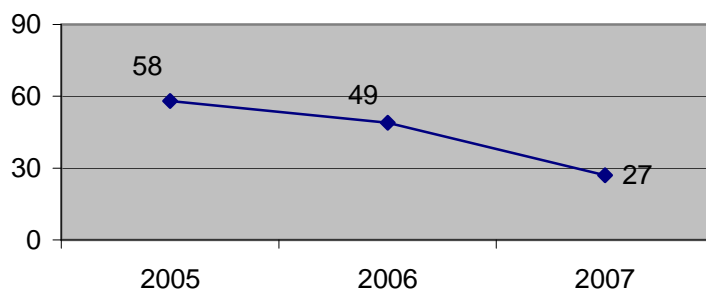
⁹⁶ Pismo z dnia 27 sierpnia 2007 r. o sygn. GI-DOLiS-430/318/07/4872

⁹⁷ Np. GI-DOLiS-430/134/07, GI-DOLiS-430/158/07, GI-DOLiS-430/207/07

⁹⁸ Np. GI-DOLiS-430/132/07, GI-DOLiS-430/40/07

⁹⁹ Np. GI-DOLiS-430/40/07/2336

¹⁰⁰ Szczegółowe informacje na temat lat ubiegłych można odnaleźć w *Sprawozdaniu z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2006, Część I, pkt 1 ppkt 8, str. 38 i n.*, *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.



Wykres 12: Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych osobowych z zakresu mieszkalnictwa, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2005-2007.

Ponadto odnotowano, że znacznie rzadziej władze spółdzielni odmawiają jej członkom dostępu do danych innych członków, które są zawarte w prowadzonych przez spółdzielnie zbiorach danych. Świadczyć to może o wzrastającej wśród władz tych podmiotów znajomości przepisów ustawy o ochronie danych osobowych.

7) Ubezpieczenia społeczne, majątkowe i osobowe

Niniejszy sektor obejmuje sprawy przetwarzania danych osobowych w związku z ubezpieczeniem społecznym i majątkowym. Skargi dotyczyły przede wszystkim kwestii pozyskania przez podmioty prowadzące działalność ubezpieczeniową danych osobowych, udostępnienia ich podmiotom (osobom) trzecim oraz nieuzasadnionej odmowy udostępnienia danych ze zbiorów prowadzonych przez ww. podmioty¹⁰¹.

GIODO badał m.in. kwestię odmowy udostępnienia przez Zakład Ubezpieczeń Społecznych [dalej: ZUS] danych osobowych z bazy danych ZUS Powiatowemu Urzędowi Pracy [dalej: PUP]. W jednej z takich spraw Dyrektor PUP wystąpił do ZUS z wnioskiem o udostępnienie danych osobowych osoby fizycznej w zakresie dotyczącym tego, czy podlega ona ubezpieczeniu społecznemu oraz z jakiego tytułu. Służyć to miało weryfikacji posiadanej przez PUP informacji, czy osoba, której dane dotyczą, prowadziła w przeszłości działalność gospodarczą, i czy w związku z tym przysługiwał jej status osoby bezrobotnej. Jako podstawę prawną tego żądania PUP wskazał art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych¹⁰². W odpowiedzi ZUS odmówił udostępnienia danych, wskazując na

¹⁰¹ Np.: GI-DOLiS-430/23/07, GI-DOLiS-430/94/07, GI-DOLiS-430/326/07

¹⁰² Zgodnie z art. 23 ust. 1 pkt 4 ustawy, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

treść art. 50 ust. 3 ustawy o systemie ubezpieczeń społecznych.¹⁰³ W tego typu sprawach Generalny Inspektor Ochrony Danych Osobowych przyznawał rację ZUS. Wspomniany przepis ustawy o systemie ubezpieczeń społecznych, określający krąg podmiotów uprawnionych do pozyskania danych przetwarzanych przez ZUS, nie podlega wykładni rozszerzającej i nie obejmuje PUP. Również art. 79 tej ustawy przewiduje, że dane zgromadzone przez ZUS od ubezpieczonych oraz płatników składek są objęte tajemnicą służbową ZUS; do jej przestrzegania zobowiązani są pracownicy ZUS i członkowie Rady Nadzorczej Zakładu. W świetle tych regulacji, GODO stwierdził, że nie zachodzi żadna z przesłanek z art. 23 ust. 1 ustawy o ochronie danych osobowych, w tym również przywoływana w tych sprawach przesłanka z pkt. 4.¹⁰⁴

W innej ze skarg złożonych do GODO zakwestionowano legalność udostępnienia danych osobowych przez zakład ubezpieczeń podmiotowi trzeciemu. W toku postępowania wyjaśniającego organ ustalił, iż owego udostępnia dokonano na rzecz podmiotu, któremu towarzystwo ubezpieczeniowe zleciło przeprowadzenie likwidacji szkody poniesionej przez osobę skarżącą. W ocenie GODO, działanie zakładu znajdowało podstawę w art. 3 ust. 6 w zw. z art. 19 ust. 2 pkt 24 ustawy o działalności ubezpieczeniowej¹⁰⁵. Stwierdzono zatem, że zastosowanie miała w tym przypadku przesłanka przetwarzania danych z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Omawiając tę grupę spraw, warto również wskazać na analizowany przez GODO przypadek udostępnienia przez zakład ubezpieczeń podmiotowi trzeciemu (firmie specjalizującej się w montażu oprzyrządowania do samochodów inwalidzkich), takich danych osobowych, jak: imię i nazwisko, adres zamieszkania oraz informacje o stopniu niepełnosprawności. Zakład wystąpił do tej firmy o udzielenie informacji o kosztach przystosowania pojazdu do potrzeb osoby niepełnosprawnej (osoby, której dotyczyły udostępnione dane). Miało to służyć rozpatrzeniu przez ubezpieczyciela zasadności roszczenia o zwrot kosztów zakupu pojazdu dostosowanego do przewożenia poszkodowanej i wózka inwalidzkiego¹⁰⁶. GODO uznał, że w tym przypadku udostępnienie wspomnianych danych, w tym danych szczególnie chronionych, nie znajdowało uzasadnienia w przywoływanym przez towarzystwo

¹⁰³ Zgodnie z art. 50 ust. 3 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2007 r. Nr 11, poz. 74 z późn. zm.), 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 centrům pomocy rodzinie oraz Komisji Nadzoru Finansowego, z uwzględnieniem przepisów dotyczących ochrony danych osobowych.

¹⁰⁴ Decyzja z dnia 27 kwietnia 2007 r. (sygn. GI-DEC-DOLiS-91/07/2566, 2567, 2568)

¹⁰⁵ Zgodnie z art. 3 ust. 6 ustawy z dnia 22 maja 2003 r. (Dz. U. Nr 124, poz. 1151 z późn. zm.), zakład ubezpieczeń może zlecać wykonanie czynności, o których mowa w ust. 4 pkt. 1-6 oraz ust. 5, innym podmiotom. Czynności, o których mowa w ust. 4 pkt. 1-6 oraz ust. 5, są traktowane jak czynności ubezpieczeniowe w zakresie, w jakim są wykonywane w imieniu i na rzecz zakładu ubezpieczeń. Z kolei zgodnie z art. 19 ust. 2 pkt 24, dopuszczalne jest udzielenie informacji dotyczących poszczególnych umów ubezpieczenia przez zakład ubezpieczeń i osoby w nim zatrudnione lub osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe na wniosek zleceniobiorców czynności określonych w art. 3 ust. 4 pkt. 1-6 oraz ust. 5, w zakresie, w jakim dotyczą one zleconych czynności.

¹⁰⁶ GI-DS-430/221/05

art. 25 ustawy o działalności ubezpieczeniowej¹⁰⁷. Dlatego nakazał ubezpieczycielowi nieudostępnianie w przyszłości danych tej osoby, w tym zwłaszcza danych o stanie zdrowia, innym podmiotom bez spełnienia jednej z przesłanek określonych w art. 27 ust. 2 ustawy o ochronie danych osobowych.¹⁰⁸ Powyższe stanowisko organu znalazło potwierdzenie w wyroku WSA w Warszawie¹⁰⁹, w którym sąd stwierdził, że pozyskanie przez ubezpieczyciela żądanych informacji „mogło odbyć się przez sam opis problemu w zakresie przystosowania pojazdu do przewozu osoby niepełnosprawnej i kosztu takiego przystosowania, bez zamieszczania w (...) pismach informacji o danych osobowych skarżącej w połączeniu z informacją o stopniu jej inwalidztwa”.

Przykładem sprawy dotyczącej legalności pozyskania danych przez ubezpieczyciela był analizowany przez GODO przypadek, w którym osoba skarżąca otrzymała od jednego z towarzystw ubezpieczeniowych pismo zawierające informację o toczącym się wobec niej postępowaniu odszkodowawczym z tytułu zalania przez nią lokalu. Skarżący rzeczywiście zalał lokal znajdujący się poniżej jego mieszkania. Osoba, która została poszkodowana, wezwała konserwatora instalacji wodno – kanalizacyjnej, a ten spisał odpowiedni protokół powstałych szkód, w którym uwzględniono również dane osobowe sprawcy. Jeden z egzemplarzy tego dokumentu za pośrednictwem poszkodowanego trafił do ubezpieczyciela, który w ten sposób pozyskał dane osobowe sprawcy.

Generalny Inspektor Ochrony Danych Osobowych uznał, że w tym przypadku nie doszło do naruszenia ustawy o ochronie danych osobowych. Udostępnienie danych miało związek z wypłatą odszkodowania właścicielowi zalanego mieszkania i w celu dochodzenia roszczeń regresowych z tytułu wypłaconego odszkodowania i jako takie, w związku z treścią art. 3 ust. 4, art. 16 ust. 1 ustawy o działalności ubezpieczeniowej¹¹⁰ oraz art. 828 § 1 Kodeksu cywilnego¹¹¹, wypełniało przesłanki legalnego przetwarzania danych z art. 23 ust. 1 pkt. 2 i 5 ustawy.

¹⁰⁷ Zgodnie z art. 25 ustawy o działalności ubezpieczeniowej, sądy, prokuratura, Policja oraz inne organy i instytucje, na wniosek zakładu ubezpieczeń, w zakresie zadań przez ten zakład ubezpieczeń wykonywanych i w celu ich wykonania, w związku z wypadkiem lub zdarzeniem będącym podstawą ustalania odpowiedzialności, udzielają informacji o stanie sprawy oraz udostępniają zebrane materiały, jeżeli są one niezbędne do ustalenia okoliczności tych wypadków i zdarzeń losowych oraz wysokości odszkodowania lub świadczenia. Sądy, prokuratura, Policja oraz inne organy i instytucje, na wniosek Ubezpieczeniowego Funduszu Gwarancyjnego, Polskiego Biura Ubezpieczycieli Komunikacyjnych lub Rzecznika Ubezpieczonych, w zakresie zadań przez nie wykonywanych i w celu ich wykonania, udzielają informacji w zakresie stanu sprawy oraz udostępniają zebrane materiały. Zakład ubezpieczeń ma obowiązek, na żądanie ubezpieczonego, uposażonego lub uprawnionego z umowy ubezpieczenia lub poszkodowanego, udostępnić posiadane przez siebie informacje związane z wypadkiem lub zdarzeniem będącym podstawą ustalenia jego odpowiedzialności oraz ustalenia okoliczności wypadków i zdarzeń losowych, jak również wysokości odszkodowania lub świadczenia.

¹⁰⁸ Decyzja z dnia 28 czerwca 2006 r. o sygn. GI-DS-227/06/617,618

¹⁰⁹ Wyrok z dnia 7 marca 2007 r. (sygn. akt II SA/Wa 2260/06)

¹¹⁰ Zgodnie z a art. 3 ust. 4 ustawy o działalności ubezpieczeniowej, czynnościami ubezpieczeniowymi są m.in.: wypłacanie odszkodowań i innych świadczeń należnych z tytułu umów, o których mowa w ust. 3 pkt 1 (pkt 4) oraz prowadzenie postępowań regresowych oraz postępowań windykacyjnych związanych z wykonywaniem umów ubezpieczenia, reasekuracji oraz gwarancji ubezpieczeniowych (pkt 5). Zgodnie z art. 16 ust. 1 ww. ustawy, po otrzymaniu zawiadomienia o zajściu zdarzenia losowego objętego ochroną ubezpieczeniową, w terminie 7 dni od dnia otrzymania tego zawiadomienia, zakład ubezpieczeń m. in. podejmuje postępowanie dotyczące ustalenia stanu faktycznego zdarzenia, zasadności zgłoszonych roszczeń i wysokości świadczenia.

Podsumowując należy zauważyć, że liczba skarg dotyczących przetwarzania danych osobowych w sektorze ubezpieczeń w porównaniu do lat ubiegłych pozostała na niezmiennym poziomie (zob. Wykres 13). Podkreślenia jednak wymaga, iż w 2007 r. – w stosunku do poprzednich okresów sprawozdawczych – odnotowano spadek liczby zasadnych skarg na niewłaściwe zabezpieczenie danych osobowych. Wyraźnej zmiany w tym zakresie upatrywać należy w efektach działań GIODO w latach poprzednich. Z racji dużej liczby przetwarzanych przez ubezpieczycieli danych, w tym danych szczególnie chronionych, organ ochrony danych osobowych, badając prawidłowość ich przetwarzania, kładł szczególny nacisk na rzetelne przestrzeganie przez te podmioty zasad wynikających z ustawy o ochronie danych osobowych, w szczególności dotyczących zabezpieczenia danych przez dostępem do nich osób nieuprawnionych oraz realizacji przez administratorów obowiązku informacyjnego.



Wykres 13: *Zestawienie porównawcze liczby skarg dotyczących sektora ubezpieczeń, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2005-2007.*

8) Telekomunikacja

Podobnie jak w poprzednich okresach sprawozdawczych, najwięcej badanych spraw z tego sektora dotyczyło kwestii udostępniania przez operatorów telekomunikacyjnych danych osobowych podmiotom trzecim w związku z dochodzeniem zaległych opłat, prawidłowości zabezpieczenia danych osobowych oraz zarzutów wykorzystywania przez operatorów danych w innych celach niż te, dla

¹¹¹ Zgodnie z art. 828 § 1 ustawy z dnia 23 kwietnia z 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.), jeżeli nie umówiono się inaczej, z dniem zapłaty odszkodowania przez ubezpieczyciela roszczenie ubezpieczającego przeciwko osobie trzeciej odpowiedzialnej za szkodę przechodzi z mocy prawa na ubezpieczyciela do wysokości zapłaconego odszkodowania. Jeżeli ubezpieczyciel pokrył tylko część szkody, ubezpieczającemu przysługuje, co do pozostałej części, pierwszeństwo zaspokojenia przed roszczeniem ubezpieczyciela.

realizacji których je pozyskano. W 2007 r. GODO zbadał również praktykę sprzedaży przez jednego z operatorów zbioru danych abonentów.

Sprawa tej sprzedaży była jedną z istotniejszych prowadzonych w tym okresie sprawozdawczym. Organ ustalił we własnym zakresie, że operator zamieścił na swojej stronie internetowej ofertę udostępniania numerów telefonów abonentów prywatnych oraz ofertę „uzupełniania baz danych” posiadanych przez podmioty zewnętrzne o numery telefonów abonentów tego operatora. Jako podstawy tego działania operator wskazał ustawę Prawo telekomunikacyjne¹¹², zgodę osoby, której dane dotyczą, na publikację danych w powszechnie dostępnych spisach abonentów, oraz brak sprzeciwu tej osoby na takie udostępnienie. Po przeanalizowaniu okoliczności faktycznych i prawnych tej sprawy GODO nakazał¹¹³ operatorowi zaprzestanie udostępniania osobom trzecim numerów telefonów użytkowników osób fizycznych bez spełnienia jednego z warunków określonych w art. 159 ust. 2 ustawy Prawo telekomunikacyjne¹¹⁴. GODO uznał, że zgoda - na którą powołuje się operator - na umieszczenie danych w „ogólnokrajowym spisie abonentów” nie może być traktowana jako zgoda na udostępnienie danych osobowych w ramach kwestionowanej usługi sprzedaży baz danych. Stanowisko GODO wyrażone we wspomnianej decyzji podzielił Wojewódzki Sąd Administracyjny w Warszawie, który wyrokiem z dnia 12 listopada 2007 r. oddalił skargę operatora.¹¹⁵

Badając w 2007 r. sprawy dotyczące przetwarzania przez operatorów telekomunikacyjnych danych osobowych w celach windykacyjnych, GODO nie stwierdził naruszeń ustawy o ochronie danych osobowych¹¹⁶. Udostępnianie podmiotom trzecim odbywało się albo w związku ze zleceniem przeprowadzenia czynności windykacyjnych i dokonywane było na podstawie art. 31 ustawy o ochronie danych osobowych¹¹⁷, albo wskutek sprzedaży wierzytelności służącej wobec osoby

¹¹² Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.)

¹¹³ Decyzja z dnia 14 maja 2007 r. o sygn. GI-DEC-DOLiS-109/07/2885

¹¹⁴ Zgodnie z art. 159 ust. 2 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800 z późn. zm.), zakazane jest zapoznavanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne, niż nadawca i odbiorca komunikatu, chyba że: 1) będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania; 2) nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą; 3) dokonanie tych czynności jest niezbędne w celu rejestrowania komunikatów i związanych z nimi danych transmisyjnych, stosowanego w zgodnej z prawem praktyce handlowej dla celów zapewnienia dowodów transakcji handlowej lub celów łączności w działalności handlowej; 4) będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi.

¹¹⁵ Sygn. akt. II SA/Wa 1252/07 (wyrok nieprawomocny).

¹¹⁶ GI-DOLiS-430/256/07

¹¹⁷ Zgodnie z art. 31 ustawy o ochronie danych osobowych, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych (ust. 1). Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie (ust. 2). Podmiot, o którym mowa w ust. 1, jest obowiązany 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 ponosi odpowiedzialność jak administrator danych (ust. 3). W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową (ust. 4). Do kontroli zgodności

skarżącej. W tym ostatnim przypadku zastosowanie znajdowała przesłanka legalnego przetwarzania danych osobowych z art. 23 ust. 1 pkt 5 w zw. z art. 23 ust. 4 tej ustawy. Organ uznał, iż sprzedaż wierzytelności (a w konsekwencji udostępnienie nabywcy danych dłużnika) było działaniem w usprawiedliwionym celu administratora danych.

Warto dodać, że pojawiały się również żądania nakazania całkowitego usunięcia danych osobowych z bazy danych operatora po wygaśnięciu umowy łączącej go z konkretnym abonentem¹¹⁸. GODO takich wniosków nie uwzględniał. Wskazywał w takich przypadkach na spoczywające na administratorach danych obowiązki wymagające dalszego przetwarzania danych osobowych, nawet już po wygaśnięciu umowy abonentów o świadczenie usług telekomunikacyjnych, np. w celach rachunkowych, archiwizacyjnych czy do czasu przedawnienia roszczeń cywilnych, które stanowiły wypełnienie przesłanki z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

W jednej ze spraw dotyczących prawidłowości zabezpieczenia danych osobowych GODO ustalił, iż w pomieszczeniu wynajętym przez niepubliczny zakład opieki zdrowotnej znajdowały się niezabezpieczone dokumenty zawierające dane osobowe należące do jednego z operatorów, który uprzednio zajmował ten lokal. Ustaliwszy konkretnego operatora, jako administratora tych danych, Generalny Inspektor Ochrony Danych Osobowych stwierdził, że doszło do popełnienia przestępstwa z art. 51 oraz 52 ustawy o ochronie danych osobowych¹¹⁹ i skierował do prokuratury stosownie zawiadomienie.¹²⁰ Innym przykładem z tej kategorii spraw może być przypadek udostępnienia przez operatora telefonii komórkowej informacji o numerze telefonu komórkowego osobie nieupoważnionej. Organ ustalił, że jeden z pracowników tego operatora, którego abonentem była osoba skarżąca, dokonał wglądu w dane osobowe abonenta, które nie było związane ze świadczeniem jakiegokolwiek usługi. W tym przypadku administrator danych wyciągnął konsekwencje służbowe wobec pracownika odpowiedzialnego za owo nielegalne przetwarzanie danych.¹²¹

Generalny Inspektor Ochrony Danych Osobowych badał również problem zasadności, skierowanego do operatora w trybie art. 33 ustawy, żądania udostępnienia m.in. kopii umów i korespondencji prowadzonej z operatorem oraz kopii nagrań rozmów telefonicznych. W tym przypadku GODO uznał, iż taki wniosek nie zasługuje na uwzględnienie.¹²² Żądanie dotyczące

przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19 (ust. 5).

¹¹⁸ Np. GI-DOLiS-430/397/07

¹¹⁹ Zgodnie z art. 51 ustawy, ten, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (ust. 2). Zgodnie z art. 52 ustawy, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabránieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

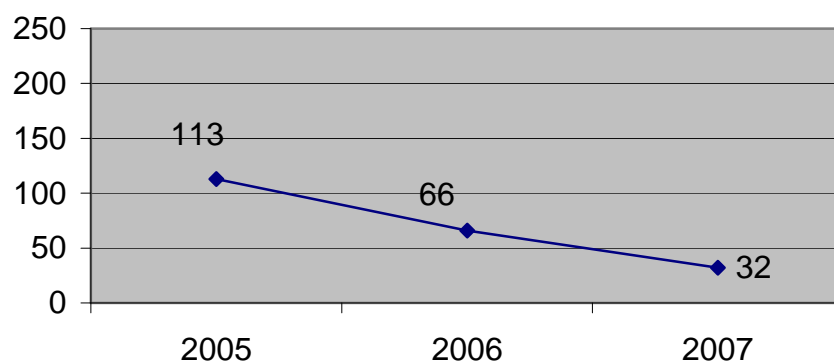
¹²⁰ Pismo z dnia 14 grudnia 2007 r. o sygn. DOLiS-440/165/07/7031

¹²¹ GI-DOLiS-430/39/07

¹²² Decyzja z dnia 12 października 2007 r. o sygn. GI-DEC-DOLiS-217/07/5785,5786

przekazania dokumentów nie może być uznane za sposób realizacji uprawnień, o których mowa w art. 32 ust. 1 pkt. 1-5a ustawy. Żaden jej przepis nie upoważnia bowiem osoby, której dane dotyczą, do żądania od administratora danych wydania nośników danych – w tym dokumentów lub ich kopii. Osoba, której dane dotyczą, może skutecznie dochodzić od administratora wyłącznie udostępnienia dotyczących jej danych osobowych, co nie jest tożsame z żądaniem wydania dokumentów zawierających te dane. Powyższe stanowisko potwierdził również Wojewódzki Sąd Administracyjny w Warszawie, który w uzasadnieniu wyroku z dnia 6 września 2005 r. stwierdził, że „ustawodawca posługuje się pojęciem >udostępnienia<, odnosząc je zawsze do danych osobowych, a nie do zawierających je dokumentów”.¹²³

Podsumowując, w 2007 r. utrzymała się tendencja spadkowa w liczbie skarg wpływających do Generalnego Inspektora Ochrony Danych Osobowych dotyczących sektora telekomunikacji.



Wykres 14: Zestawienie porównawcze liczby skarg dotyczących sektora telekomunikacji, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2005-2007.

Bez wątpienia świadczy to o skuteczności dotychczasowych działań organu w zakresie rozpowszechniania wiedzy o przepisach regulujących proces przetwarzania danych osobowych wśród administratorów danych z tego sektora oraz o tym, że z wielu przypadków naruszenia ustawy stwierdzonych w latach ubiegłych, operatorzy telekomunikacyjni wyciągnęli wnioski i skutecznie wyeliminowali przyczyny ich powstawania. Odnotować należy, iż w analizowanym okresie GODO nie stwierdził – często spotykanych w latach poprzednich – skarg na bezprawne udostępnienie zastrzeżonych numerów telefonów. Ponadto zmniejszył się wpływ skarg dotyczących bezprawnego przetwarzania danych osobowych w związku z niezasadnym – w ocenie osób skarżących – dochodzeniem należności. Przypisać należy to utrwalonemu od lat stanowisku GODO oraz

¹²³ Wyrok z dnia 6 września 2005 r. (sygn. akt II SA 825/05)

orzecznictwu sądowo-administracyjnemu¹²⁴. Podobnie jak w roku 2006, do GIODO nie wpłynęły skargi na niewykonanie przez operatorów obowiązku informacyjnego bądź źle sformułowaną klauzulę zgody na przetwarzanie danych.

9) Sektor zatrudnienia

Podobnie jak w latach ubiegłych, przeważająca część skarg z analizowanego sektora dotyczyła udostępniania przez pracodawców (administratorów danych) osobom trzecim danych osobowych pracowników i byłych pracowników ze zbiorów danych utworzonych w związku z zatrudnieniem, a także przetwarzania danych osobowych w procesie rekrutacji.

W 2007 r. pojawił się również problem pozyskiwania danych osobowych przez pracodawców za pomocą różnego rodzaju kwestionariuszy w zakresie szerszym niż wynika to z powszechnie obowiązujących przepisów prawa (art. 22¹ § 1 Kodeksu pracy, rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika¹²⁵). W jednej z takich spraw¹²⁶ GIODO ustalił, iż pracodawca pozyskiwał m.in. takie dane osobowe pracowników jak te, w jakim miejscu zamieszkuje pracownik (własny dom, wynajmowany dom, u rodziców, akademik, mieszkanie służbowe), z jakiego środka transportu korzysta (pieszo, komunikacja miejska, firmowy samochód, własny transport), jakiego jest wyznania, jaką ma wagę, wzrost, stan wzroku (normalny, plus, minus) oraz grupę krwi. Efektem zainteresowania się sprawą przez GIODO były usunięcie przez pracodawcę danych pozyskanych w zakresie szerszym niż pozwalają na to przepisy prawa oraz zmiana treści stosowanego kwestionariusza w celu dostosowania go do obowiązujących przepisów.

W innej z tego typu spraw¹²⁷ organ wszczął postępowanie mające za przedmiot zbadanie legalności pozyskiwania i przetwarzania przez jedną ze szkół wyższych danych osobowych jej pracowników naukowych pozyskiwanych za pomocą „Arkusza okresowej oceny nauczyciela akademickiego”, a zwłaszcza części zatytułowanej „Działalność poza uczelnią” W ten sposób szkoła gromadziła m.in. informacje „o dodatkowej pracy zarobkowej o charakterze stałym, wykonywanej poza uczelnią”, działalności dydaktycznej wykonywanej poza uczelnią, działalności „na rzecz nauki i dydaktyki wykonywanej poza uczelnią”, pełnionych funkcjach z wyboru w krajowych i międzynarodowych towarzystwach naukowych, stowarzyszeniach i organizacjach zawodowych oraz

¹²⁴ Np.: wyrok WSA w Warszawie z dnia 21 września 2005 r. (sygn. akt II SA/Wa 1443/05), wyrok NSA z dnia 4 października 2005 r. (sygn. akt I OSK 667/05), wyrok WSA w Warszawie z dnia 16 listopada 2005 r. (sygn. akt II SA/Wa 138/05)

¹²⁵ Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286 z późn. zm.)

¹²⁶ GI-DOLiS-430/181/07

działalności niezarobkowej w instytucjach państwowych i samorządowych. W tym przypadku GODO nie stwierdził jednak działania sprzecznego z ustawą o ochronie danych osobowych. Ustalił bowiem, że podstawą prawną przetwarzania danych osobowych są w tym przypadku postanowienia ustawy Prawo o szkolnictwie wyższym, a konkretnie art. 132 ust. 2¹²⁸, który odsyła do statutu uczelni jako dokumentu regulującego szczegółowo tę kwestię. Z kolei § 98 pkt 4 Statutu tej konkretnej placówki wskazuje, że szczegółowe kryteria i tryb dokonywania oceny nauczycieli akademickich określa regulamin uchwalony przez senat. Senat zaś 22 lutego 2007 r. uchwalił „Regulamin oceny nauczycieli akademickich”, który w pkt. 4 wskazuje, że do oceny pracownika wykorzystuje się „Arkusze okresowej oceny nauczyciela akademickiego ” obejmujący m.in. analizowane przez GODO informacje o działalności poza uczelnią. Ponadto z art. 129 Prawa o szkolnictwie wyższym wynika, że nauczyciel akademicki ma obowiązek zawiadomienia rektora o podjętym dodatkowym zatrudnieniu i wymiarze czasu pracy lub prowadzeniu działalności gospodarczej.

Powyższe okoliczności nakazywały Generalnemu Inspektorowi Ochrony Danych Osobowych stwierdzenie, iż nie było podstaw do zakwestionowania – z punktu widzenia przepisów ustawy o ochronie danych osobowych – zakresu danych osobowych pozyskiwanych przez uczelnię w opisany sposób.

GODO analizował również skuteczność kierowanych do niedoszłych pracodawców (po zakończeniu postępowania kwalifikacyjnego) żądań usunięcia danych osobowych pozyskanych podczas rekrutacji. Reprezentował przy tym pogląd, że przetwarzanie danych po zakończeniu procesu rekrutacji, który nie zakończył się zatrudnieniem dysponenta danych osobowych, nie znajduje uzasadnienia w przepisach ustawy o ochronie danych osobowych, a uzyskane w ten sposób dane powinny być usunięte. Ustalił bowiem cel, dla którego zostały pozyskane.¹²⁹

W tym miejscu należy również wspomnieć o badanym przez GODO zagadnieniu legalności pozyskiwania przez przyszłego pracodawcę danych osobowych w czasie postępowania konkursowego na stanowisko w administracji publicznej (samorządzie gminnym) bez zgody kandydata, tj. osoby, której dane dotyczą. Konkretnie chodziło o prawo burmistrza do samodzielnego występowania i pozyskiwania danych osobowych osoby ubiegającej się o stanowisko w administracji samorządowej od byłych pracodawców takiej osoby. GODO uznał w tym przypadku, iż takie działanie jest legalne, gdyż ma uzasadnienie w art. 22¹ § 1 i 2 Kodeksu pracy oraz art. 3 ust. 3 pkt 3 ustawy o pracownikach samorządowych¹³⁰ i jako takie spełnia przesłankę z art. 23 ust. 1 pkt 2 ustawy o ochronie danych

¹²⁷ GI-DOLiS-430/441/07

¹²⁸ Zgodnie z art. 132 ust. 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2005 r. Nr 164, poz. 1365 z późn. zm.), oceny dokonuje podmiot wskazany w statucie, nie rzadziej niż raz na cztery lata lub na wniosek kierownika jednostki organizacyjnej, w której nauczyciel akademicki jest zatrudniony.

¹²⁹ Pismo z dnia 12 lipca 2007 r. o sygn. GI-DOLiS-430/91/07/4008

¹³⁰ Zgodnie z art. 3 ust. 3 pkt 3 ustawy z dnia 22 marca 1990 r. o pracownikach samorządowych (Dz. U. z 2001 r. Nr 142, poz. 1593 z późn. zm.), pracownikiem samorządowym zatrudnionym na stanowisku urzędniczym może być osoba zatrudniana na podstawie art. 2 pkt. 2 i 4, która spełnia wymagania określone w ust. 1 oraz dodatkowo cieszy się nieposzlakowaną opinią.

osobowych. Zbieranie informacji od byłych pracodawców miało bowiem na celu ustalenie, czy ewentualny przyszły pracownik spełnia przesłankę posiadania nieposzlakowanej opinii. Odnośnie do tego zagadnienia wypowiedział się również WSA w Warszawie, który podzielił stanowisko reprezentowane przez GODO.¹³¹

Przedmiotem analizy była również legalność żądania przez Izbę Aptekarską przedstawienia przez osobę ubiegającą się o możliwość prowadzenia apteki ogólnodostępnej „imiennej listy przewidywanego personelu fachowego apteki wraz adresami dotychczasowych miejsc pracy oraz prywatnymi telefonami tych osób” przed zaopiniowaniem przez Izbę Aptekarską wniosku o wydanie zezwolenia na prowadzenie apteki¹³². Organ przeprowadził postępowanie, w wyniku którego ustalił, iż ww. podmiot nie legitymuje się podstawami prawnymi do pozyskania żądanych danych przed zaopiniowaniem wspomnianego wniosku. Przepisy prawa nie warunkują wydania opinii od udostępnienia takich danych. W konsekwencji w wydanej decyzji administracyjnej zakazano Izbie Aptekarskiej pozyskiwania danych osobowych przyszłych pracowników apteki w związku z opiniowaniem wniosku o wydanie zezwolenia na jej prowadzenie.¹³³

Ponadto w roku 2007 r. Generalny Inspektor podjął u Ministra Sprawiedliwości - Prokuratora Generalnego interwencję w związku z wystąpieniem posłów na Sejm RP do organu ochrony danych osobowych. Celem tej interwencji było spowodowanie, aby podlegli Ministrowi Sprawiedliwości prokuratorzy przeprowadzili czynności wyjaśniające nieprawidłowości w procesie przetwarzania danych osobowych zawartych w dokumentacji pracowniczej byłych pracowników Huty Szkła „J.”. Zachodziło bowiem podejrzenie popełnienia przestępstwa z art. 51 ustawy o ochronie danych osobowych polegającego na umożliwieniu dostępu do danych osobom nieupoważnionym lub przestępstwa określonego w art. 52 tej ustawy¹³⁴ polegającego na naruszeniu obowiązku zabezpieczenia danych przed zabraniami przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.¹³⁵ Działanie to okazało się skuteczne. GODO został poinformowany przez Zastępcę Prokuratora Generalnego, iż w przedstawionej sprawie prokuratura podjęła działania zmierzające do jej procesowego rozpoznania¹³⁶. Aktualnie GODO oczekuje na informacje o wynikach tych działań.

¹³¹ Wyrok z dnia 5 czerwca 2007 r. (sygn. akt II SA/Wa 8/07)

¹³² GI-DOLiS-430/325/07

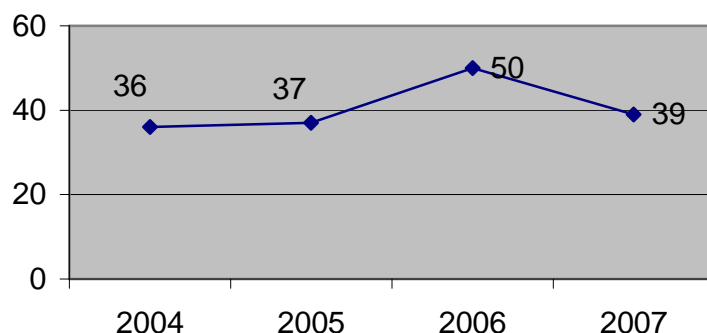
¹³³ Decyzja z dnia 17 września 2007 r. o sygn. GI-DEC-DOLiS-197/07/5291

¹³⁴ Zgodnie z art. 52 ustawy o ochronie danych osobowych, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniami przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

¹³⁵ Pismo z dnia 27 sierpnia 2007 r. o sygn. GI-DOLiS-430/487/07/4873

¹³⁶ Pismo z dnia 5 września 2007 r. o sygn. PR III Ko 3586/07

W analizowanym okresie, w stosunku do roku poprzedniego, nieznacznie spadła liczba skarg dotyczących przetwarzania danych przez pracodawców w szeroko rozumianym sektorze zatrudnienia, zbliżając się do stanu odnotowanego w latach 2004 i 2005.



Wykres 15: *Zestawienie porównawcze liczby skarg dotyczących sektora zatrudnienia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2004-2007.*

Dodać przy tym trzeba, że podobnie jak w latach ubiegłych, skargi z tego sektora często obejmowały zarzut naruszenia dóbr osobistych osób skarżących bądź nieprawidłowego prowadzenia akt pracowniczych. W każdym z takich przypadków organ ochrony danych osobowych informował o swojej niewłaściwości co do roszczeń cywilnych oraz konieczności skierowania sprawy na drogę sądową. Natomiast w sprawach, w których kwestionowano prawidłowość prowadzenia przez pracodawców dokumentacji pracowniczej bądź zasadność umieszczenia określonych informacji w treści akt osobowych, wskazywano, iż właściwy do badania problemu prawidłowości prowadzenia przez pracodawcę akt pracowniczych jest sąd powszechny, i że zastosowane być powinny przepisy procedury cywilnej.¹³⁷

10) Inne

Wśród skarg badanych przez GIODO w 2007 r. była grupa zagadnień, których nie można było zakwalifikować do żadnego z omówionych wcześniej rozdziałów, ale sprawy, w których organ musiał dokonać rozstrzygnięcia, były na tyle istotne, że należało je przedstawić w niniejszym Sprawozdaniu.

W omawianym okresie wiele problemów dotyczyło przetwarzania danych osobowych osób publicznych w toku przygotowywania i publikowania materiałów prasowych. W analizowanych skargach pojawiały się dwie kwestie, tj. ocena legalności udostępniania przez podmioty publiczne informacji o swoich pracownikach (osobach publicznych) dziennikarzom w kontekście ustawy o dostępie do

informacji publicznej¹³⁸ oraz ocena legalności publikowania (ujawniania) tych danych w materiałach prasowych¹³⁹.

W pierwszym przypadku zasadnicze znaczenia miało ustalenie przez organ relacji między postanowieniami ustawy o ochronie danych osobowych a ustawą o dostępie do informacji publicznej, w drugim zaś zbadanie, czy zastosowanie miała w konkretnym przypadku tzw. klauzula prasowa, tj. art. 3a ust. 2 ustawy o ochronie danych osobowych¹⁴⁰, który ogranicza jej stosowanie m.in. w odniesieniu do prasowej działalności dziennikarskiej w rozumieniu ustawy Prawo prasowe¹⁴¹, gdy nie narusza to istotnie praw i wolności osoby, której dane dotyczą.

GIODO stanął na stanowisku, że udostępnienie dziennikarzowi przez instytucję publiczną informacji (danych osobowych) ściśle związanych ze sprawowaną przez konkretnego pracownika funkcją publiczną i stanowiących w związku z tym informację publiczną w rozumieniu ustawy o dostępie do informacji publicznej, stanowiło realizację prawa dostępu obywateli do tego typu informacji i jako takie wypełniało przesłankę legalnego przetwarzania danych osobowych z punktów 4 i 5 art. 23 ust. 1 ustawy o ochronie danych osobowych¹⁴². Badając natomiast przypadki publikowania danych w materiale prasowym, w każdej z tego typu spraw GIODO stwierdzał zastosowanie wspomnianego art. 3a ust. 2 ustawy o ochronie danych osobowych wyłączającego możliwość oceny tego rodzaju przetwarzania danych w kontekście regulacji ustawy o ochronie danych osobowych.¹⁴³

GIODO prowadził również postępowania, w wyniku których ustalano, że kwestionowane przez osobę skarżącą przetwarzanie danych osobowych odbywało się w celach osobistych lub domowych¹⁴⁴. W jednej z takich spraw, wskazana w skardze osoba, niezgodnie z ustawą o ochronie danych osobowych weszła w posiadanie danych osobowych na podstawie nr rejestracyjnego samochodu będącego własnością osoby skarżącej, tj. z bazy danych właścicieli pojazdów. Organ wszczął stosowne postępowanie wyjaśniające w tej sprawie. Na podstawie materiału dowodowego ustalono, iż w rzeczywistości wskazana w skardze osoba weszła w posiadanie danych osobowych osoby skarżącej nie wskutek ich pozyskania z bazy danych właścicieli pojazdów, ale od członka swojej rodziny. Ponadto ustalono, iż w analizowanej sprawie nie miało miejsca przetwarzanie danych w zbiorach danych

¹³⁷ Np. GI-DOLiS-430/373/07

¹³⁸ Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. Nr 112, poz. 1198 z późn. zm.)

¹³⁹ Np. GI-DOLiS-430/572/06, GI-DOLiS-430/298/07, GI-DOLiS-430/297/07

¹⁴⁰ Zgodnie z art. 3a ust. 2 ustawy o ochronie danych osobowych, z wyjątkiem przepisów art. 14-19 i art. 36 ust. 1, nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. Nr 5, poz. 24 z późn. zm.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

¹⁴¹ Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24 z późn. zm.)

¹⁴² Zgodnie z art. 23 ust. 1 pkt. 4 i 5 ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (pkt 4) lub dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (pkt 5).

¹⁴³ Np. GI-DS-430/572/06

¹⁴⁴ Np. GI-DOLiS-430/53/07

osobowych oraz nie doszło do dalszego udostępnienia danych innym osobom (podmiotom). Powyższe ustalenia nakazywały uznać zatem, że przetwarzano dane w celach osobistych. Zgodnie zaś z art. 3a ust. 1 ustawy o ochronie danych osobowych¹⁴⁵, w takich przypadkach ustawy tej nie stosuje się.

W innej z rozpatrywanych spraw pojawiło się pytanie o legalność pozyskiwania danych osobowych z dowodu osobistego klienta dokonującego w sklepie płatności za pomocą karty płatniczej¹⁴⁶. GODO ustalił, że powyższego przetwarzania dokonywano w celu potwierdzenia tożsamości okaziciela karty płatniczej. Działanie to znajdowało podstawy w odpowiednich przepisach prawa, a mianowicie art. 8 ust. 1 pkt 2 i art. 10 ust. 1 ustawy o elektronicznych instrumentach płatniczych¹⁴⁷ i jako takie zgodne było z ustawą o ochronie danych osobowych (art. 23 ust. 1 pkt 2).

W analizowanym okresie GODO był również adresatem żądań dotyczących nakazania administratorowi danych usunięcia posiadanych przez niego kopii różnego rodzaju dokumentów zawierających dane osobowe. W każdej z tego typu spraw GODO oceniał takie żądanie za bezzasadne. Ustawa o ochronie danych osobowych reguluje bowiem kwestię przetwarzania, a więc m.in. usuwania danych osobowych, a nie ich nośników, w tym np. fotokopii dokumentów zawierających dane osobowe. Stanowisko takie poparł również Wojewódzki Sąd Administracyjny w Warszawie, który w wyroku z dnia 6 września 2005 r. wskazał, że „w ustawie o ochronie danych osobowych brak jest przepisów obligujących administratora do udostępnienia dokumentów zawierających dane osobowe. Ustawodawca posługuje się pojęciem >udostępnienia<, odnosząc je zawsze do danych osobowych, a nie do zawierających je dokumentów”¹⁴⁸. Analizując takie sprawy, GODO nie stwierdził również przypadków przetwarzania danych osobowych w zakresie szerszym niż pozwalają na to obowiązujące przepisy prawa, co mogłoby skutkować ewentualnym nakazaniem usunięcia takich danych.

W 2007 r. pojawiły się również sprawy, w których materiał dowodowy zgromadzony w toku postępowania administracyjnego uzasadniał podejrzenie popełnienia czynu zagrożonego odpowiedzialnością karną z ustawy o ochronie danych osobowych. W takich przypadkach GODO kierował stosowane zawiadomienia do właściwych prokuratur. Jedno z nich dotyczyło np. stwierdzonego przez organ opublikowania bez podstawy prawnej przez osobę prywatną na stronie internetowej imienia, nazwiska adresu zamieszkania oraz numeru telefonu dużej liczby abonentów jednego z operatorów telefonii stacjonarnej, bez zgody tych osób oraz bez spełnienia wobec nich

¹⁴⁵ Zgodnie z art. 3a ust. 1, ustawy o ochronie danych osobowych nie stosuje się do osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych.

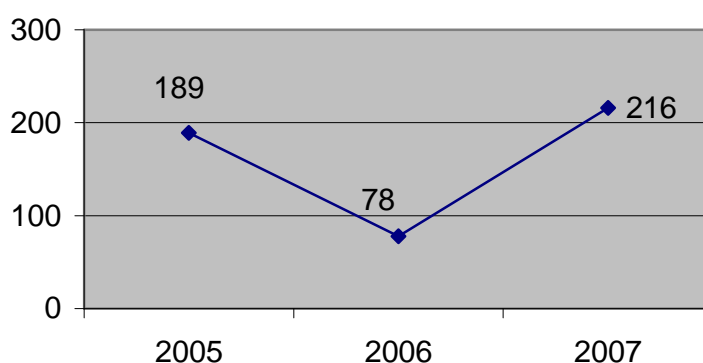
¹⁴⁶ GI-DOLiS-430/262/07

¹⁴⁷ Zgodnie z art. 8 ust. 1 pkt 2 ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. Nr 169, poz. 1385 z późn. zm.), umowa pomiędzy agentem rozliczeniowym a akceptantem o przyjmowanie zapłaty przy użyciu elektronicznych instrumentów płatniczych powinna określać w szczególności stosowane procedury, w tym procedury bezpieczeństwa, oraz obowiązki akceptanta w związku z dokonywaniem operacji. Zgodnie zaś z art. 10 ust. 1 tej ustawy, akceptant może żądać, aby posiadacz elektronicznego instrumentu płatniczego lub użytkownik karty płatniczej okazał dokument stwierdzający tożsamość w razie uzasadnionych wątpliwości co do jego tożsamości.

¹⁴⁸ Sygn. akt II SA/Wa 825/05

obowiązku informacyjnego z art. 25 ustawy. W ocenie GODO, takie działanie wypełniało znamiona czynów określonych w art. 49 oraz 54 ustawy o ochronie danych osobowych¹⁴⁹ i dlatego skierował do prokuratury zawiadomienie o podejrzeniu popełnienia przestępstwa¹⁵⁰.

Podsumowując powyższy rozdział należy odnotować, iż mimo dużej liczby skarg, które wpłynęły do GODO w 2007 r., w stosunku do lat ubiegłych znacznie zmniejszyła się liczba przypadków, w których organ stwierdził naruszenie ustawy o ochronie danych osobowych. Wynikać to może z konsekwentnej polityki informacyjnej GODO zmierzającej do upowszechnienia wiedzy o prawach i obowiązkach zarówno administratorów danych, jak i osób, których dane dotyczą.



Wykres 16: *Zestawienie porównawcze liczby skarg z sektora Inne, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2005–2007.*

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

Jednymi z ustawowych zadań Generalnego Inspektora Ochrony Danych Osobowych są prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach¹⁵¹. Zadania te, realizowane w Departamencie Rejestracji Zbiorów Danych Osobowych Biura Generalnego

¹⁴⁹ Zgodnie z art. 49 ustawy, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (ust. 1). Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3 (ust. 2).

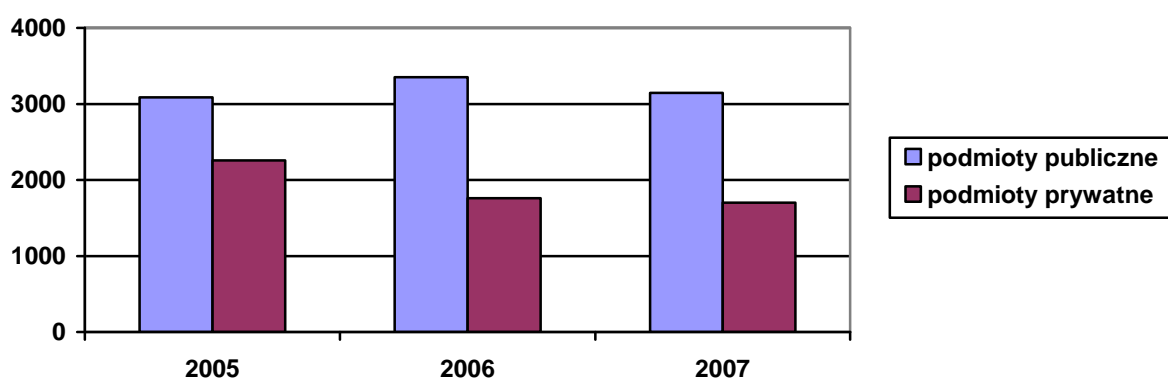
Zgodnie z art. 54 ustawy, kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

¹⁵⁰ Pismo z dnia 3 grudnia 2007 r. o sygn. DOLiS-440-107/07/6765

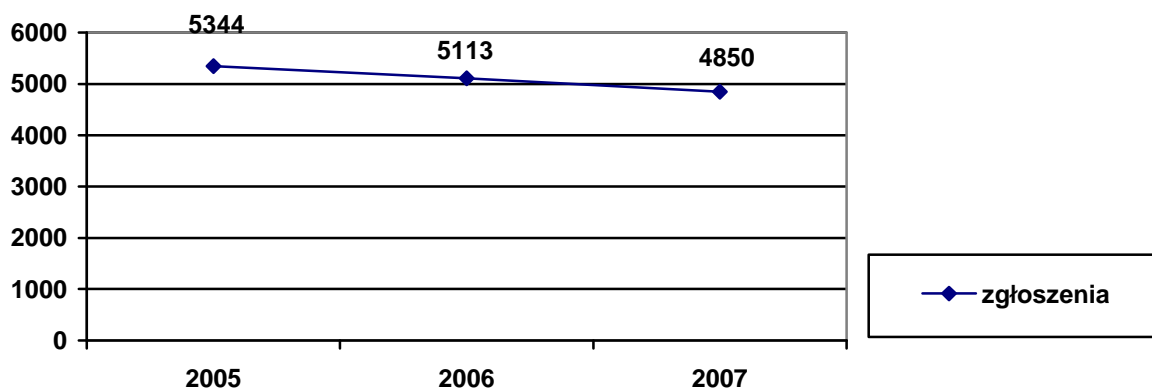
¹⁵¹ Zadania Generalnego Inspektora zostały określone w art. 12 ustawy.

Inspektora Ochrony Danych Osobowych, skorelowane zostały z nałożonym na administratorów danych obowiązkiem zgłaszania zbiorów danych osobowych do rejestracji¹⁵². Prowadzenie ogólnokrajowego rejestru zbiorów danych osobowych umożliwia Generalnemu Inspektorowi m.in. sprawowanie kontroli nad prawidłowością procesu przetwarzania danych osobowych, a także zapewnia obywatelom dostęp do informacji o administratorach danych i prowadzonych przez nich zbiorach danych osobowych. Na stronie internetowej www.giodo.gov.pl, w ramach Platformy e-GIODO, zamieszczone są informacje o zarejestrowanych zbiorach danych osobowych umożliwiające wyszukanie zbiorów danych według podstawowych kryteriów, m.in. nazwy administratora danych, miejscowości czy nazwy zbioru danych.

W roku 2007 administratorzy danych zgłosili do rejestracji **4850 zbiorów**, z czego podmioty z sektora administracji publicznej zgłosiły 3149 zbiorów, co stanowi 65% ogólnej liczby zgłoszeń dokonanych w tym okresie, a podmioty z sektora prywatnego 1701 zbiory, co stanowi 35% ogólnej liczby zgłoszonych zbiorów.



Wykres 17: *Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2005-2007 przez podmioty z sektora publicznego i prywatnego.*



¹⁵² Zgodnie z art. 40 ustawy, administrator danych obowiązany jest zgłosić zbiór danych do rejestracji, z wyjątkiem przypadków określonych w art. 43 ust. 1 ustawy.

Wykres 18: Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2005-2007.

Można stwierdzić, że liczba zgłoszonych zbiorów od roku 2005 wciąż utrzymuje się na wysokim poziomie.

Wśród zgłoszeń dokonanych przez podmioty z sektora publicznego (podobnie jak w roku 2006) dominującymi pod względem ilościowym były zgłoszenia zbiorów danych osób, w odniesieniu do których wydawane są orzeczenia o niepełnosprawności oraz orzeczenia o wskazaniu do ulg i uprawnień osób posiadających orzeczenia o inwalidztwie lub niezdolności do pracy, jak również zgłoszenia związane z realizacją szeroko rozumianej pomocy społecznej. Ponadto odnotować należy liczne zgłoszenia pochodzące od jednostek samorządu terytorialnego, zwłaszcza zgłoszenia zbiorów danych osobowych tworzonych w gminach i powiatach. Natomiast wśród podmiotów prywatnych zanotowano wzrost zgłoszeń zbiorów danych osobowych pochodzących od pośredników w obrocie nieruchomościami.

Podobnie jak w latach ubiegłych, część ze zgłoszonych zbiorów danych nie podlegała obowiązkowi rejestracji. Najczęstszą podstawą zwolnienia z obowiązku rejestracji była jedna z przesłanek określonych w art. 43 ustawy. Przykładowo z obowiązku rejestracji zwalniani są administratorzy danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej¹⁵³, zbiorów tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu¹⁵⁴, zbiorów dotyczących osób korzystających z usług medycznych administratora danych¹⁵⁵, jak również zbiorów danych osobowych obecnych i byłych pracowników administratora danych, zbiorów danych osób ubiegających się o zatrudnienie u administratora danych (kandydaci do pracy), zbiorów danych osób zrzeszonych (np. członkowie stowarzyszenia)¹⁵⁶. W 2007 r. przygotowano 121 projektów pism informujących o zwolnieniu administratora danych na podstawie art. 43 ustawy.

Zgłoszenia do rejestracji nadsyłały również podmioty, które nie są administratorami danych zgromadzonych w zgłoszonych zbiorach. Do tych wnioskodawców Generalny Inspektor Ochrony Danych Osobowych skierował 39 pism informujących o braku obowiązku rejestracyjnego z ich strony. Przede wszystkim były to podmioty, którym administratorzy danych powierzyli przetwarzanie danych na podstawie art. 31 ustawy.

Do Generalnego Inspektora wpływały ponadto zgłoszenia zbiorów danych, w stosunku do których przepisy ustawy o ochronie danych osobowych nie miały zastosowania. W większości

¹⁵³ Zgłoszenie nr R 000041/06

¹⁵⁴ Zgłoszenie nr R 000055/07

¹⁵⁵ Zgłoszenie nr R 004943/06

przypadków zgromadzone w takich zbiorach dane dotyczyły przedsiębiorców i były ściśle związane z prowadzoną przez nich działalnością gospodarczą. W związku z tym do wnioskodawców w 2007 r. wysłano 18 pism ze stosowną informacją.

Należy zauważyć, iż w dalszym ciągu administratorzy danych przetwarzanych w zbiorach podlegających obowiązkowi zgłoszenia do rejestracji, przy wypełnianiu formularza zgłoszenia, popełniają wiele błędów. W związku z tym w okresie sprawozdawczym w toku prowadzonych postępowań rejestracyjnych skierowano do wnioskodawców **1760 pism** wskazujących braki w nadesłanych zgłoszeniach. Ujawnione nieprawidłowości dotyczyły w zasadzie wszystkich elementów ujętych w zgłoszeniu. Niemniej wśród najczęściej powtarzających się uchybień należy wymienić:

- nieadekwatny (zbyt szeroki), w stosunku do celu przetwarzania, zakres danych osobowych pozyskiwanych do zbioru – administratorzy dokonujący zgłoszeń zbiorów danych prowadzonych w celach marketingowych niejednokrotnie pozyskiwali dane osobowe w zbyt szerokim zakresie (wnioskodawcy w treści zgłoszeń informowali, iż gromadzą w zbiorach jednocześnie dane w postaci numeru ewidencyjnego PESEL oraz numeru i serii dowodu osobistego, przy czym numer ewidencyjny PESEL jest daną osobową, która w sposób jednoznaczny umożliwia zidentyfikowanie osoby),
- nieprawidłowe wskazanie przesłanki legalności przetwarzania danych – podmioty publiczne, dla których przepisy prawa stanowią, co do zasady, przesłankę upoważniającą je do przetwarzania danych osobowych w związku z wykonywaniem przez nie zadań określonych przepisami prawa, wielokrotnie wskazywały, jako przesłankę legalności, zgodę osoby, której dane dotyczą,
- braki w części zgłoszenia dotyczącej informacji o sposobie wypełnienia warunków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy o ochronie danych osobowych – np. informacji o opracowaniu i wdrożeniu dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki ich ochrony,
- deklarowany przez administratorów danych poziom bezpieczeństwa przetwarzania danych w systemie informatycznym nie spełniał warunków określonych w rozporządzeniu wykonawczym do ustawy¹⁵⁷ - np. administrator danych informował, iż zastosował środki bezpieczeństwa na poziomie podstawowym, mimo iż gromadzi dane określone w art. 27 ustawy i tym samym zobowiązany jest do zastosowania co najmniej podwyższonego poziomu bezpieczeństwa.

Warto podkreślić jednak, iż dzięki udostępnionemu na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych programowi wspomagającemu wypełnianie formularza zgłoszenia (w

¹⁵⁶ Zgłoszenie nr R 000231/07

¹⁵⁷ 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).

ramach Platformy e-GIODO) liczba błędnie wypełnionych zgłoszeń stopniowo maleje. Program ten, poprzez system podpowiedzi i komunikatów o popełnionych błędach, ma na celu minimalizację możliwości nieprawidłowego wypełnienia zgłoszenia. Program wspomagający wypełnianie formularza zgłoszenia jest coraz częściej stosowany przez wnioskodawców. W celu rozpowszechnienia tej formy wypełniania zgłoszenia, w pismach wysyłanych w toku postępowania rejestracyjnego zamieszczana jest informacja o możliwości wypełniania zgłoszeń przy użyciu tego programu. Również podczas konsultacji telefonicznych wnioskodawcy instruowani są o sposobie korzystania z tego programu. W okresie sprawozdawczym zanotowano zatem wzrost liczby zgłoszeń zbiorów danych osobowych wypełnionych przy użyciu ww. programu. Od momentu uruchomienia tego programu do końca 2006 r. odsetek zgłoszeń wypełnionych z jego użyciem wyniósł 16% (370 zgłoszeń), natomiast w roku 2007 r. na 4850 zgłoszeń wykorzystano go 1189 przypadkach, co stanowi 25% ogólnej liczby zgłoszeń. Wypełnianie formularza przy użyciu programu wspomagającego pozwala uniknąć popełnienia wielu błędów, zwłaszcza poprawnie wypełnić zgłoszenie w zakresie sposobu spełnienia wymagań technicznych i organizacyjnych zastosowanych w celu zabezpieczenia zbioru danych osobowych - (części E i F zgłoszenia). Niemniej ww. program nie jest w stanie wyeliminować wszystkich uchybień. Nadal znaczna liczba zgłoszeń zawiera błędy, zarówno formalne (np. brak podpisu pod treścią zgłoszenia), jak i merytoryczne (np. błędna podstawa prawna prowadzenia zbioru danych).

W wyniku prowadzonych postępowań wyjaśniających w większości przypadków dochodzi do rejestracji zbioru – w okresie sprawozdawczym **do rejestru** prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych **zostało wpisanych 2698 zbiorów danych**. Są jednak sytuacje, w których zachodzą przesłanki do wydania decyzji o odmowie rejestracji zbioru danych osobowych¹⁵⁸. W 2007 r. Generalny Inspektor Ochrony Danych Osobowych odmawiał rejestracji zgłoszonego zbioru najczęściej ze względu na:

- naruszenie zasad ochrony danych osobowych, np. brak przesłanki legalności przetwarzania danych, nieadekwatność przetwarzania danych w stosunku do celu ich przetwarzania, przetwarzanie danych wrażliwych¹⁵⁹ bez podstawy prawnej,
- niespełnienie wymogów¹⁶⁰ rozporządzenia wykonawczego do ustawy,
- brak wyczerpującego opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy o ochronie danych osobowych, zwłaszcza informacji dotyczących opracowania i wdrożenia dokumentacji opisującej sposób przetwarzania danych

¹⁵⁸ Przesłanki odmowy rejestracji zbioru danych określone zostały w art. 44 ust. 1 ustawy.

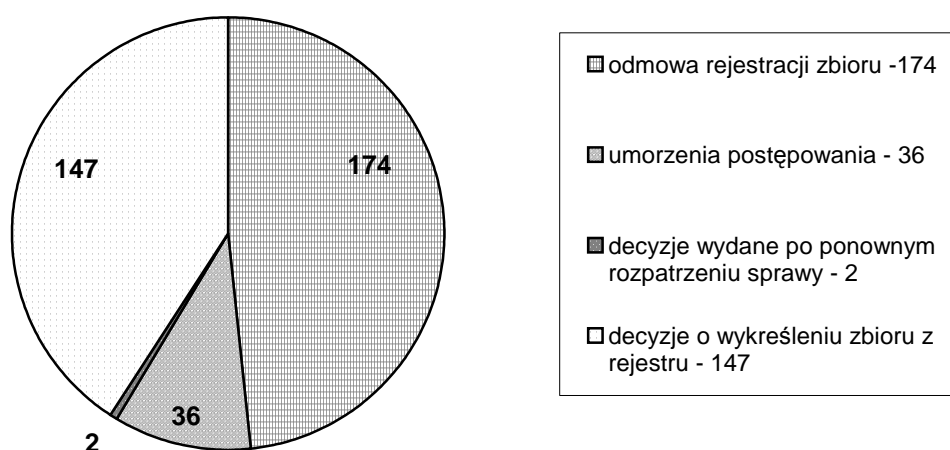
¹⁵⁹ Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

¹⁶⁰ Zgłoszenie nr R 000496/05 – wnioskodawca, mimo połączenia urządzeń systemu informatycznego służącego do przetwarzania danych osobowych z siecią publiczną, nie wprowadził środków bezpieczeństwa na poziomie wysokim.

osobowych, oraz środków ich ochrony, wyznaczenia administratora bezpieczeństwa informacji, nadania upoważnień osobom dopuszczonym do przetwarzania danych osobowych, a także prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

Należy zauważyć, iż obowiązek opracowania i wdrożenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki ich ochrony spoczywa również na administratorach danych przetwarzanych w systemach tradycyjnych. Nie zawsze jednak administratorzy danych w nadsyłanych zgłoszeniach informują o opracowaniu i wdrożeniu ww. dokumentacji, co w rezultacie prowadzi do odmowy rejestracji zgłoszonego zbioru¹⁶¹.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **174 decyzje o odmowie rejestracji zbioru danych, 36 decyzji o umorzeniu postępowania** (np. ze względu na zaprzestanie przetwarzania danych w zbiorze niewpisanym jeszcze do rejestru czy też rezygnację z utworzenia zbioru). **Dwie decyzje wydał po ponownym rozpatrzeniu sprawy**, zaś **147 decyzji dotyczyło wykreślenia zbioru z rejestru** (we wszystkich decyzjach przesłanką wykreślenia było zaprzestanie przetwarzania danych w zarejestrowanym zbiorze).



Wykres 19: *Liczbowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2007 r.*

W 2007 r. Generalny Inspektor Ochrony Danych Osobowych przygotował projekty **104 postanowień**, przy czym największy odsetek stanowiły postanowienia o zwrocie zgłoszenia z tytułu nieuwiszczenia opłaty skarbowej, których w okresie sprawozdawczym było **94** (postanowienia wydane w stosunku do zgłoszeń, które wpłynęły do rejestracji przed 1 stycznia 2007 r.).

W roku sprawozdawczym rozpatrzono **1154 zgłoszenia aktualizacyjne** dokonane przez

¹⁶¹ Zgłoszenie nr R 005085/06

administratorów danych w trybie art. 41 ust. 2 ustawy o ochronie danych osobowych. Aktualizacje dotyczyły najczęściej zmiany siedziby administratora danych, zmiany zakresu przetwarzanych danych, a także zmian dotyczących środków technicznych i organizacyjnych zastosowanych w celu ochrony przetwarzanych danych osobowych (chodzi głównie o przypadki zmiany systemu przetwarzania danych w zbiorze, tj. z systemu tradycyjnego na informatyczny). Należy również zaznaczyć, iż nie zawsze nadsyłane przez administratorów informacje o zmianach w zbiorze powodowały zmiany zapisów w księdze rejestrowej (np. informacje dotyczące zmiany osoby administratora bezpieczeństwa informacji, zmiany liczby danych w zbiorze – zwykle chodzi o większą liczbę klientów administratora).

Prowadzony przez Generalnego Inspektora Ochrony Danych Osobowych ogólnokrajowy, jawny rejestr zbiorów danych osobowych umożliwia obywatelom dostęp do informacji o administratorach danych i zgłoszonych przez nich zbiorach danych osobowych. Zasada jawności rejestru realizowana jest poprzez zapewnienie możliwości przeglądania go w Internecie, a także w siedzibie Generalnego Inspektora Ochrony Danych Osobowych.

W omawianym okresie Generalny Inspektor Ochrony Danych Osobowych wydał ponadto - z urzędu bądź na żądanie administratora danych - **2059 zaświadczeń o zarejestrowaniu zbioru**.

W roku sprawozdawczym, głównie drogą elektroniczną, wpływało wiele pytań dotyczących rejestracji zbiorów danych osobowych, co może świadczyć o rosnącym zainteresowaniu tym zagadnieniem. W związku z tym w okresie od stycznia do grudnia 2007 r. GODO przygotował **53 odpowiedzi na zapytania** dotyczące problematyki rejestracji zbiorów danych osobowych.

Jak wspomniano wyżej, w 2007 r. wśród wniosków o rejestrację pochodzących od przedsiębiorców dominowały zgłoszenia pośredników w obrocie nieruchomościami. Przeważnie nie wymagały one dodatkowych wyjaśnień, z reguły bowiem sporządzane były przy użyciu programu wspomagającego E-GODO. Wśród podmiotów publicznych szczególną aktywność w zakresie zgłaszania zbiorów danych do rejestracji wykazywały podmioty działające w sferze pomocy społecznej. Niestety, mimo precyzyjnych przepisów kompetencyjnych, nie zawsze ich reprezentanci potrafili zinterpretować pojęcie administratora danych przetwarzanych w konkretnym zbiorze. W związku z tym różne jednostki organizacyjne przypisywały sobie status administratora danych. Charakterystyczny przykład stanowiły zgłoszenia zbiorów danych osób, w stosunku do których wydawane były orzeczenia o niepełnosprawności oraz orzeczenia o wskazaniach do ulg i uprawnień osób posiadających orzeczenia o inwalidztwie lub niezdolności do pracy. Takie zbiory zgłaszane były do rejestracji przez Powiatowe Centra Pomocy Rodzinie, Powiatowe Zespoły do Spraw Orzekania o Niepełnosprawności oraz powiaty. Podmioty niebędące w świetle prawa administratorami danych wskazywały jako podstawę swych kompetencji zarządzenia czy regulaminy wewnętrzne określające podział zadań w urzędzie. Tymczasem z treści obowiązujących przepisów, zwłaszcza znowelizowanej

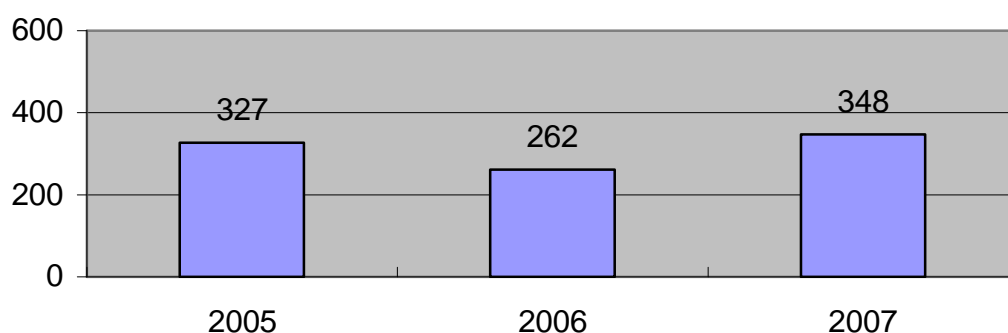
ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych¹⁶² oraz wydanego rozporządzenia wykonawczego do ustawy¹⁶³, wynika, że kompetencje w tym zakresie posiadają powiatowe zespoły do spraw orzekania o niepełnosprawności i to one mają status administratora w stosunku do danych osób niepełnosprawnych. Stąd w toku prowadzonych postępowań wyjaśniających informowano właściwych administratorów danych o ciążyącym na nich obowiązku zgłoszenia do rejestracji zbioru danych osobowych.

Niezmienne rejestrację ww. zbiorów utrudniały liczne uchybienia w części zgłoszenia dotyczącej informacji o sposobie wypełnienia warunków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy o ochronie danych osobowych. Niejednokrotnie także deklarowany poziom bezpieczeństwa przetwarzania danych w systemie informatycznym nie spełniał wymogów określonych w rozporządzeniu wykonawczym do ustawy.

5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych

Istotną rolę w działalności Generalnego Inspektora Ochrony Danych Osobowych odgrywa opiniowanie projektów aktów normatywnych (ustaw oraz rozporządzeń) dotyczących ochrony danych osobowych. Uprawnienie to zostało ustanowione w art. 12 ust. 4 ustawy o ochronie danych osobowych. Dzięki niemu możliwe jest wyeliminowanie nieprawidłowości już na etapie tworzenia prawa.

W analizowanym roku sprawozdawczym do zaopiniowania przez Generalnego Inspektora skierowano **348 projektów aktów prawnych**.



¹⁶² Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. Nr 123, poz. 776 z późn. zm.)

¹⁶³ Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 28 listopada 2007 r. w sprawie warunków, sposobu oraz trybu gromadzenia i usuwania danych w ramach Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności (Dz. U. Nr 228, poz. 1681)

Wykres 20: Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania Generalnemu Inspektorowi Ochrony Danych Osobowych w latach 2005-2007.

Generalnemu Inspektorowi do zaopiniowania przedkładane są nie tylko projekty aktów normatywnych ściśle związane z przetwarzaniem danych osobowych i już w samym tytule niepozostawiające co do tego żadnych wątpliwości (np. *projekt rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie przetwarzania przez Policję informacji o osobach*¹⁶⁴), ale również te związane z tematyką przetwarzania danych osobowych w stopniu nieznacznym, jak choćby projekt *rozporządzenia Ministra Rozwoju Regionalnego w sprawie szczegółowego sposobu dokonywania wydatków związanych z realizacją programów operacyjnych*¹⁶⁵, czy projekt *rozporządzenia Ministra Rolnictwa i Rozwoju Wsi w sprawie szczegółowych sposobów postępowania przy zwalczaniu i zapobieganiu rozprzestrzeniania się bakterii *Clavibacter michiganensis* ssp. *sepedonicus**.¹⁶⁶

Jak co roku, nieprawidłowości z punktu widzenia przepisów ustawy o ochronie danych osobowych dotyczyły braku doprecyzowania zakresu danych osobowych, możliwość przetwarzania których wprowadzały poszczególne projekty.¹⁶⁷ Generalny Inspektor kwestionował takiego rodzaju przepisy ze względu na niebezpieczeństwo naruszenia jednej z naczelnych zasad przetwarzania danych osobowych, którą jest zasada adekwatności (relewantności) danych w stosunku do celów ich przetwarzania.¹⁶⁸ Ponadto Generalny Inspektor sprzeciwiał się wprowadzaniu do polskiego porządku prawnego przepisów przewidujących zbyt długi okres przechowywania danych osobowych i zwracał uwagę na art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych wprowadzający zasadę ograniczenia czasowego przetwarzania danych.¹⁶⁹

¹⁶⁴ GI-DOLiS-023/154/07

¹⁶⁵ GI-DOLiS-023/207/07

¹⁶⁶ GI-DOLiS-023/73/07

¹⁶⁷ Np. projekt ustawy o zmianie ustawy – Kodeks pracy (GI-DOLiS-023/276/07) w jednym z przepisów stanowił o obowiązku przekazywania przez pracodawcę pracownikom „informacji o osobach” wyznaczonych do udzielania pierwszej pomocy oraz wykonywania czynności w zakresie ochrony przeciwpożarowej i ewakuacji pracowników, nie precyzując jednocześnie zakresu tych informacji, oraz projekt rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych (GI-DOLiS-023/131/07); warto odnotować, że rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 217, pod poz. 1614, a uwagi Generalnego Inspektora Ochrony Danych Osobowych zostały w nim uwzględnione.

¹⁶⁸ Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych nakłada na administratora danych przetwarzającego dane obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnienia, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

¹⁶⁹ Wskazane uwagi zostały zgłoszone m.in. do projektu rozporządzenia Ministra Finansów w sprawie szczegółowego zakresu przetwarzanych informacji dotyczących osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów oraz trybu usuwania tych informacji (GI-DOLiS-023/50/07) przewidującego 12-letni okres przechowywania przez banki i inne instytucje ustawowo upoważnione do udzielania kredytów, bez zgody ich klientów, informacji stanowiących tajemnicę bankową, w tym danych osobowych, po wygaśnięciu zobowiązań wynikających z umów zawartych przez tych klientów z bankami (§ 4 ust. 2);

W okresie objętym sprawozdaniem Generalny Inspektor uczestniczył w pracach nad projektem *ustawy o zmianie ustawy o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944 – 1990 oraz treści tych dokumentów*. W ich toku organ do spraw ochrony danych osobowych zwrócił uwagę na art. 1 pkt 18 ppkt 35 nowelizujący art. 71 ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz. U. Nr 155, poz. 1016 z późn. zm.). Nowelizacja ta przewidywała wyłączenie stosowania wobec Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (dalej „IPN”) przepisów ustawy o ochronie danych osobowych. Generalny Inspektor podkreślił, że zapisy tej ustawy są w generalnych założeniach zgodne ze standardami europejskimi oraz wypełniają delegację, o której mowa w art. 51 ust. 5 Konstytucji RP. Ustawa o ochronie danych osobowych implementuje bowiem do polskiego porządku prawnego postanowienia dyrektywy Parlamentu Europejskiego i Rady nr 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, która wyznacza europejskie normy w tej dziedzinie. Generalny Inspektor zaznaczył, że przyjęta w projekcie koncepcja całkowitego wyłączenia stosowania wobec IPN przepisów ustawy o ochronie danych osobowych spowodować może postawienie przez instytucje europejskie zarzutu niewypełniania przez Rzeczpospolitą Polską, wbrew istniejącemu obowiązkowi, europejskich wymagań w zakresie ochrony danych osobowych, zwłaszcza że opiniowana ustawa nie zawiera własnych unormowań dotyczących zabezpieczeń zbiorów danych osobowych przetwarzanych przez IPN, a jej wejście w życie uchyli w stosunku do IPN obowiązywanie wszelkich regulacji w tym zakresie. Wskazał jednocześnie, iż w sytuacji, gdyby zamiarem ustawodawcy było przyznanie IPN szczególnego statusu, niestosowanego w przypadku innych instytucji publicznych, niezbędne jest zamieszczenie w ustawie o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu całościowej regulacji dotyczącej zabezpieczeń prowadzonych przez tenże zbiorów danych osobowych.¹⁷⁰

W czasie opiniowania projektów aktów prawnych Generalny Inspektor zakwestionował również niektóre propozycje przepisów przedstawione w **projekcie ustawy o zawodzie farmaceuty**.¹⁷¹ Wątpliwości z punktu widzenia zgodności z przepisami ustawy o ochronie danych osobowych budził m.in. wprowadzony do wymienionego projektu przepis odnoszący się do zwolnienia farmaceuty z obowiązku zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z

uwagi Generalnego Inspektora zostały uwzględnione, a rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 56, pod poz. 373. Niemniej przepis przyznający tym podmiotom prawo do przechowywania takich informacji przez 12 lat dla celów stosowania metod statystycznych wprowadzono – wbrew stanowisku Generalnego Inspektora – do ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm., a konkretnie art. 105a ust. 5 Prawa bankowego).

¹⁷⁰ GI-DOLiS-023/7/07; uwagi Generalnego Inspektora nie zostały uwzględnione (stosownych zmian do ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu także nie wprowadzono), a nowelizację ustawy opublikowano w Dzienniku Ustaw z 2007 r. Nr 165 pod poz. 1171.

¹⁷¹ GI-DOLiS-023/167/07

wykonywaniem czynności zawodowych, w przypadku, gdy jest to niezbędne dla celów naukowych. Generalny Inspektor podkreślił wówczas szczególne znaczenie informacji dotyczących stanu zdrowia dla prywatności osoby, której dane dotyczą. Wskazał kolejny raz na fakt, iż przetwarzanie danych osobowych szczególnie chronionych jest dopuszczalne, gdy zezwalający na powyższe przepis rangi ustawy stwarza pełne gwarancje ochrony tych danych.¹⁷² Podkreślił przy tym, że omawiany wyjątek od generalnej zasady zakazu przetwarzania tej kategorii danych osobowych dotyczy jedynie przepisów, których, po pierwsze, brzmienie nie pozostawia wątpliwości w kwestii uchylenia zakazu przetwarzania danych, po drugie – wyraźnie wskazujących, iż przetwarzanie danych osobowych jest dopuszczalne bez zgody osoby, której dane dotyczą, i po trzecie i najważniejsze, które stwarzają pełne gwarancje ochrony, przez co należy rozumieć gwarancje ochrony wrażliwych danych osobowych. Dopiero wówczas, gdy określony przepis spełnia wszystkie powyższe warunki łącznie, można go uznać za podstawę do przetwarzania, w tym ujawniania przez administratora danych dotyczących osoby. Generalny Inspektor skonstatował, że projektowany przepis, jako przewidujący możliwość ujawnienia informacji o stanie zdrowia dotyczących pacjenta zawsze wtedy, gdy jest to „niezbędne dla celów naukowych” bez jakichkolwiek dodatkowych ograniczeń, nie spełnia wymienionych wyżej warunków, gdyż nie gwarantuje ochrony tych danych. Wskazał przy tym na niektóre przepisy Konstytucji Rzeczypospolitej Polskiej dotyczące ingerencji w sferę prywatności jednostek¹⁷³ oraz na orzecznictwo Trybunału Konstytucyjnego dotyczące przesłanek, po spełnieniu których istnieje możliwość ingerencji w sferę prywatności jednostek.¹⁷⁴ Opiniując projektowany przepis, Generalny Inspektor Ochrony Danych Osobowych podkreślił, iż możliwość przetwarzania danych m.in. o stanie zdrowia dla celów naukowych została już w polskim porządku prawnym przewidziana. Wprowadziła ją ustawa o ochronie danych osobowych, która jednocześnie zastrzega, że publikowanie wyników tego typu badań nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone.¹⁷⁵

Kolejną kwestionowaną w tym projekcie regulacją był przepis nakładający na obywatela państwa należącego do Europejskiego Obszaru Gospodarczego [dalej: EOG], innego niż Polska, zainteresowanego uzyskaniem prawa do wykonywania zawodu farmaceuty na terytorium Rzeczypospolitej Polskiej, obowiązek złożenia oświadczenia przed Prezesem Naczelnej Rady

¹⁷² Art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych

¹⁷³ Zgodnie z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej, 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.

¹⁷⁴ Np. wyrok Trybunału Konstytucyjnego z dnia 20 listopada 2002 r. (sygn. akt K 41/02), w którym Trybunał orzekł, iż wkroczenie w prywatność jednostki jest działaniem konstytucyjnym, o ile jest konieczne dla osiągnięcia wskazanych w art. 31 ust. 3 Konstytucji RP celów, które jedynie są władne uzasadnić naruszenie praw i wolności jednostki i przy tym jest środkiem najmniej dotkliwym dla osoby, której wolność lub prawo doznaje ograniczenia.

¹⁷⁵ Zgodnie z art. 27 ust. 2 pkt 9 ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne, jeżeli jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu

Aptekarskiej oraz przedstawienia zaświadczenia z rejestru karnego wydanego w państwie, którego farmaceuta jest obywatelem. Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę na okoliczność, że zakres zaświadczenia o niekaralności w przypadku obywateli polskich ograniczono w przedłożonym projekcie ustawy do przestępstw umyślnych przeciwko życiu i zdrowiu. Negując zgodność z prawem powyższego przepisu, podkreślił, iż taka forma dyskryminacji obywateli państw EOG w dostępie do uzyskania prawa wykonywania zawodu jest niedopuszczalna, choćby ze względu na przepisy Traktatu Ustanawiającego Wspólnotę Europejską zakazujące podejmowania wszelkich działań mających charakter dyskryminacyjny w zakresie zatrudnienia.¹⁷⁶ Organ do spraw ochrony danych osobowych wskazał także na bogate orzecznictwo Trybunału Sprawiedliwości Wspólnot Europejskich w podobnej materii.¹⁷⁷

Generalny Inspektor wskazał również na nieprawidłowości w sformułowaniu jednego z przepisów projektu *ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji oraz o zmianie ustawy Ordynacja podatkowa*.¹⁷⁸ Podkreślił, iż doprecyzowania wymaga dyspozycja – dodanego przez art. 1 pkt 29 ustawy nowelizującej – art. 32a ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.). Przepis ten w pierwotnym brzmieniu upoważniał egzekutora – jeszcze przed przystąpieniem lub już w podczas wykonywania czynności egzekucyjnych – do żądania od każdej osoby okazania dokumentu umożliwiającego ustalenie jej tożsamości. Generalny Inspektor zwrócił uwagę, iż trudno jest wskazać przyczyny, dla których egzekutorom przyznano tak szerokie uprawnienie do ingerencji w sferę prywatności osób fizycznych. Tym bardziej że z treści przepisu nie wynika w sposób jednoznaczny, by obowiązek legitymowania się dotyczył jedynie osób uczestniczących w jakimkolwiek charakterze w prowadzonych (planowanych) czynnościach egzekucyjnych. Organ do spraw ochrony danych osobowych podkreślił wobec tego, iż istnieje konieczność takiego uszczegółowienia projektowanego przepisu, by wprost określał on krąg podmiotów zobowiązanych do okazania egzekutorowi dokumentu umożliwiającego ustalenie ich tożsamości w związku z czynnościami egzekucyjnymi.

ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone.

¹⁷⁶ Art. 12 Traktatu Ustanawiającego Wspólnotę Europejską (Dz. U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.) stanowi, że „(...) w zakresie zastosowania niniejszego Traktatu i bez uszczerbku dla postanowień szczególnych, które on przewiduje, zakazana jest wszelka dyskryminacja ze względu na przynależność państwową (...)", a zgodnie z art. 39 ust. 1 i 2 Traktatu, zapewnia się swobodę przepływu pracowników wewnątrz Wspólnoty. Swoboda ta obejmuje zniesienie wszelkiej dyskryminacji ze względu na przynależność państwową między pracownikami Państw Członkowskich w zakresie zatrudniania, wynagrodzenia i innych warunków pracy.

¹⁷⁷ Np. odnoszący się wprawdzie do innej sytuacji, ale mogący – poprzez analogię – stanowić cenną wskazówkę interpretacyjną wyrok Trybunału Sprawiedliwości Wspólnot Europejskich z dnia 2 sierpnia 1993 r. w sprawie Pilar Allé i Carmel Mary Coonan i inni przeciwko Università degli studi di Venezia i Università degli studi di Parma (sprawa C-259/91, C-331/91 oraz C 332/91), w którym Trybunał orzekł, iż ustawodawstwo Państwa Członkowskiego, ograniczając, w każdym przypadku, czas trwania umów o pracę zawartych z lektorami języka obcego do jednego roku, z możliwością odnowienia, podczas, gdy takie ograniczenie nie istnieje, co do zasady, w odniesieniu do innych nauczycieli, pozostaje w sprzeczności z art. 39 Traktatu.

¹⁷⁸ GI-DOLiS-023/61/07

Powtarzającym się błędem w procesie tworzenia prawa było naruszanie regulacji art. 27 ustawy o ochronie danych osobowych, która dotyczy przetwarzania danych szczególnie chronionych, m.in. poprzez wprowadzanie przepisów dotyczących tej kwestii w aktach prawnych rangi rozporządzenia. Generalny Inspektor podkreślał wówczas, że ustawa o ochronie danych osobowych wprowadza ogólny zakaz przetwarzania danych osobowych o takim charakterze. Katalog danych szczególnie chronionych (określony w ust. 1 tego przepisu) ma charakter zamknięty i obejmuje dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Organ do spraw ochrony danych osobowych wskazywał w takich przypadkach, że zakaz przetwarzania omawianej kategorii danych osobowych zostaje uchylony wyłącznie w sytuacji spełnienia przez administratora jednej z przesłanek określonych w ust. 2 art. 27, tj. m.in. wówczas, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której one dotyczą, i stwarza pełne gwarancje ochrony danych (art. 27 ust. 2 pkt 2 ustawy). Podkreślał przy tym, iż wprowadzanie do rozporządzenia przepisów nakładających na podmioty obowiązek ujawniania danych szczególnie chronionych i przyznających administratorowi danych prawo ich przetwarzania na podstawie aktu prawnego rangi niższej niż ustawa, nie jest rozwiązaniem prawidłowym.¹⁷⁹

W związku z opiniowaniem projektu *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*

¹⁷⁹ Np. projekt rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wymagań dla jednostek organizacyjnych właściwych w zakresie oceny zgodności wyrobów przeznaczonych na potrzeby obronności państwa (GI-DOLiS-023/200-204/07) wprowadzający przepis zobowiązujący osoby zasiadające w gremiach kierowniczych jednostek organizacyjnych ubiegających się o udzielenie akredytacji w zakresie obronności i bezpieczeństwa do składania oświadczeń o toczących się przeciwko nim postępowaniach karnych (§ 3 ust. 3 pkt 7 projektu); uwaga podniesiona przez Generalnego Inspektora nie została uwzględniona, a rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 72 pod poz. 483. Zob. też projekt rozporządzenia Ministra Pracy i Polityki Społecznej w sprawie placówek opiekuńczo – wychowawczych (GI-DOLiS-023/137/07) nakładający na wolontariuszy ubiegających się o zawarcie porozumień z dyrektorami tych placówek obowiązek składania oświadczeń o niekaralności (§ 22 ust. 2 pkt 2); uwaga Generalnego Inspektora nie została uwzględniona, rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 37 pod poz. 331; projekt rozporządzenia Ministra Rozwoju Regionalnego w sprawie ekspertów powoływanych w celu rzetelnej i bezstronnej oceny projektów realizowanych w ramach programów operacyjnych (GI-DOLiS-023/67-70/07) przewidujący uprawnienie do pozyskiwania przez Ministra Rozwoju Regionalnego informacji dotyczących karalności osoby ubiegającej się o wpis na listę ekspertów za przestępstwo popełnione umyślnie; uwagi Generalnego Inspektora przedstawionej do tego projektu nie uwzględniono, rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 93 pod poz. 626; projekt rozporządzenia Ministra Finansów w sprawie szczegółowego zakresu danych gromadzonych w bazach danych tworzonych przez Polską Izbę Ubezpieczeń oraz okresu przechowywania tych danych (GI-DOLiS-023/45/07) przewidujący w § 6 uprawnienie dla Polskiej Izby Ubezpieczeń do przetwarzania w prowadzonych przez ten podmiot bazach danych informacji dotyczących osób, przeciwko którym było prowadzone postępowanie karne w związku z podejrzeniem popełnienia przez nie przestępstwa na szkodę zakładu ubezpieczeń, zakończone prawomocnym wyrokiem skazującym lub warunkowym umorzeniem postępowania;

publicznej na rok 2007 Generalny Inspektor podniósł po raz kolejny (pierwszy raz miało to miejsce w związku opracowywaniem programu badań statystycznych na rok 2004), iż z punktu widzenia ustawy o ochronie danych osobowych wątpliwość budzą wzór formularza sprawozdawczego do badań statystycznych „MZ/n – 1a – karta zgłoszenia nowotworu złośliwego” i wzór formularza sprawozdawczego do badań statystycznych „MZ/Szp – 11B – karta statystyczna psychiatryczna” zawarte w załączniku nr 3 do owego rozporządzenia. Generalny Inspektor zauważył, że w obu wzorach formularzy przewidziano zbieranie szerokiego katalogu danych osobowych pacjentów, w tym o stanie zdrowia podlegających szczególnej ochronie na podstawie art. 27 ust. 1 ustawy. Po raz kolejny podkreślił, że w myśl art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych tego rodzaju bez zgody osoby, której one dotyczą, jest dopuszczalne na podstawie przepisu szczególnego rangi ustawowej stwarzającego pełną gwarancję ich ochrony. W tym przypadku brak jest natomiast stosownej regulacji ustawowej upoważniającej Ministra Zdrowia do prowadzenia zbiorów danych pacjentów cierpiących na choroby nowotworowe i hospitalizowanych z powodu schorzeń psychicznych. Uprawnienie do prowadzenia takich zbiorów nie może zaś wynikać z rozporządzenia, gdyż jest ono aktem prawnym rangi zbyt niskiej w stosunku do „wagi” przetwarzanych danych.¹⁸⁰

Generalny Inspektor przypomniał, iż uwzględniając celowość prowadzenia przez Ministerstwo Zdrowia analizy zachorowalności na choroby nowotworowe i psychiczne oraz ich niezbędność dla prawidłowego wypełniania przez resort jego zadań, dopuścił warunkowo przetwarzanie danych osobowych w zbiorach, o których mowa, z tym zastrzeżeniem, że Ministerstwo Zdrowia podejmie prace legislacyjne, w wyniku których dojdzie do opracowania aktu prawnego rangi ustawy zawierającej unormowania upoważniające Ministra Zdrowia do tworzenia zbiorów danych osobowych pacjentów dla celów statystyki medycznej. Organ do spraw ochrony danych osobowych przypomniał także, iż w razie braku podstawy prawnej do przetwarzania danych osobowych wydać może nakaz usunięcia zebranych danych, na podstawie art. 18 ust. 1 pkt 6 ustawy o ochronie danych osobowych.¹⁸¹

Podobne uwagi Generalnego Inspektora Ochrony Danych Osobowych w kwestii konieczności przetwarzania danych osobowych natury szczególnie chronionej na podstawie przepisów rangi ustawy, pojawiły się również w związku z projektem **rozporządzenia Ministra Pracy i Polityki Społecznej w sprawie zakresu danych gromadzonych w centralnym rejestrze dłużników alimentacyjnych**.¹⁸² Zaznaczyć należy, że organ do spraw ochrony danych osobowych już w czasie prac parlamentarnych oponował przeciwko przekazaniu do regulacji w akcie prawnym rangi rozporządzenia zagadnienia

uwaga zgłoszona przez Generalnego Inspektora nie została uwzględniona, zaś rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 159 pod poz. 1119.

¹⁸⁰ Rozporządzenie opublikowano w Dzienniku Ustaw Nr 210 pod poz. 1525.

¹⁸¹ GI-DP-023/150/06/07

¹⁸² DOLiS-033-34/07

zakresu danych przetwarzanych w centralnym rejestrze dłużników alimentacyjnych. Niestety, mające charakter ekspercki uwagi Generalnego Inspektora Ochrony Danych Osobowych zostały zignorowane przez Parlament. Generalny Inspektor podczas opiniowania projektu rozporządzenia, o którym mowa, wskazał wobec tego, że – zawierający delegację do wydania przedmiotowego rozporządzenia – art. 16 ust. 6 ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. Nr 192, poz. 1778 z późn. zm.) budzi wątpliwości co do zgodności z Konstytucją Rzeczypospolitej Polskiej. Przypomniawszy, że w uzasadnieniu postanowienia z dnia 31 stycznia 2007 r. (S. 1/2007) Trybunał Konstytucyjny stwierdził, iż art. 92 ust. 1 Konstytucji Rzeczypospolitej Polskiej zwiększył rygoryzm wymagań upoważnienia ustawowego i aktu wykonawczego wydanego na jego podstawie. Wprowadził bowiem pojęcie „wytycznych dotyczących treści aktu”. Otóż, zdaniem Trybunału, wytyczne zawarte w ustawie muszą dotyczyć materialnego kształtu regulacji, która ma być zawarta w rozporządzeniu. Z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie „cedować” funkcji prawodawczych na organy władzy wykonawczej. Zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, jak dalej podkreślił Trybunał Konstytucyjny, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej. Tymczasem wbrew ugruntowanemu stanowisku Trybunału Konstytucyjnego, ustawodawca w art. 16 ust. 6 ustawy o pomocy osobom uprawnionym do alimentów (której projekt nie wpłynął do Biura Generalnego Inspektora do zaopiniowania) nie zawarł wytycznych, którymi powinien się kierować minister właściwy do spraw zabezpieczenia społecznego przy ustalaniu w akcie wykonawczym zakresu danych, jakie mają być gromadzone w centralnym rejestrze dłużników alimentacyjnych. Generalny Inspektor wskazał, że wobec faktu, iż powyższa ustawa w żadnym przepisie nie zawiera zamkniętego katalogu danych, których przetwarzanie jest legalne dla realizacji jej celów, zawarte w jej art. 16 ust. 6 stwierdzenie, że określenie w rozporządzeniu zakresu danych ma nastąpić z zachowaniem zasady adekwatności do celu, jakim jest wzmoczenie odpowiedzialności osób zobowiązanych do alimentacji, nie jest zrozumiałą wytyczną dotyczącą treści aktu wykonawczego. Generalny Inspektor podkreślił bowiem, iż na podstawie tak lakonicznie sformułowanego upoważnienia ustawowego, minister właściwy do spraw zabezpieczenia społecznego może w rozporządzeniu nakazać zbieranie w centralnym rejestrze dłużników alimentacyjnych dowolnych danych tych osób.

W tej sytuacji, Generalny Inspektor Ochrony Danych Osobowych stwierdził, że skoro kwestionuje dopuszczalność uregulowania w rozporządzeniu kwestii zakresu danych, jakie mają być gromadzone w centralnym rejestrze dłużników alimentacyjnych, niezasadne jest wyrażanie opinii w sprawie spełnienia przez katalog danych przewidziany w omawianym projekcie rozporządzenia kryterium adekwatności, o którym mowa w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Podkreślił, iż skoro dłużnikiem alimentacyjnym – w rozumieniu art. 2 pkt 3 ustawy o pomocy osobom uprawnionym do alimentów – jest osoba zobowiązana do alimentów na podstawie tytułu wykonawczego, przeciwko której egzekucja stała się bezskuteczna, to sam fakt pozostawania dłużnikiem alimentacyjnym jest informacją o orzeczeniu wydanym w postępowaniu sądowym, czyli daną szczególnie chronioną w myśl art. 27 ust. 1 ustawy o ochronie danych osobowych. Natomiast zgodnie z dyspozycją art. 27 ust. 2 pkt 2 tej ustawy, jej przetwarzanie wymaga istnienia przepisu szczególnego innej ustawy.

W analizowanym okresie sprawozdawczym dość częstym uchybieniem było zamieszczanie w przepisach wykonawczych (rozporządzeniach) zagadnień, które ze względu na treść delegacji ustawowej znaleźć się tam nie powinny. Dotyczyło to zwłaszcza prób wskazywania w przepisach rozporządzeń okresu przetwarzania danych osobowych. Innymi słowy, w upoważnieniu ustawowym nie wskazywano, iż rozporządzenie ma regulować również kwestię okresu przechowywania danych osobowych przetwarzanych na jego podstawie, a tymczasem projektodawcy taki okres ustanawiali. W takich przypadkach Generalny Inspektor wskazywał na treść § 115 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie Zasad techniki prawodawczej (Dz. U. Nr 100, poz. 908), zgodnie z którym, w rozporządzeniu zamieszcza się jedynie przepisy regulujące sprawy przekazane do unormowania w przepisie upoważniającym. Zatem gdy kwestia choćby okresu przetwarzania danych osobowych pominięta została w delegacji ustawowej stanowiącej podstawę do wydania rozporządzenia, zagadnienie to nie może znaleźć się w przepisach aktu wykonawczego.¹⁸³

Do Generalnego Inspektora Ochrony Danych Osobowych w okresie objętym sprawozdaniem wpłynęła również prośba o zaopiniowanie projektu *rozporządzenia Rady Ministrów w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego realizującego zasady ochrony lotnictwa*.¹⁸⁴ Projekt ten w § 17 ust. 3 pkt 2 załącznika nakładał na Straż Graniczną obowiązek oceny, czy osoba ubiegająca się o przepustkę spełnia wymagania niezbędne do otrzymania dostępu do strefy zastrzeżonej lotniska. Po analizie obowiązujących w tej materii przepisów, jak i przepisów projektowanego rozporządzenia organ do spraw ochrony danych osobowych zauważył, że brak jest w ich treści bliższego określenia pojęcia „wymagania niezbędne”. Podkreślił, że ochrona osób fizycznych przed

¹⁸³ Wskazana sytuacja miała miejsce np. w odniesieniu do projektu rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych (GI-DOLiS-023/131/07). § 44 projektowanego rozporządzenia wprowadzał pięćdziesięcioletni okres przechowywania dokumentacji medycznej wytworzonej przez komisje lekarskie Ministerstwa Spraw Wewnętrznych i Administracji, mimo braku upoważnienia ustawowego do jego określania oraz brzmienia art. 18 ust. 4f ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. z 2007 r. Nr 14, poz. 89 z późn. zm.), który w sposób wyczerpujący reguluje zagadnienie okresu przechowywania dokumentacji medycznej; uwagi Generalnego Inspektora zostały uwzględnione, a rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 217 pod poz. 1614; podobnie było z projektem rozporządzenia Ministra Obrony Narodowej w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez Ministra Obrony Narodowej (GI-DOLiS-023/316/07).

¹⁸⁴ GI-DOLiS-023/46/07

arbitralnością decyzji podmiotów publicznych wymaga, by w przedłożonym projekcie w sposób jednoznaczny wskazano wymagania, od których spełnienia uzależnione jest wydanie osobie fizycznej przepustki uprawniającej ją do wykonywania obowiązków w strefie zastrzeżonej lotniska.

Generalny Inspektor wskazał również na konieczność doprecyzowania pojęcia „dane każdego pasażera” oraz „dane osobowe osoby odpowiedzialnej za ochronę lotniska i szkolenie w tym zakresie osób zatrudnionych na lotnisku” oraz katalogu danych osobowych przetwarzanych w związku z nałożonym na Prezesa Urzędu Lotnictwa Cywilnego obowiązkiem prowadzenia listy Operatorów Kontroli Bezpieczeństwa. Uznał to za niezbędne dla uniknięcia wątpliwości interpretacyjnych i przetwarzania danych nieadekwatnych w stosunku do celów, jakim miałyby służyć, a więc wbrew zasadzie wynikającej z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.¹⁸⁵

Generalny Inspektor Ochrony Danych Osobowych uczestniczył również w pracach legislacyjnych nad projektem *ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej*¹⁸⁶ mającej istotne znaczenie w kontekście problematyki ochrony danych osobowych. Ustanawia ona bowiem nowe kompetencje Generalnego Inspektora Ochrony Danych Osobowych. Potrzeba przyjęcia ustawy wynikała z członkostwa Polski w Unii Europejskiej, a zwłaszcza z tzw. dorobku prawnego Schengen, którego urzeczywistnienie w pełnym zakresie było uwarunkowane włączeniem do Systemu Informacyjnego Schengen.

Dnia 14 czerwca 1985 r. – jak czytamy w treści uzasadnienia do projektu ustawy – w Schengen pięć państw: Francja, Niemcy, Belgia, Holandia oraz Luksemburg podpisało umowę o stopniowym znoszeniu kontroli na wspólnych przejściach granicznych (tzw. Schengen I), zwaną dalej „Układem z Schengen”. Przyjęcie układu miało na celu umożliwienie realizacji swobody przemieszczania się osób na terytorium Unii Europejskiej. Dorobek Schengen został bezpośrednio włączony do Traktatu Amsterdamskiego z 1997 r. i stał się integralną częścią prawa wspólnotowego obowiązującego wszystkie państwa członkowskie UE. W celu wprowadzenia swobody przemieszczania się wewnątrz terytorium Unii Europejskiej oraz jednoczesnego wzmocnienia ochrony jej zewnętrznych granic, został utworzony System Informacyjny Schengen (SIS). Rozszerzenie UE w roku 2004 spowodowało konieczność włączenia do Obszaru Schengen dziesięciu nowych Państw Członkowskich. Dotychczasowa infrastruktura techniczna SIS została przewidziana do obsługi maksymalnie 18 państw i nie była przygotowana do objęcia nowych instalacji narodowych. Poza tym

¹⁸⁵ Uwag Generalnego Inspektora nie uwzględniono, a rozporządzenie opublikowano w Dzienniku Ustaw z 2007 r. Nr 116 pod poz. 803.

¹⁸⁶ Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej weszła w życie (z wyjątkiem niektórych przepisów) 24 sierpnia 2007 r., a opublikowano ją w Dzienniku Ustaw Nr 165 pod poz. 1170.

postęp techniczny, który miał miejsce w ciągu ostatniego dziesięciolecia, umożliwia przetwarzanie nie tylko danych tekstowych, ale również innych danych, np. biometrycznych. W związku z tym w celu dostosowania SIS do najnowszych rozwiązań informatycznych i technologicznych oraz umożliwienia przystąpienia do niego nowych Państw Członkowskich UE, zdecydowano o zastąpieniu SIS nowym systemem, dostosowanym do obsługi wszystkich Państw Członkowskich i umożliwiającym przekazywanie większej kategorii danych (np. danych biometrycznych). Chodzi tu o System Informacyjny Schengen drugiej generacji [dalej: SIS II] i uzupełniający go system wymiany informacji wizowej między Państwami Członkowskimi – System Informacji Wizowej (zwany dalej VIS). System VIS ma na celu wymianę danych o wizach między Państwami Członkowskimi, które zniosły kontrole na swoich granicach wewnętrznych i uczestniczą w systemie swobodnego przepływu osób bez kontroli na granicach wewnętrznych.

Artykuł 8 ust. 1 ustawy przewiduje, że Generalny Inspektor sprawuje kontrolę nad tym, czy wykorzystywanie gromadzonych w SIS i VIS danych nie narusza praw osób, których dane te dotyczą. Generalny Inspektor jest uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego (czyli – stosownie do art. 2 pkt 11 ustawy – zespołu współpracujących ze sobą urządzeń, oprogramowania, procedur przetwarzania informacji, narzędzi programowych w celu przetwarzania danych oraz infrastruktury telekomunikacyjnej, umożliwiających organom administracji publicznej i organom wymiaru sprawiedliwości przekazywanie oraz dostęp do danych zgromadzonych w SIS i VIS), w celu sprawowania kontroli (art. 8 ust. 2-3). Natomiast przepisy rozdziału 5 ustawy stanowiące o obowiązkach centralnego organu technicznego KSI (którym jest Komendant Główny Policji), nakładają na ten organ obowiązek wystąpienia przed uruchomieniem KSI do Generalnego Inspektora z wnioskiem o przeprowadzenie kontroli w zakresie spełnienia przez ten system wymogów określonych w art. 36–39 ustawy o ochronie danych osobowych oraz przepisach wydanych na podstawie art. 39a tej ustawy (tryb postępowania przy prowadzeniu kontroli został określony w art. 30–32 ustawy).

Zaznaczyć należy, iż omawiana ustawa wprowadziła istotną zmianę w przepisach ustawy o ochronie danych osobowych. W art. 43 ust. 1 po pkt 2a dodany został pkt 2b, według którego z obowiązku zgłoszenia zbioru danych Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji zwolnieni są administratorzy danych przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej.¹⁸⁷

¹⁸⁷ W związku ze wstąpieniem do strefy Schengen, Generalny Inspektor opiniował również projekty rozporządzeń bezpośrednio związanych z tym zagadnieniem, wydanych na podstawie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, wśród nich zaś: projekt rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie trybu przekazywania Policji osób lub przedmiotów na skutek wglądu do danych SIS, a także związanych z tym obowiązków Policji (rozporządzenie weszło w życie 18 grudnia 2007 r., a

Opiniując związany z powyższą ustawą projekt *rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wiz dla cudzoziemców*¹⁸⁸, Generalny Inspektor zwrócił uwagę na zbędność, przewidzianej w pkt. 44 Załącznika nr 3 „Wniosku o wydanie wizy Schengen”, formuły zgody składającego wniosek na przekazanie dotyczących go danych osobowych do odpowiednich organów w państwach obszaru Schengen i przetwarzanie tych danych w zakresie niezbędnym do wydania wizy. Podkreślił, iż skoro z przepisów art. 12 ust. 1 i art. 15 ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach (Dz. U. z 2006 r. Nr 234, poz. 1694 z późn. zm.), zawierającej delegację do wydania omawianego rozporządzenia, wynika obowiązek cudzoziemca ubiegającego się o wizę podania określonych danych, jego zgoda na przetwarzanie danych w tym zakresie jest zbędna. Swoboda osoby, której dane dotyczą, w kwestii określenia katalogu danych, które decyduje się przekazać organowi uprawnionemu do wydawania wiz, jest w tym przypadku całkowicie wyłączona.¹⁸⁹

Z kolei w związku z pracami nad projektem *ustawy o systemie informacji w ochronie zdrowia*¹⁹⁰ Generalny Inspektor wskazał na kilka przyjętych przez projektodawców rozwiązań, które z punktu widzenia przepisów o ochronie danych osobowych nie mogły zyskać akceptacji. W pierwszej kolejności za niezrozumiałą uznał sformułowaną w projekcie definicję „danych” i podał w wątpliwość celowość jej wprowadzenia. Autorzy projektu uzależnili bowiem uznanie „liter, słów, tekstów, liczb, znaków, symboli, obrazów, kombinacji liter, liczb, symboli i znaków” za „dane” w rozumieniu jego art. 2 pkt 5 od warunku „zebrania ich w zbiory”, nie wskazując, o jakie zbiory w tym przepisie chodzi. Generalny Inspektor zwrócił również uwagę na przyjęte w projekcie znaczenie terminu „gromadzenie danych”. Zawężało ono bowiem czynność gromadzenia danych jedynie do pozyskiwania danych bezpośrednio od podmiotów, których dane dotyczą, lub pozyskiwania danych, dla których określony system informatyczny jest systemem, w którym są one zbierane po raz pierwszy. Przy takim natomiast

opublikowano je w Dzienniku Ustaw Nr 235 pod poz. 1731); w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny (rozporządzenie weszło w życie 19 grudnia 2007 r., a opublikowano je w Dzienniku Ustaw Nr 236 pod poz. 1743); w sprawie wzorów kart wpisu i wzorów kart zapytania o dane w Systemie Informacyjnym Schengen oraz sposobu ich wypełniania (rozporządzenie weszło w życie 23 listopada 2007 r., a opublikowano je w Dzienniku Ustaw Nr 219 pod poz. 1630); w sprawie trybu dostępu do Krajowego Systemu Informatycznego (rozporządzenie weszło w życie 18 grudnia 2007 r., a opublikowano je w Dzienniku Ustaw Nr 235 pod poz. 1730); w sprawie szczegółowego sposobu rejestrowania przypadków, w których uzyskano dostęp do danych lub wykorzystano dane w inny sposób przez Krajowy System Informatyczny. Ostatnie z ww. rozporządzeń weszło w życie 27 listopada 2007 r., a opublikowano je w Dz. U. Nr 221 pod poz. 1643, bez uwzględnienia uwag podnoszonych przez organ do spraw ochrony danych osobowych. Generalny Inspektor protestował przeciwko rozwiązaniu przewidzianemu brak konieczności istnienia we wszystkich organach uprawnionych do dostępu do Krajowego Systemu Informatycznego takich rejestrów wewnętrznych, które pozwalają na jednoznaczną identyfikację pracowników (funkcjonariuszy) tych organów, którzy uzyskali dostęp do danych, a także na ustalenie, jakiego rodzaju czynności były przez te osoby wykonywane w związku z przedmiotowym dostępem. Organ do spraw ochrony danych osobowych podkreślił, iż powyższe jest warunkiem koniecznym dla uznania, że Krajowy System Informatyczny spełnia wymóg rozliczalności określony w § 7 rozporządzenia Ministra Spraw Wewnętrznych 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).

¹⁸⁸ DOLiS-033-63/07

¹⁸⁹ Podniesioną przez Generalnego Inspektora uwagę uwzględniono; rozporządzenie zostało opublikowane w Dzienniku Ustaw z 2007 r. Nr 217 pod poz. 1613.

rozumieniu cytowanego pojęcia pozyskanie danych od podmiotu przetwarzającego je w systemie informatycznym nie byłoby gromadzeniem danych w świetle przedłożonego projektu. Natomiast pozyskanie identycznych danych od podmiotu przetwarzającego je w sposób tradycyjny („papierowy”) za takie „gromadzenie danych” byłoby uznane. Generalny Inspektor podniósł, iż uwzględniając fakt pominięcia przedmiotowej kwestii w uzasadnieniu i jednocześnie istnienie już w obrocie prawnym pojęcia „przetwarzanie danych”¹⁹¹, brak jest przesłanek, by na gruncie projektu ustawy, o którym mowa, formułować odmienne, niż powszechnie przyjęte w polskim porządku prawnym, rozumienie pojęcia „przetwarzania danych”.

Ponadto w związku z podjętą przez projektodawcę próbą wprowadzenia w art. 5 ust. 3 ww. projektu zamkniętego katalogu danych osobowych usługobiorców przetwarzanych w systemie informacji w ochronie zdrowia, Generalny Inspektor podniósł, iż założenie to nie zostało zrealizowane w sposób konsekwentny. Zauważył bowiem, iż w dalszych przepisach opiniowanego projektu przewidziano możliwość przetwarzania danych osobowych usługobiorców w zakresie szerszym niż wskazany w cytowanym przepisie, obejmującym: nadane usługobiorcom identyfikatory (art. 14 ust. 3 pkt 1 projektu), numery identyfikacyjne (art. 16 ust. 3 pkt. 4 i 5) oraz adresy poczty elektronicznej (art. 14 ust. 2 pkt 3), które w pewnych sytuacjach mogą być traktowane jako dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych¹⁹² (np. adresy poczty elektronicznej zawierające w swojej treści imię i nazwisko). W tym stanie rzeczy, przewidziany w art. 5 ust. 3 projektu ustawy katalog danych, jak podkreślił organ do spraw ochrony danych osobowych, powinien zostać tak rozszerzony, by rzeczywiście obejmował wszystkie kategorie danych osobowych usługobiorców przetwarzanych w systemie informacji w ochronie zdrowia.

Analizując dalej ww. projekt, Generalny Inspektor wskazał, iż dla celów zapewnienia ciągłości leczenia lub prowadzonego postępowania diagnostycznego (lecniczego) przyznaje on usługodawcom uprawnienia do dostępu do danych osobowych i jednostkowych danych osobowych zgromadzonych w systemach teleinformatycznych innych usługodawców. Zauważył jednak, iż w projekcie brak jest regulacji zapewniających możliwość kontroli, czy pozyskiwane tą drogą dane osobowe i jednostkowe dane osobowe usługobiorców nie zostaną wykorzystane do innych, niż wyżej wskazane, celów. Opierając się na treści opiniowanego projektu ustawy (art. 14 ust. 2 pkt 3 i art. 35), a także jego

¹⁹⁰ GI-DOLiS-023/320/07

¹⁹¹ Zgodnie z art. 7 pkt 2 ustawy o ochronie danych osobowych, pod pojęciem przetwarzania danych osobowych rozumie się jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

¹⁹² Stosownie do tego przepisu, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

uzasadnienia, podkreślił, że nie sposób jednoznacznie rozstrzygnąć, czy realizacja prawa usługobiorcy (osoby, której dane dotyczą) do uzyskania informacji o udostępnieniu jego danych osobowych (art. 33 ust. 1 pkt 4 ustawy o ochronie danych osobowych) jest możliwa tylko w przypadku, gdy posiada on adres poczty elektronicznej. Generalny Inspektor wskazał, iż w przypadku jednak, gdyby zamiarem projektodawcy było takie ukształtowanie przedmiotowego prawa, zaproponowana regulacja byłaby sprzeczna z dyspozycją art. 33 ustawy o ochronie danych osobowych. Cytowany przepis nakazuje bowiem wykonywanie obowiązku informacyjnego w formie zrozumiałej dla osoby, której dane dotyczą, na jej pisemny wniosek – art. 33 ust. 2 ustawy o ochronie danych osobowych). Natomiast nakładanie na nią dodatkowego obowiązku (posiadania adresu poczty elektronicznej) dla realizacji jej ustawowego uprawnienia, nie znajduje w kontekście tego przepisu uzasadnienia.

Uwzględniając, iż art. 44h ust. 1 pkt 4 ustawy o ewidencji ludności i dowodach osobistych reguluje kwestię udostępniania danych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych państwowym i komunalnym jednostkom organizacyjnym oraz innym podmiotom (w zakresie niezbędnym do realizacji zadań publicznych określonych w odrębnych przepisach) na ich wniosek, Generalny Inspektor uznał również za niezrozumiałą dyspozycję art. 16 ust. 4 pkt 1 projektu ustawy, który – z powołaniem się na wyżej wskazaną regulację – nakłada na organy prowadzące zbiór PESEL obowiązek przekazywania danych do Centralnego Wykazu Usługobiorców. Przepis ten nie precyzował przy tym zakresu danych podlegających przekazaniu. Generalny Inspektor wskazał również, iż w jego ocenie, przekazywanie do tego wykazu danych ze zbioru NIP (art. 16 ust. 4 pkt 3 projektu) w ogóle nie znajduje uzasadnienia.

W toku dalszej analizy projektowanych przepisów Generalny Inspektor zwrócił uwagę na art. 17 ust. 4 nakładający na usługodawców (w rozumieniu art. 2 pkt 20 projektu) obowiązek przekazywania do Centralnego Wykazu Usługodawców (utworzonego na podstawie art. 17 ust. 1 tego projektu) danych o pracownikach medycznych udzielających świadczeń opieki zdrowotnej, w którego treści nie wskazano, jakie dane osób fizycznych będą podlegały przekazaniu. Podkreślił, że mimo iż art. 5 ust. 3 projektu określa zakres danych osobowych, które mogą być przetwarzane w systemie informacji w ochronie zdrowia, to powołany wyżej przepis projektu nie zawiera odesłania do tej regulacji. Zaproponowane brzmienie art. 17 ust. 4 projektu pozostaje zatem – jak skonstatował organ do spraw ochrony danych osobowych – w sprzeczności z dyspozycją art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, który ustanawia zasadę adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane.¹⁹³

¹⁹³ Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych nakłada na administratora danych przetwarzającego dane obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnienia, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

Przedmiotem analizy GIODO były też rządowy projekt ustawy o *zmianie ustawy – Prawo telekomunikacyjne i ustawy o Państwowym Ratownictwie Medycznym* oraz poselski projekt ustawy o *zmianie ustawy – Prawo telekomunikacyjne i ustawy o Państwowym Ratownictwie Medycznym*. Generalny Inspektor podzielił stanowisko o konieczności budowy systemu zapewniającego przekazywanie służbom ustawowo powołanym do niesienia pomocy niezbędnych informacji o abonentach wywołujących połączenia z numerami alarmowymi. Podkreślił jednak, iż nie znajduje uzasadnienia dla tworzenia przy Prezesie Urzędu Komunikacji Elektronicznej [dalej: UKE] centralnej bazy zawierającej dane¹⁹⁴ wszystkich abonentów i zarejestrowanych użytkowników usługi przedpłaconej. Organ do spraw ochrony danych osobowych zaznaczył bowiem, iż z jednej strony, skoro deklarowanym celem utworzenia systemu jest zapewnienie lokalizacji osób dzwoniących na numery alarmowe, trudno wskazać przyczynę, dla której system ten miałby obejmować także dane abonentów, którzy połączeń z numerami alarmowymi nie wywoływali. Z drugiej zaś podkreślił, że wobec faktu, iż centralna baza utworzona przy Prezesie UKE ma zawierać jedynie dane wskazane w art. 169 ust. 1 pkt 1–3 ustawy – Prawo telekomunikacyjne, zapewnienie lokalizacji osoby dzwoniącej na numer alarmowy jest całkowicie uzależnione od dostarczenia do systemu przez operatora publicznej sieci telefonicznej danych lokalizacyjnych wskazanych w znowelizowanym art. 78 ust. 2 ustawy – Prawo telekomunikacyjne (dokładnego adresu zainstalowania, zakończenia sieci – w przypadku stacjonarnej publicznej sieci telefonicznej albo geograficznego położenia urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych – w przypadku ruchomej publicznej sieci telefonicznej). Zdaniem GIODO, w tym stanie rzeczy nie można ustalić, w jaki sposób istnienie przy Prezesie UKE centralnej bazy wszystkich abonentów i zarejestrowanych użytkowników usługi przedpłaconej miałoby się przyczynić do zapewnienia lokalizacji osób dzwoniących na numery alarmowe. Niezależnie od tych uwag Generalny Inspektor podniósł, iż w projektach obu ustaw brak jest wskazania, przez jaki okres w systemie będą przechowywane dane lokalizacyjne abonenta, który wywołał połączenie z numerem alarmowym.¹⁹⁵

Generalny Inspektor Ochrony Danych Osobowych opiniował również w bieżącym okresie sprawozdawczym projekt *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Indii o wzajemnej ochronie informacji niejawnych* oraz projekt *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Kazachstanu o wzajemnej ochronie informacji niejawnych*.¹⁹⁶ Projekty

¹⁹⁴ Zgodnie z Art. 169 ust. 1 pkt. 1–3 ustawy – Prawo telekomunikacyjne, dane osobowe zawarte w publicznie dostępnym spisie abonentów, wydawanym w formie książkowej lub elektronicznej, a także udostępniane za pośrednictwem służb informacyjnych przedsiębiorcy telekomunikacyjnego powinny być ograniczone do: 1) numeru abonenta lub znaku identyfikującego abonenta; 2) nazwiska i imion abonenta; 3) nazwy miejscowości oraz ulicy, przy której znajduje się zakończenie sieci udostępnione abonentowi - w przypadku stacjonarnej publicznej sieci telefonicznej albo miejsca zameldowania abonenta na pobyt stały - w przypadku ruchomej publicznej sieci telefonicznej.

¹⁹⁵ Pismo Generalnego Inspektora z dnia 14 grudnia 2007 r. o sygn. DOLiS-070-3-07 skierowane do Ministerstwa Spraw Wewnętrznych i Administracji oraz Przewodniczącego Komisji Zdrowia w Sejmie Rzeczypospolitej Polskiej.

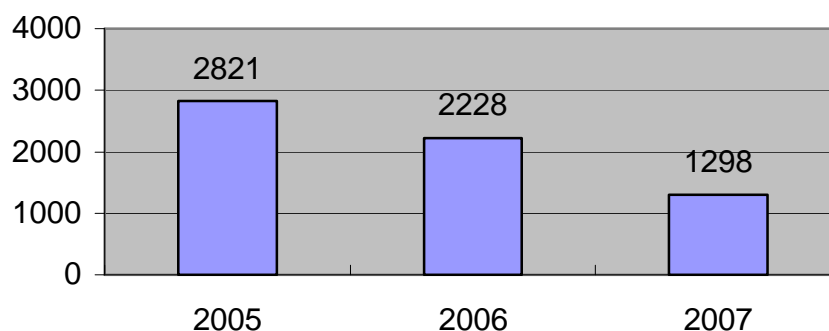
¹⁹⁶ GI-DP-023/213-214/06

powyższych umów po raz pierwszy przesłane zostały do Generalnego Inspektora Ochrony Danych Osobowych w roku 2006. Generalny Inspektor kwestionował wówczas zawarte w ich treści przepisy, które w kwestii ochrony danych osobowych osób przybywających z wizytą do – odpowiednio – Republiki Indii lub Republiki Kazachstanu – w kwestiach związanych z dostępem do informacji niejawnych odsyłały do prawa wewnętrznego Umawiających się Stron w sytuacji, gdy oba te państwa w ogóle nie mają ustawodawstwa dotyczącego ochrony danych osobowych. Generalny Inspektor podkreślił, iż skoro art. 47 ust. 1 ustawy o ochronie danych osobowych dopuszcza przekazywanie tych danych do państwa nienależącego do Europejskiego Obszaru Gospodarczego (tzw. państwa trzeciego – art. 7 pkt 7 tej ustawy) w przypadku, gdy państwo to daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, niezbędnym jest, aby ww. Umowy zawierały w swej treści unormowania zapewniające stosowny stopień ochrony danych osobowych przekazywanych – zgodnie z ich postanowieniami – do Republiki Indii oraz Republiki Kazachstanu.

Projekty Umów, o których mowa wyżej, skierowane do Generalnego Inspektora w bieżącym okresie sprawozdawczym zawierały przepisy poprawione według jego wcześniejszych wskazówek, dlatego zostały przez ten organ wstępnie zaakceptowane. Wskazywały bowiem, iż, cyt.: „(...) Uprawnione podmioty obu Umawiających się Stron zapewniają ochronę danych osobowych osób przybywających z wizytą (...)”.

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 2007 do GODO wpłynęło 1298 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 2005–2007 przedstawia *Wykres 21*.



Wykres 21: Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do Generalnego Inspektora w latach 2005–2007.

W porównaniu z latami ubiegłymi, w okresie objętym sprawozdaniem zmniejszyła się liczba wpływających do organu do spraw ochrony danych osobowych pytań mających formę pisemną (1298 pytań). Należy to uznać za konsekwencję coraz większej popularności uruchomionej przez Generalnego Inspektora Ochrony Danych Osobowych linii telefonicznej, poprzez którą udzielane są porady z zakresu ochrony danych osobowych, oraz znaczącego wzrostu liczby organizowanych przez ten organ seminariów i szkoleń poświęconych tej tematyce. Zagadnienia te będą jednak przedmiotem rozważań w dalszej części Sprawozdania zatytułowanej „Działalność informacyjna”.

Biorąc pod uwagę przedmiot kierowanych do Generalnego Inspektora pytań, należy zauważyć, że utrzymującą się od lat tendencją jest duża liczba wątpliwości z zakresu stosowania innych, niż ustawa o ochronie danych osobowych, aktów prawnych. Tym samym odpowiedź na pytania formułowane przez podmioty przetwarzające dane wymagała uprzedniej analizy szczególnych wobec ustawy o ochronie danych osobowych przepisów prawa regulujących działalność tych podmiotów.

6.1. Interpretacja przepisów

Jak co roku jedną z najliczniejszych grup spraw wpływających do Biura GIODO stanowiły problemy związane z przetwarzaniem danych osobowych przez podmioty **sektora publicznego**.

I tak, na kierowane przez organy gminy pytania w sprawie zgodności z przepisami ustawy o ochronie danych osobowych udostępniania danych adresowych zgromadzonych w prowadzonych przez te organy zbiorach meldunkowych, Generalny Inspektor odpowiadał, że tego rodzaju kwestie należy rozważać przede wszystkim na podstawie przepisów ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.). Generalny Inspektor wskazywał, iż przepisy tej ustawy określają krąg podmiotów, którym udostępnia się oraz którym mogą być udostępnione dane z ewidencji ludności, a także przesłanki, po spełnieniu których udostępnienie w przedmiotowym zakresie staje się możliwe (art. 44h). Podkreślał

również, iż decyzja, czy wnioskodawca należy do kategorii upoważnionych do pozyskania danych osobowych, spoczywa w gestii podmiotu, w posiadaniu którego określony zbiór się znajduje, a zgodnie z art. 44i ust. 1 ustawy o ewidencji ludności i dowodach osobistych, dane ze zbiorów meldunkowych oraz ewidencji wydanych i utraconych dowodów osobistych udostępnia organ gminy.

Generalny Inspektor Ochrony Danych Osobowych konstatował, że jeżeli przepisy ustawy o ewidencji ludności i dowodach osobistych przewidują możliwość udostępnienia określonemu podmiotowi wnioskowanych przez niego danych osobowych, ustawa o ochronie danych osobowych nie stoi na przeszkodzie takiemu działaniu.¹⁹⁷

W wielu pismach nadsyłanych w tym okresie przez organy administracji publicznej pojawiał się problem posiadania przymiotu administratora danych przez organy, którym składane są oświadczenia lustracyjne, w kontekście ewentualnego obowiązku zgłoszenia przez nie powstałego w ten sposób zbioru danych Generalnemu Inspektorowi do rejestracji, zgodnie z obowiązkiem wynikającym z art. 40 ustawy o ochronie danych osobowych.¹⁹⁸ Generalny Inspektor stwierdził, że organy, którym składane są oświadczenia, przekazują je niezwłocznie do Biura Lustracyjnego Instytutu Pamięci Narodowej, nie mając jednocześnie na tym etapie prawa do zapoznawania się z ich treścią. Należy więc przyjąć, że podmioty te nie posiadają w takim przypadku statusu administratorów danych i tym samym po ich stronie nie powstaje obowiązek rejestracyjny wynikający z przepisów ustawy o ochronie danych osobowych.¹⁹⁹

Wątpliwości pytających (najczęściej organów wykonawczych jednostek samorządu terytorialnego) budziła też kwestia jawności danych zawartych w składanych przez zobowiązane do tego osoby oświadczeniach majątkowych, w tym możliwości publikowania informacji o adresie zamieszkania osoby składającej oświadczenie w Biuletynie Informacji Publicznej. Generalny Inspektor zwracał wówczas uwagę na przepisy ustaw samorządowych²⁰⁰, według których informacje zawarte w oświadczeniach majątkowych są jawne, z wyłączeniem informacji o adresie zamieszkania składającego oświadczenie oraz o miejscu położenia nieruchomości. W takim oto „jawnym” zakresie, udostępniane są one w Biuletynie Informacji Publicznej prowadzonym na podstawie przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.).

¹⁹⁷ Np. GI-DOLiS-024/17/07, GI-DOLiS-024/453/07, GI-DOLiS-024/546/07

¹⁹⁸ GI-DOLiS-024/436/07

¹⁹⁹ O obowiązku natychmiastowego przekazywania oświadczeń lustracyjnych stanowi art. 7 ust. 5 ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990 oraz treści tych dokumentów (Dz. U. z 2007 r. Nr 63, poz. 425 z późn. zm.).

²⁰⁰ Odpowiednio: art. 24i ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.); art. 25d ust. 1 i 3 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.); art. 27d ust. 1 i 3 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r. Nr 142, poz. 1590 z późn. zm.).

W tym miejscu zauważyć należy, że zarówno przepisy ustaw samorządowych, jak i powołanego wyżej aktu prawnego, nie regulują wprost kwestii okresu, w ciągu którego oświadczenia majątkowe powinny znajdować się na stronach internetowych Biuletynu Informacji Publicznej właściwych podmiotów oraz sposobu postępowania z oświadczeniem w przypadku zaprzestania sprawowania określonej funkcji przez osobę je składającą. Powyższy problem był przedmiotem analizy Generalnego Inspektora Ochrony Danych Osobowych w następstwie pytania, jakie do niego wpłynęło.²⁰¹ Organ powołany do spraw ochrony danych osobowych zaznaczył, że wobec braku literalnego uregulowania omawianego zagadnienia w szczególnych, wobec ustawy o ochronie danych osobowych aktach prawnych regulujących wprost kwestie publikacji oświadczeń majątkowych, problem ten należy rozstrzygnąć na podstawie wykładni celowościowej tych przepisów z uwzględnieniem zasad przetwarzania danych osobowych zawartych w ustawie o ochronie danych osobowych.²⁰² Zwrócił uwagę na fakt, że ze sprawowaniem funkcji publicznej łączy się pewna transparentność życia prywatnego osoby pełniącej taką funkcję, która obejmuje także sferę jej życia zawodowego i gospodarczego, co bezpośrednio wiąże się z posiadanym przez nią majątkiem. Z tego właśnie powodu przepisy ustaw samorządowych wprowadziły obowiązek publikowania w Biuletynie Informacji Publicznej oświadczeń majątkowych pewnych kategorii osób. Wprowadzenie tego obowiązku miało na celu wdrożenie realnej i szerokiej kontroli społecznej działań osób pełniących określone funkcje publiczne i zahamowanie wciąż obecnego w życiu publicznym i szkodliwego dla rozwoju społeczeństwa obywatelskiego zjawiska korupcji. Generalny Inspektor podkreślał, że aby możliwa była skuteczna realizacja tej kontroli, obywatele powinni mieć możliwość łatwego dostępu do danych zawartych w oświadczeniach w celu przeanalizowania, jak w czasie sprawowania funkcji publicznej zmieniał się status majątkowy osoby ją pełniącej oraz porównania jej obecnej sytuacji majątkowej z poprzednią. Żeby możliwa była realizacja tego założenia, powszechny dostęp do oświadczenia nie powinien, zdaniem Generalnego Inspektora, kończyć się z chwilą zaprzestania sprawowania funkcji publicznej przez osobę je składającą.

Generalny Inspektor konstatawał, że skoro przepisy ustaw samorządowych stanowią o 6-letnim okresie przechowywania oświadczeń majątkowych²⁰³, to powyższe w zestawieniu z wprowadzonym obowiązkiem udostępnienia jawnych informacji zawartych w oświadczeniach majątkowych w BIP przemawia za możliwością upubliczniania tych danych przez cały ten okres (płynący od momentu złożenia oświadczenia). Udostępnienie oświadczeń na stronie Biuletynu przez wskazany czas uznać należy za niezbędne dla osiągnięcia celu przetwarzania zawartych w nich danych

²⁰¹ GI-DOLiS-024/407/07

²⁰² Zgodnie z art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych, administrator danych jest obowiązany zapewnić, aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

osobowych, którym jest zapewnienie łatwego i długotrwałego dostępu do informacji o sytuacji majątkowej osoby pełniącej funkcję publiczną szerokiemu kręgowi obywateli.

W związku z przeprowadzonymi w roku sprawozdawczym wyborami parlamentarnymi Generalny Inspektor wypowiedział się również w kwestii legalności zamieszczenia na oficjalnej stronie internetowej jednego z miast danych osobowych członków obwodowej komisji wyborczej. Zwrócił uwagę, że zgodnie z art. 48 ust. 8 ustawy z dnia 12 kwietnia 2001 r. Ordynacja wyborcza do Sejmu Rzeczypospolitej Polskiej i Senatu Rzeczypospolitej Polskiej (Dz. U. Nr 46, poz. 499 z późn. zm.), obwodowa komisja wyborcza na pierwszym posiedzeniu wybiera ze swego grona przewodniczącego i jego zastępcę, zaś skład komisji podaje się do wiadomości publicznej w sposób zwyczajowo przyjęty. Generalny Inspektor podkreślił, iż ze względu na fakt istnienia szczególnej regulacji prawnej dotyczącej przetwarzania danych w związku z wyborami parlamentarnymi, to im trzeba przyznać prymat stosowania w przypadkach tego rodzaju (art. 23 ust. 1 pkt 2 oraz art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych).²⁰⁴

W 2007 r. Generalny Inspektor zajął się też analizą przepisów ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. Nr 157, poz. 1119 z późn. zm.). Zgodnie bowiem z jej art. 66, od 31 grudnia 2007 r. znosi się Komisję Nadzoru Finansowego i likwiduje się Generalny Inspektorat Nadzoru Bankowego. W związku z tym do Biura Generalnego Inspektora Ochrony Danych Osobowych zwrócił się Urząd Komisji Nadzoru Finansowego [dalej: UKNF] z prośbą o opinię, czy „przejęcie” przez ten Urząd pracowników Generalnego Inspektoratu Nadzoru Bankowego [dalej: GINB] możliwe jest na podstawie umowy powierzenia przetwarzania danych osobowych, o której stanowi art. 31 ustawy o ochronie danych osobowych. W piśmie wskazano, iż celem umowy powierzenia byłoby, cyt.: „(...) przygotowanie systemów informatycznych (definicje użytkowników, nadanie haseł, nadanie uprawnień, przeniesienie plików) oraz poczty elektronicznej (nowe adresy e – mail, migracja skrzynek pocztowych) do przejęcia obsługi z dniem 1 stycznia 2008 r. (...)”.²⁰⁵

Generalny Inspektor, analizując zagadnienie, wskazał, iż istotnie, w świetle art. 31 ust. 1 ustawy o ochronie danych osobowych, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych. Podmiot, któremu powierzono przetwarzanie takich danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie (ust. 2). Ponadto jest on obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39 ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w jej art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych (ust. 3). W przypadku powierzenia przetwarzania danych

²⁰³ Odpowiednio: art. 24h ust. 6 zd. 3 ustawy o samorządzie gminnym; art. 25c ust. 6 zd. 3 ustawy o samorządzie powiatowym; art. 27c ust. 6 zd. 3 ustawy o samorządzie województwa.

²⁰⁴ DOLiS-035-40/07

odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodne z tą umową (ust. 4). Generalny Inspektor podkreślił przy tym, iż cytowana regulacja może mieć zastosowanie jedynie wówczas, gdy administrator danych chce przekazać innemu podmiotowi wykonywanie pewnych czynności na danych osobowych w jego imieniu i dla realizacji jego celów. Intencją ustawodawcy było, aby ten, komu powierzono przetwarzanie danych osobowych (zlecniodawca) nie był traktowany jako administrator danych.²⁰⁶ Podmiot ten, jak dalej zaznaczył organ do spraw ochrony danych osobowych, nie może zatem samodzielnie decydować o celach i środkach procesu przetwarzania danych, a działania na danych prowadzone przez taki podmiot nie powinny mieć charakteru samoistnego, oderwanego od zadań administratora danych. Tym samym wątpliwości budziła możliwość skorzystania w zasygnalizowanej sprawie przez Generalny Inspektorat Nadzoru Bankowego i Urząd Komisji Nadzoru Bankowego z konstrukcji powierzenia przetwarzania danych osobowych pracowników pierwszego podmiotu. Generalny Inspektor zwrócił bowiem uwagę, iż z treści nadesłanej korespondencji wynika, że po przekazaniu omawianych danych UKNF będzie je przetwarzać dla realizacji własnych celów, związanych z przyszłym zatrudnieniem pracowników GINB w tym Urzędzie. Tym samym UKNF, chcąc przetwarzać takie dane, powinien legitymować się jedną z przesłanek legalności ich przetwarzania wymienionych w art. 23 ust. 1 pkt. 1–5 ustawy o ochronie danych osobowych.²⁰⁷

W omawianym okresie sprawozdawczym, Generalny Inspektor Ochrony Danych Osobowych z własnej inicjatywy wielokrotnie występował także do różnych podmiotów ze sfery publicznej, sygnalizując swoje wątpliwości co do zgodności przyjętej przez nie praktyki z przepisami regulującymi kwestie ochrony danych osobowych.

I tak, w wystąpieniu do Komendanta Głównego Policji, do którego impulsem stały się podawane w środkach masowego przekazu informacje o podjęciu przez Policję czynności operacyjnych wobec członków organizacji ekologicznych w związku z protestami dotyczącymi budowy obwodnicy w dolinie Rospudy, Generalny Inspektor podniósł, iż organy władzy publicznej zobowiązane są – zgodnie z Konstytucją Rzeczypospolitej Polskiej – do działania na podstawie i w granicach prawa (art. 7) i że mogą pozyskiwać jedynie informacje niezbędne w demokratycznym

²⁰⁵ DOLiS-035-83/07

²⁰⁶ Por. J. Barta, R. Markiewicz, P. Fajgielski, *Ochrona Danych Osobowych. Komentarz*, Wolters Kluwer Polska – LEX, Kraków 2007, s. 560.

²⁰⁷ Zgodnie z treścią tego przepisu, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

państwie prawnym (art. 51 ust. 2 Konstytucji RP). Generalny Inspektor wskazał, iż dopuszczalność pozyskiwania przez Policję informacji zawierających dane osobowe jest uzależniona od spełnienia jednej z przesłanek określonych w ustawie o ochronie danych osobowych, które zróżnicowane zostały w zależności od kategorii danych, jakie mają podlegać przetwarzaniu (w tym zbieraniu), a ich katalog został zawarty w art. 23 ust. 1 oraz art. 27 ust. 2 ustawy o ochronie danych osobowych. Generalny Inspektor zwrócił się do Komendanta Głównego Policji o wskazanie podstawy prawnej niniejszych działań.²⁰⁸ W odpowiedzi na powyższe Komendant Główny Policji wskazał, iż „(...) informacje dotyczące (...) podjęcia przez Policję czynności operacyjnych wobec członków organizacji ekologicznych w związku z protestami dotyczącymi budowy obwodnicy w dolinie Rospudy (...) nie mają uzasadnienia, ponieważ Policja nie prowadzi działań wobec członków organizacji ekologicznych, tylko określone czynności w celu realizacji zadań ustawowych (...)”. Podmiot ten wskazał, iż działania podejmowane przez Policję w związku z realizacją inwestycji drogowej w dolinie Rospudy nie były nakierowane na zbieranie informacji o protestujących ekologach, tylko na pozyskiwanie informacji o ewentualnych zagrożeniach porządku publicznego, albowiem jednym z podstawowych zadań Policji nałożonym na tę formację przepisami ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2002 r. Nr 7, poz. 58 z późn. zm.) jest ochrona bezpieczeństwa i porządku publicznego (art. 1 ust. 2 pkt 2 tej ustawy). Działania te – jak wyjaśnił Komendant Główny Policji – polegały na skorzystaniu ze wsparcia osób postronnych, które mogły posiadać informacje pomocne z punktu widzenia konieczności zapewnienia przez funkcjonariuszy Policji bezpieczeństwa publicznego. Możliwość taką przewiduje art. 22 ustawy o Policji, w myśl którego, Policja przy wykonywaniu swych zadań, może korzystać z pomocy osób niebędących policjantami.²⁰⁹

W 2007 r. miało również miejsce – nagłośnione w środkach masowego przekazu – podjęcie przez Centralne Biuro Antykorupcyjne czynności polegających na zabezpieczeniu dokumentacji medycznej szpitala MSWiA w Warszawie. W związku z wątpliwościami, co do legalności powyższego działania, zwłaszcza wobec obowiązku podejmowania przez organy władzy publicznej jedynie takich działań, które mieszczą się w granicach prawa, oraz możliwości pozyskiwania przez te organy wyłącznie takich informacji, które są niezbędne w demokratycznym państwie prawnym (powołane powyżej art. 7 i art. 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej), Generalny Inspektor, na podstawie art. 14 pkt 2 ustawy o ochronie danych osobowych, zwrócił się do Szefa Centralnego Biura Antykorupcyjnego z prośbą o wskazanie podstawy prawnej dla tych działań.²¹⁰ W tej sytuacji Generalny Inspektor podjąć mógł właściwie jedynie takie działania, albowiem wiele jego kompetencji wobec zbiorów danych przetwarzanych m.in. przez CBA – mocą art. 43 ust. 2 ustawy o ochronie

²⁰⁸ Wystąpienie Generalnego Inspektora z dnia 23 lutego 2007 r. o sygn. GI-DOLiS-024/232/07

²⁰⁹ Pismo Komendanta Głównego Policji z dnia 29 marca 2007 r. o sygn. Gp-2155/1504/07/JJ

²¹⁰ Wystąpienie Generalnego Inspektora z dnia 20 lipca 2007 r. o sygn. GI-DOLiS-024/631/07

danych osobowych – zostało wyłączonych. Zgodnie z tym przepisem, w odniesieniu do zbiorów, o których mowa w jego ust. 1 pkt. 1 i 3 (m.in. objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwowe, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego) oraz zbiorów, o których mowa w ust. 1 pkt 1a (które zostały uzyskane w toku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności), Generalnemu Inspektorowi nie przysługują uprawnienia określone w art. 12 pkt 2 ustawy o ochronie danych osobowych (wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych), art. 14 pkt. 1 i 3-5 (prawo wstępu do pomieszczeń, gdzie przetwarzane są dane osobowe i przeprowadzania niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą; wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii; przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych; zlecenia sporządzania ekspertyz i opinii) oraz w art. 15–18 (dotyczące uprawnień w związku z przeprowadzaniem przez inspektora kontroli przetwarzania danych pod względem zgodności z obowiązującymi przepisami o ich ochronie).

W odpowiedzi na wystąpienie GODO szef CBA²¹¹ wskazał na podstawę prawną swego działania - art. 217 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.) i postanowienie Prokuratora Prokuratury Okręgowej w Warszawie z dnia 11 lutego 2007 r. dotyczące żądania wydania rzeczy w związku z nadzorowanym przez ww. Prokuraturę śledztwie w sprawie nieprawidłowości w Centralnym Szpitalu Klinicznym MSWiA w Warszawie i na art. 22 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 z późn. zm.).²¹²

²¹¹ Pismo Szefa Centralnego Biura Antykorupcyjnego z dnia 18 czerwca 2007 r. o sygn. ZOŚ-11-795/07

²¹² Zgodnie z ust. 1 tego przepisu, w zakresie swojej właściwości CBA może uzyskiwać informacje, w tym także niejawnie, gromadzić je, sprawdzać i przetwarzać. CBA w celu zapobieżenia lub wykrycia przestępstw, określonych w art. 2 ust. 1 pkt 1 ustawy, oraz identyfikacji osób może przetwarzać informacje, w tym również dane osobowe ze zbiorów prowadzonych na podstawie odrębnych przepisów przez organy władzy publicznej i państwowe jednostki organizacyjne, a w szczególności z Ewidencji Działalności Gospodarczej, Krajowej Ewidencji Podatników, Krajowego Rejestru Karnego, Krajowego Rejestru Sądowego, Powszechnego Elektronicznego Systemu Ewidencji Ludności, Rejestru Podmiotów Gospodarki Narodowej, Centralnego Rejestru Ubezpieczonych i Centralnego Rejestru Płatników Składek, Centralnej Ewidencji Pojazdów i Kierowców, Krajowego Centrum Informacji Kryminalnych. Administratorzy danych gromadzonych w tych rejestrach są obowiązani do nieodpłatnego ich udostępniania (ust. 2). Dane ze zbiorów, o których mowa w ust. 2 – stosownie do art. 22 ust. 3 ustawy o Centralnym Biurze Antykorupcyjnym – przekazuje się w szczególności na nośniku optycznym, magnetycznym lub w drodze teletransmisji. Ponadto w zakresie swojej właściwości CBA może zbierać także wszelkie niezbędne dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 27 ust. 1 ustawy o ochronie danych osobowych, a także korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je, w rozumieniu ustawy o ochronie danych osobowych, bez wiedzy i zgody osoby, której te dane dotyczą (ust. 4). Ust. 5 stanowi natomiast, że administrator zbioru danych jest obowiązany udostępnić określone w upoważnieniu dane osobowe, o których mowa w ust. 4, na podstawie imiennego upoważnienia wydanego przez Szefa CBA okazanego przez funkcjonariusza wraz z legitymacją służbową. Dane osobowe zebrane w celu wykrycia przestępstwa przechowuje się przez okres, w którym są one niezbędne dla realizacji ustawowych zadań wykonywanych przez CBA. Funkcjonariusze CBA dokonują weryfikacji tych danych nie rzadziej niż co 10 lat od dnia uzyskania informacji, usuwając

Koleją sprawą zasygnalizowaną w środkach masowego przekazu, czego konsekwencją stało się wystąpienie Generalnego Inspektora Ochrony Danych Osobowych do Ministra Finansów, była kwestia dotycząca prawidłowego wywiązywania się przez naczelników urzędów skarbowych z nałożonego na administratorów danych mocą art. 37 ustawy o ochronie danych osobowych obowiązku zapewnienia, aby do przetwarzania danych zostały dopuszczone jedynie takie osoby, które legitymują się stosownym upoważnieniem. W związku z zatrudnianiem w tych urzędach praktykantów i stażystów powstały wątpliwości, czy osobom tym nadawane są upoważnienia do przetwarzania danych osobowych. Intencją Generalnego Inspektora Ochrony Danych Osobowych było podkreślenie, że na konieczność legitymowania się upoważnieniem określonym w art. 37 ustawy nie ma wpływu rodzaj umowy łączącej pracodawcę z osobą świadczącą daną pracę.²¹³ W odpowiedzi wskazano, że naczelnicy urzędów skarbowych, mając na uwadze konieczność ochrony danych osobowych podatników, przestrzegają zasad ochrony danych osobowych niezależnie od tego, czy czynności na rzecz urzędu wykonuje jego pracownik, czy też osoba odbywająca staż, praktykę zawodową lub studencką.²¹⁴

Generalny Inspektor Ochrony Danych Osobowych nie mógł również nie zareagować na pojawiające się w materiałach prasowych informacje dotyczące zamiaru instalowania na terenie szkół i placówek oświatowych urządzeń umożliwiających rejestrowanie rozmów. W wystąpieniu do Ministra Edukacji Narodowej kategorycznie sprzeciwił się tego rodzaju próbom ograniczania prywatności osób przebywających na terenie szkół i placówek oświatowych, gdyż w obowiązującym prawie nie ma wystarczających podstaw do takiego działania. Podkreślił, iż jedynym powszechnie obowiązującym aktem prawnym regulującym tę kwestię jest rozporządzenie Rady Ministrów z dnia 6 września 2007 r. w sprawie form i zakresu finansowego wspierania organów prowadzących w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w publicznych szkołach i placówkach (Dz. U. Nr 163, poz. 1155), które ma rangę niższą niż ustawa, a zatem w świetle dyspozycji art. 31 ust. 3 Konstytucji RP nie może skutecznie wprowadzić ograniczeń w zakresie korzystania z konstytucyjnych wolności i praw człowieka i obywatela. Przepis ten stanowi bowiem, że 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,

dane zbędne (ust. 6). Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową oraz dane o stanie zdrowia, nałogach lub życiu seksualnym osób podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, które nie zostały skazane za te przestępstwa, podlegają komisijnemu i protokolarnemu zniszczeniu niezwłocznie po uprawnieniu się stosownego orzeczenia (ust. 7).

²¹³ Wystąpienie Generalnego Inspektora z dnia 14 sierpnia 2007 r. o sygn. GI-DOLiS-024/897/07

²¹⁴ Pismo Podsekretarza Stanu w Ministerstwie Finansów z dnia 19 września 2007 r. o sygn. AP9-066-35/SA/MB7-11240/2007

bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.²¹⁵

W okresie objętym sprawozdaniem Generalny Inspektor zajmował się również sprawą odnalezienia na terenie należącym niegdyś do upadłej Huty Szkła „J.” niezabezpieczonej dokumentacji pracowniczej byłych pracowników tej huty. Media doniosły bowiem, iż pracownicy ci odnaleźli dotyczące ich dokumenty, m.in. listy płac, premii, a nawet wyroki sądowe (alimentacyjne), cyt.: „(...) na trawniku koło dawnego biurowca (...)”. Generalny Inspektor w wystąpieniu kierowanym w tej sprawie do Ministra Sprawiedliwości podniósł, iż pozostawienie dokumentacji zawierającej dane osobowe byłych pracowników huty w niezabezpieczonej postaci, w miejscu ogólnodostępnym, świadczy o niedopełnieniu – choćby w minimalnym stopniu – wymogów ochrony danych przewidzianych w ustawie o ochronie danych osobowych. Wskazał, że z określonym w art. 36 ustawy obowiązkiem stosownego zabezpieczenia danych osobowych koresponduje art. 52 tego aktu prawnego, zgodnie z którym ten, kto administrując danymi, narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności. Jednocześnie zaznaczył, iż okoliczności tej sprawy uzasadniają rozpatrzenie jej również w kontekście możliwego zaistnienia przestępstwa stypizowanego w art. 51 ust. 1 ustawy, w myśl którego, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2; jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 51 ust. 2 ustawy).

Ustalenie osób odpowiedzialnych za przetwarzanie danych osobowych utrwalaonych w ww. dokumentacji i dokonanie oceny stopnia ich zawinienia, wymagało podjęcia odpowiednich czynności wyjaśniających przez organy ścigania i wymiaru sprawiedliwości. Wobec powyższego Generalny Inspektor zwrócił się w wystąpieniu do Ministra Sprawiedliwości z prośbą o spowodowanie przeprowadzenia przez podległych mu prokuratorów czynności wyjaśniających w tej sprawie, wobec podejrzenia popełnienia przestępstw przez osoby odpowiedzialne za przetwarzanie przedmiotowych danych.²¹⁶

W analizowanym okresie sprawozdawczym z publikacji prasowych wynikało również, że Zarząd Transportu Miejskiego w W. zamierza wprowadzić nowe karty miejskie uprawniające do określonego rodzaju przejazdów. Na kartach tych miałyby być zamieszczana – poza innymi – także informacja o numerze PESEL poszczególnych podróżnych. Doniesienia te spowodowały wystąpienie organu do

²¹⁵ Wystąpienie Generalnego Inspektora z dnia 31 października 2007 r. o sygn. GI-DOLiS-035-93/07

²¹⁶ Wystąpienie Generalnego Inspektora z dnia 27 sierpnia 2007 r. o sygn. GI-DOLiS-430/487/07

spraw ochrony danych osobowych do Przewodniczącego Komisji Infrastruktury i Inwestycji Rady m.st. Warszawy, w którym GODO zwrócił uwagę, iż nawet w sytuacji, gdy podstawę do przetwarzania danych osobowych stanowią przepisy prawa (np. uchwała), administrator danych – dla uznania procesu przetwarzania przez niego danych osobowych za legalny – musi uczynić zadość wielu innym obowiązkom nałożonym na niego przepisami o ochronie danych osobowych. I tak art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, jak wskazał Generalny Inspektor w swym wystąpieniu, ustanawia zasadę adekwatności (relewantności) danych w stosunku do celów ich przetwarzania, co oznacza, że dane osobowe swym rodzajem i treścią nie powinny wykraczać poza potrzeby wynikające z celu, jakemu służy ich przetwarzanie (w tym ujawnianie). Konieczność zachowywania równowagi między uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych – na co również Generalny Inspektor zwrócił uwagę w treści wystąpienia – podniósł w jednym ze swych wyroków Wojewódzki Sąd Administracyjny.²¹⁷ Generalny Inspektor zasygnalizował, że zamieszczanie na karcie miejskiej tak szczegółowej informacji o osobie, jak jej numer PESEL, trudno uznać za niezbędne do realizacji umowy przewozu.²¹⁸

Ten przypadek oraz coraz częstsze próby organów stanowiących jednostek samorządu terytorialnego zmierzające do określenia w aktach prawa miejscowego (uchwałach) zakresu danych osobowych przetwarzanych w związku z przewozem osób w ramach transportu miejskiego z pominięciem zasady adekwatności danych w stosunku do celów ich przetwarzania spowodowały, że Generalny Inspektor wystąpił również do Marszałka Sejmu. W przesłanym do niego piśmie wskazał na niezgodność tego typu praktyk z literą prawa.²¹⁹ Wyraził przy tym zaniepokojenie praktyką pozyskiwania coraz szerszego zakresu danych od osób, których one dotyczą, przez różnorakie podmioty pod pretekstem „uniwersalności” wydawanych przez nie dokumentów. Tytułem przykładu wskazał, iż nowo powstające bilety elektroniczne mają służyć – według doniesień prasowych – m.in. jako karnety na basen, siłownię czy karty biblioteczne. Podobne – bo uniwersalne – funkcje przypisuje się elektronicznym legitymacjom studenckim. W założeniu miały być one jedynie dokumentem poświadczającym status studenta, który mógł być używany jako karta dostępu do biblioteki oraz karta dostępu do urządzeń technicznych i laboratoriów, a tymczasem w przyszłości spełniać mają również funkcję tzw. elektronicznych portmonetek. Studenci za ich pomocą mają mieć także możliwość zapłaty za obiad w stołówce czy uiszczenia opłaty w kawiarence internetowej. Generalny Inspektor podniósł, iż w każdym przypadku planowania przedsięwzięcia, z którym wiąże się przetwarzanie, w tym

²¹⁷ W wyroku z dnia 1 grudnia 2005 r. (sygn. akt II SA/Wa 917/2005) WSA w Warszawie stwierdził, iż adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator danych zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełniania celu, w jakim dane są przetwarzane.

²¹⁸ Wystąpienie Generalnego Inspektora z dnia 31 października 2007 r. o sygn. DOLiS-035-94/07

²¹⁹ Wystąpienie Generalnego Inspektora z dnia 23 listopada 2007 r. o sygn. DOLiS-035-149/07

ujawnianie, danych osobowych, należy mieć na względzie nie tylko konieczność unormowania tej okoliczności w odpowiednim akcie prawnym, ale i wynikającą z przepisów ustawy o ochronie danych osobowych zasadę adekwatności danych w stosunku do celów ich przetwarzania. Brak jej uwzględnienia w działalności administratora danych może wpłynąć w sposób negatywny na jakość ochrony przetwarzanych przez ten podmiot danych osobowych.

Naruszenie przepisów o ochronie danych osobowych Generalny Inspektor zasygnalizował także Prezesowi Krajowej Rady Komorniczej. Impulsem do wystąpienia do tego podmiotu stała się stosowana w kancelariach komorniczych praktyka polegająca na wysyłaniu do pracodawców informacji o zajęciu wynagrodzenia za pracę dłużnika bez wstępnego sprawdzenia, czy dana osoba jest rzeczywiście zatrudniona u pracodawcy, do którego zajęcie zostało skierowane. Generalny Inspektor w swym wystąpieniu podkreślił, że praktyka taka prowadzi, w przypadku doręczenia zajęcia osobie, która w rzeczywistości dłużnika nigdy nie zatrudniała, do ujawnienia osobie nieuprawnionej danych osobowych dłużnika, w tym danych szczególnie chronionych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych. Podkreślił, iż art. 51 ustawy o ochronie danych osobowych przesądza o odpowiedzialności karnej wobec osoby administrującej zbiorem danych lub będącej obowiązana do ochrony danych osobowych za udostępnienie lub umożliwienie dostępu do zgromadzonych przez nią danych osobom nieupoważnionym zarówno w przypadku zachowania umyślnego, jak i działania o charakterze nieumyślnym.²²⁰

Prezes Krajowej Rady Komorniczej nie uznał argumentów Generalnego Inspektora. Stwierdził, iż komornik sądowy jest zobowiązany prowadzić egzekucję według sposobu zgłoszonego przez wierzyciela; nie ma przy tym ani prawa, ani możliwości weryfikowania wniosku wierzyciela pod kątem zatrudnienia dłużnika u danego pracodawcy. Stwierdził również, iż ustalenie faktu zatrudnienia określonej osoby wymaga ujawnienia pracodawcy jej imienia i nazwiska. Czynności podejmowane w tym zakresie przez komorników są zgodne – w jego opinii – z obowiązującymi w tym zakresie przepisami prawa, tj. ustawą z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego oraz ustawą z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (Dz. U. z 2006 r. Nr 167, poz. 1191 z późn. zm.).²²¹ Generalny Inspektor nie podzielił opinii Prezesa Krajowej Rady Komorniczej i podtrzymał swoje stanowisko, iż sygnalizowane działanie komorników stanowi naruszenie ciążącego na nich, jako na administratorach danych, obowiązku ich zabezpieczenia, o którym mowa w art. 36 ustawy o ochronie danych osobowych. Generalny Inspektor poinformował przy tym, iż ze względu na fakt, że za naruszenie tego obowiązku przewidziano w ustawie o ochronie danych osobowych odpowiedzialność karną, w

²²⁰ Wystąpienia Generalnego Inspektora z dnia 27 sierpnia 2007 r. i 6 listopada 2007 r. o sygn. GI-DOLiS-024/666/07

²²¹ Pismo Prezesa Krajowej Rady Komorniczej z dnia 6 września 2007 r. i 16 listopada 2007 r. o sygn. KRK/III/970/07

przypadku uzyskania informacji o kolejnych przypadkach stosowania przez komorników opisanej praktyki będzie on uprawniony do rozważenia skierowania do właściwego organu ścigania zawiadomienia o popełnieniu przestępstwa.²²²

Podkreślenia w tym miejscu wymaga, iż Generalny Inspektor Ochrony Danych Osobowych został ustawowo powołany nie tylko do podejmowania władczych działań w sprawach niezgodnego z prawem udostępniania danych osobowych, ale także do czuwania nad prawidłowym ich udostępnianiem w sytuacji, gdy odmowa w tym przedmiocie jest bezzasadna. Dlatego wobec wpływających do Generalnego Inspektora informacji o przypadkach odmowy udostępniania przez niektórych operatorów publicznej sieci telefonicznej służbom obsługującym numery alarmowe danych lokalizacyjnych abonentów wywołujących połączenia z tymi numerami, organ do spraw ochrony danych osobowych w piśmie skierowanym do ww. podmiotów zwrócił uwagę na art. 171 ust. 8 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.) jednoznacznie obligujący 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, jeżeli jest to konieczne do umożliwienia tym służbom wykonywania zadań w możliwie najbardziej efektywny sposób. Generalny Inspektor podkreślił, że regulacje zawarte w ustawie o ochronie danych osobowych w żadnym razie nie mogą stanowić uzasadnienia dla nieudostępniania informacji niezbędnych do prowadzenia działań ratujących życie.²²³

W roku sprawozdawczym 2007 Generalny Inspektor zwrócił się także do Ministra Sportu i Turystyki o podjęcie działań legislacyjnych mających na celu uregulowanie w ustawie z dnia 18 stycznia 1996 r. o kulturze fizycznej (Dz. U. z 2001 r. Nr 81, poz. 889 z późn. zm.) obowiązku złożenia przez kandydata do przyznania odznaki „Za Zasługi dla Sportu” oświadczenia o niekaralności za umyślne przestępstwo lub przestępstwo skarbowe, dołączanego do wniosku o przyznanie odznaki, i usunięcie tego wymogu (§ 4 ust. 5) z rozporządzenia Ministra Sportu z dnia 6 czerwca 2007 r. w sprawie nagradzania za szczególne osiągnięcia w dziedzinie kultury fizycznej (Dz. U. Nr 113, poz. 777).²²⁴ Jednocześnie zwrócił uwagę na art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, który stanowi, że przetwarzanie danych osobowych tzw. wrażliwych, m.in. dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, jest dopuszczalne wtedy, gdy na przetwarzanie

²²² Zgodnie z art. 19 ustawy o ochronie danych osobowych, w razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będących administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

²²³ Wystąpienia Generalnego Inspektora z dnia 5 marca 2007 r. o sygn. GI-DOLiS-024/275/07

²²⁴ Wystąpienie Generalnego Inspektora z dnia 27 grudnia 2007 r. o sygn. GI-DOLiS-024/879/07

takich danych bez zgody osoby, której one dotyczą, zezwala przepis szczególny innej ustawy i stwarza pełne gwarancje ich ochrony. Tymczasem – jak podkreślił organ powołany do spraw ochrony danych osobowych – upoważnienie do wydania przedmiotowego rozporządzenia, zawarte w art. 45 ust. 3 ustawy o kulturze fizycznej, nie odnosi się w ogóle do zagadnienia przetwarzania danych, a w związku z tym nie może stanowić podstawy legalizującej proces przetwarzania informacji dotyczących karalności za popełnione umyślnie przestępstwo lub przestępstwo skarbowe odnoszących się do kandydata do przyznania odznaki. Rozporządzenie natomiast jest aktem prawnym zbyt niskiej rangi, aby można było uznać, że przesłanka określona w art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych była w tym przypadku spełniona.

Ponadto w omawianej sprawie Generalny Inspektor zaproponował rozważenie, czy celowe było ustanowienie wymogu składania oświadczeń o niekaralności w przypadku wnioskowania o przyznanie odznaki „Za Zasługi dla Sportu”. Podkreślił, iż zgodnie z § 2 ust. 2 rozporządzenia, odznaka ta jest przyznawana osobom wyróżniającym się szczególną aktywnością i uzyskującym wybitne osiągnięcia w działalności zawodowej i społecznej w dziedzinie kultury fizycznej, a zatem jest dowodem uznania dla dokonań konkretnej osoby w tym zakresie. Generalny Inspektor wskazał wobec tego, że nie wydaje się, aby niekaralność osoby za przestępstwa umyślne stanowiła warunek konieczny, którego spełnienie ma decydujące znaczenie dla przyznania odznaki (co nie oznacza oczywiście zamiaru deprecjonowania tego warunku).

W bieżącym okresie sprawozdawczym GIODO zasygnalizowano również budzącą wątpliwości kwestię stosowania art. 5 ust. 3 ustawy z dnia 18 grudnia 2003 r. o krajowym systemie ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności (Dz. U. z 2004 r. Nr 10, poz. 76 z późn. zm.), a konkretnie udostępniania danych z rzeczzonego zbioru danych na wniosek administracyjnego organu egzekucyjnego, który nie został wymieniony w powołanym wyżej przepisie jako podmiot uprawniony do ich pozyskania.²²⁵ W sprawie tej zaistniał problem legalności udostępnienia danych z Krajowego Systemu Ewidencji Producentów, Ewidencji Gospodarstw Rolnych oraz Ewidencji Wniosków o Przyznanie Płatności na wniosek administracyjnego organu egzekucyjnego, który ze swym żądaniem występuje na podstawie art. 36 § 1 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.).²²⁶ W piśmie, które wpłynęło do Generalnego Inspektora, podniesiono, że skoro przepis art. 5 ust. 3 ustawy o krajowym systemie

²²⁵ Stosownie do treści art. 5 ust. 3 tej ustawy, dane indywidualne zawarte w systemie mogą być udostępniane wyłącznie organom statystyki publicznej oraz organom Inspekcji Weterynaryjnej w zakresie identyfikacji producentów, natomiast dane zbiorcze mogą być udostępniane innym organom administracji publicznej prowadzącym systemy informacyjne.

²²⁶ Zgodnie z tym przepisem, w zakresie niezbędnym do prowadzenia egzekucji organ egzekucyjny może żądać od uczestników postępowania informacji i wyjaśnień, jak również zwracać się o udzielenie informacji do organów

ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności uprawnia do udostępnienia danych indywidualnych zawartych we wskazanym systemie wyłącznie organom statystyki publicznej oraz organom Inspekcji Weterynaryjnej w zakresie identyfikacji producentów, w swym obecnym kształcie uniemożliwia on innym podmiotom, takim jak np. administracyjny organ egzekucyjny lub komornik, realizację ich ustawowych zadań. Generalny Inspektor, analizując problem, zwrócił uwagę na okoliczność, iż krąg podmiotów, do których organ egzekucyjny może się zwracać o udzielenie informacji, jest nieograniczony.²²⁷ Podniósł, iż art. 77 ust. 1 Konstytucji RP przesądza o uprawnieniu każdego do wynagrodzenia szkody, jaka została mu wyrządzona przez niezgodne z prawem działanie organu władzy publicznej, oraz wskazał, że w kwestii tej wypowiedział się również Sąd Najwyższy.²²⁸ Podkreślił dalej, że także z punktu widzenia ustawy o ochronie danych osobowych działanie administracyjnego organu egzekucyjnego ma uzasadnienie w jej art. 23 ust. 1 pkt 2.²²⁹ Organ do spraw ochrony danych osobowych w związku z faktem, iż w jego ocenie ten stan rzeczy jest sprzeczny z postulatem wewnętrznej spójności systemu prawa, wystąpił do Ministra Rolnictwa i Rozwoju Wsi o podjęcie działań zmierzających do zmiany treści przepisu art. 5 ust. 3 ustawy o krajowym systemie ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności w celu umożliwienia innym podmiotom realizowania ich uprawnień wynikających z innych, niż powołana wyżej ustawa, przepisów prawa, a tym samym zapewnienia wewnętrznej spójności systemu prawa.²³⁰

Uwagę Generalnego Inspektora Ochrony Danych Osobowych zwrócił również problem ewentualnej podstawy prawnej do udostępniania przez przedsiębiorców niemających statusu biura informacji gospodarczej i zajmujących się windykacją wierzytelności, w drodze ogłoszenia publicznego, informacji obejmujących dane dłużnika, kwotę i tytuł prawny oferowanych, w celu sprzedaży, wierzytelności. Kwestię tę sygnalizowały Generalnemu Inspektorowi osoby, których dane zostały ujawnione w sieci Internet, w powyższym celu, przez niemających statusu biura informacji gospodarczej przedsiębiorców, którzy jako podstawę prawną do podejmowania ww. działań wskazywali art. 3 ustawy z dnia 14 lutego 2003 r. o udostępnianiu informacji gospodarczych

administracji publicznej oraz jednostek organizacyjnych im podległych lub podporządkowanych, a także innych podmiotów.

²²⁷ Wszystkie podmioty, do których zwróci się organ egzekucyjny, są zobowiązane do udzielenia mu informacji, chyba że przysługuje im prawo odmowy zeznań w charakterze świadka (art. 83 § 1 Kodeksu postępowania administracyjnego) lub prawo odmowy odpowiedzi na zadane pytanie (art. 83 § 2 K.p.a.).

²²⁸ W wyroku z dnia 30 czerwca 2004 r. (sygn. akt IV CK 491/2003, opubl. *Gazeta Prawna* 2004/127, s. 18) Sąd Najwyższy – Izba Cywilna orzekł, iż Skarb Państwa ponosi odpowiedzialność na podstawie art. 77 ust. 1 Konstytucji za szkodę wyrządzoną taką działalnością legislacyjną organu władzy publicznej, której następstwem jest faktyczne pozbawienie lub ograniczenie możliwości realizacji uprawnień wynikających z innego aktu prawnego, co czyni system prawny w tym zakresie dysfunkcyjnym i wewnętrznie sprzecznym.

²²⁹ Stosownie do treści tego przepisu, przetwarzanie danych osobowych jest dopuszczalne, jeżeli jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

(Dz. U. Nr 50, poz. 424 z późn. zm.)²³¹ w związku z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Generalny Inspektor, analizując opisaną sprawę zauważył, iż w literaturze przedmiotu podkreśla się, że art. 3 ustawy o udostępnianiu informacji gospodarczych ustanawia wyjątek od zasady wyłączności udostępniania przez biura informacji gospodarczej informacji gospodarczych osobom trzecim, nieoznaczonym w chwili przeznaczania tych informacji. Udostępnianie informacji gospodarczych w celu sprzedaży wierzytelności przez ogłoszenie publiczne „nie tylko nie wymaga utworzenia biura informacji gospodarczej, ale także nie jest regulowane przepisami niniejszej ustawy. (...) Przy okazji omawiania zagadnienia związanego z udostępnianiem informacji o istniejących zobowiązaniach osobom nieoznaczonym w chwili ich udostępniania, np. na stronach internetowych, w celu sprzedaży wierzytelności przez ogłoszenie publiczne, należy wspomnieć, iż ustawa nie przesądza w sposób generalny, że publikowanie informacji o sprzedaży wierzytelności (tzw. kierowanie oferty *ad incertas personas*) w sposób umożliwiający identyfikację dłużnika jest dozwolone. Zapis ten ma jedynie na celu wyraźne zaznaczenie, że tego typu działalność nie jest objęta działalnością biura informacji gospodarczych.”²³²

Wobec powyższego Generalny Inspektor wystąpił do Ministra Gospodarki, jako dysponenta ustawy o udostępnianiu informacji gospodarczych, z prośbą o przedstawienie stanowiska w zasygnalizowanej sprawie²³³ oraz Prezesa Urzędu Ochrony Konkurencji i Konsumentów z prośbą o wyrażenie opinii, czy opisana praktyka, w sytuacji, gdy dłużnik jest konsumentem, nie narusza zbiorowych interesów konsumentów, o których mowa w art. 24 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. Nr 50, poz. 331 z późn. zm.).²³⁴

Często rozstrzyganymi przez Generalnego Inspektora wątpliwościami sygnalizowanymi przez **podmioty prywatne** były te z sektora zatrudnienia. Organ do spraw ochrony danych osobowych wypowiedział się m.in. w kwestii dopuszczalności stosowania przez pracodawców systemu rejestracji czasu pracy poprzez tzw. czytnik linii papilarnych lub czytnik obrazu tęczówki oka.²³⁵ Generalny Inspektor wskazał na art. 22¹ § 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.), na podstawie którego pracodawca może żądać od pracownika podania - niezależnie od danych osobowych, o których mowa w § 1 (tj. imię/imiona, nazwisko, imiona rodziców,

²³⁰ Wystąpienie Generalnego Inspektora z dnia 28 grudnia 2007 r. o sygn. DOLiS-035-166/07

²³¹ Zgodnie z tym przepisem, udostępnianie informacji gospodarczych osobom trzecim nieoznaczonym w chwili przeznaczania tych informacji do udostępniania następuje wyłącznie za pośrednictwem biur informacji gospodarczej, chyba że udostępnianie, o którym mowa powyżej, następuje w celu sprzedaży wierzytelności przez ogłoszenie publiczne lub przepisy prawa przewidują inny tryb udostępniania danych.

²³² Zob.: A. Mednis, J. Noga-Bogomilska, *Ustawa o udostępnianiu informacji gospodarczych. Komentarz*. Warszawa 2003, Wydawnictwo Prawnicze LexisNexis (wydanie I), s. 152.

²³³ Wystąpienie Generalnego Inspektora z dnia 27 grudnia 2007 r. o sygn. DOLiS-035-80/07

²³⁴ Wystąpienie Generalnego Inspektora z dnia 27 grudnia 2007 r. o sygn. DOLiS-035-80/07

²³⁵ Np. GI-DOLiS-024/270/07, GI-DOLiS-024/389/07, GI-DOLiS-024/610/07, GI-DOLiS-024/680/07

datę urodzenia, miejsce zamieszkania, adres do korespondencji, wykształcenie, przebieg dotychczasowego zatrudnienia) - również innych danych osobowych, 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, oraz numeru PESEL. Zakres danych osobowych pracownika, jakie pracodawca może gromadzić w związku z zatrudnieniem, został zatem szczegółowo określony w powołanych wyżej przepisach prawa. Jednocześnie z przepisów prawa pracy wynika, iż poza danymi wymienionymi w art. 22¹ § 1 i 2 Kodeksu pracy, pracodawca ma prawo żądać od pracownika podania tylko tych danych osobowych, w stosunku do których obowiązek ich podania wynika z odrębnych przepisów prawa (§ 4 tego artykułu).

Generalny Inspektor zauważył, że w obowiązującym porządku prawnym brak jest przepisów powszechnie obowiązujących odnoszących się do szerokiej kategorii podmiotów, na podstawie których pracodawca - celem kontroli czasu pracy podległych mu pracowników - mógłby pozyskiwać od nich dane biometryczne, do których należą m.in. linie papilarne czy obraz tęczy oka. Wskazywał, iż pozyskiwanie przez pracodawcę od pracowników ich danych biometrycznych w celu, o którym wyżej mowa, jest niedopuszczalne.

Do Generalnego Inspektora Ochrony Danych Osobowych zwróciła się również osoba zaniepokojona działaniem swego przełożonego, który pod jej nieobecność w pracy zlecił przeprowadzenie kontroli zawartości jej komputera służbowego, w tym treści archiwum rozmów komunikatora internetowego.²³⁶ Generalny Inspektor, analizując takie działanie, odniósł się do treści wyroku Europejskiego Trybunału Praw Człowieka w Strasburgu dotyczącego monitoringu rozmów telefonicznych i e-maili pracowników.²³⁷ Trybunał podkreślił w nim, iż zgodnie z art. 8 Europejskiej Konwencji Praw Człowieka (ratyfikowanej także przez Polskę), każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Trybunał uznał, że pracownicy powinni być poinformowani przez pracodawcę o dopuszczalności przeprowadzania przez niego kontroli w przedmiotowym zakresie. Wskazał dalej, że brak powiadomienia pracownika o monitorowaniu jego rozmów czy przesyłanej elektronicznie korespondencji, a także innej aktywności, można rozpatrywać w kontekście ewentualnego naruszenia jego prawa do prywatności. Wobec faktu, iż prawo do prywatności - podobnie jak inne dobra osobiste człowieka - podlega ochronie wynikającej z przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny, Generalny Inspektor wskazał w powyższym przypadku na możliwość dochodzenia roszczeń na drodze postępowania cywilnego, z tytułu ewentualnego naruszenia dóbr osobistych.²³⁸

²³⁶ GI-DOLiS-024/423/07

²³⁷ Wyrok ETPC z dnia 3 kwietnia 2007 r. w sprawie Copland v. The United Kingdom (no. 62617/00).

²³⁸ Zgodnie z art. 23 Kodeksu cywilnego, „(...) Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony

W innej sprawie, sygnalizowanej tym razem przez związek zawodowy jednego z pracodawców działających w sektorze bankowym, podnoszona była kwestia podstawy prawnej żądania przez tego pracodawcę imiennej listy osób objętych ochroną związkową. Generalny Inspektor zwrócił w pierwszej kolejności uwagę na jeden z wyroków Sądu Najwyższego²³⁹, w którym Sąd ten zgodził się z poglądem wyrażonym przez K. Rączkę w krytycznej glosie do wcześniejszego wyroku SN.²⁴⁰ Autor wskazał w niej, iż wynikający z art. 30 ust. 2¹ ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2001 r. Nr 79, poz. 854 z późn. zm.)²⁴¹ obowiązek pracodawcy zwrócenia się do organizacji związkowej o „informację o pracownikach korzystających z jej obrony” aktualizuje się w „indywidualnych sprawach pracowniczych”. Po pierwsze więc, analizowany przepis stanowi o jednej informacji dotyczącej pewnej zbiorowości, a nie o informacjach dotyczących poszczególnych pracowników. Po drugie, obowiązek zasięgnięcia stosownej informacji związany jest z pewną kategorią spraw, nie zaś ze sprawą konkretną. Jeśliby więc ustawodawcy rzeczywiście chodziło o każdorazowe zasięgnięcie informacji, gdy istnieje potrzeba współpracy pracodawcy ze związkami zawodowymi, to przepisowi temu nadałby inne brzmienie, a mianowicie wskazałby, iż w każdej sprawie, w której przepisy wymagają współdziałania z zakładową organizacją związkową, podmiot zatrudniający powinien zasięgać informacji o tym, czy konkretny pracownik, którego dotyczy dana sprawa, korzysta ze związkowej reprezentacji. Według stanowiska glosatora, przywołanego w tej sprawie przez Generalnego Inspektora Ochrony Danych Osobowych, obowiązek pracodawcy określony w powołanym przepisie ma charakter jednorazowy, a wszelkie zmiany w reprezentacji pracowników organizacje związkowe powinny sygnalizować pracodawcy bez ponowienia zwrócenia się o informację. Generalny Inspektor wskazał, że Sąd Najwyższy, opowiadając się za powyższym stanowiskiem, zwrócił uwagę na fakt, iż wprowadzenie w art. 30 ust. 2¹ ustawy o związkach zawodowych obowiązku udzielenia przez organizację związkową informacji w określonym terminie, pod rygorem zwolnienia pracodawcy z obowiązku konsultacji w sprawach indywidualnych, miało na celu przesunięcie konsekwencji bezczynności organizacji związkowej na tę organizację. Ponadto Sąd przywołał uzasadnienie wcześniejszego swojego wyroku²⁴², w którym sformułowano tezę, że

przewidzianej w innych przepisach (...)", zaś na podstawie art. 24 § 1 Kodeksu, „(...) Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny (...).”

²³⁹ Wyrok SN z dnia 23 stycznia 2002 r. (sygn. akt I PKN 809/2000, opubl. OSNP z 2004 r. nr 2, poz. 31)

²⁴⁰ Wyrok SN z dnia 21 kwietnia 1999 r. (sygn. akt I PKN 36/99, opubl. OSNAPiUS z 2000 r. nr 13, poz. 507)

²⁴¹ Zgodnie z treścią tego przepisu, w indywidualnych sprawach ze stosunku pracy, w których przepisy prawa pracy zobowiązują pracodawcę do współdziałania z zakładową organizacją związkową, pracodawca jest obowiązany zwrócić się do tej organizacji o informację o pracownikach korzystających z jej obrony, zgodnie z przepisami ust. 1 i 2. Nieudzielenie tej informacji w ciągu 5 dni zwalnia pracodawcę od obowiązku współdziałania z zakładową organizacją związkową w sprawach dotyczących tych pracowników.

²⁴² Wyrok SN z dnia 23 stycznia 2002 r. (sygn. akt I PKN 809/2000, opubl. OSNP z 2004 r. nr 2, poz. 31)

procedura konsultacji zamiaru wypowiedzenia umowy o pracę przewidziana w art. 38 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, nie obejmuje obowiązku pracodawcy zwrócenia się do zakładowej organizacji związkowej o informację o pracownikach korzystających z jej obrony. W uzasadnieniu tym Sąd stwierdził, że pracodawca nie ma obowiązku ponawiania wniosku o informację przed podejmowaniem każdej czynności wymagającej współdziałania ze związkami zawodowymi. Rzeczą związku zawodowego jest aktualizacja wykazu pracowników korzystających z jego obrony, a zobowiązuje go do tego generalna zasada wyrażona w art. 1 ust. 1 ustawy o związkach zawodowych, zgodnie z którą jest on powołany przez „ludzi pracy” do reprezentowania i obrony ich praw. Obrona „człowieka pracy” jest obowiązkiem związku zawodowego i na nim w pierwszej kolejności, a nie na pracodawcy, spoczywa obowiązek prawidłowej jej realizacji.

Generalny Inspektor wskazał, iż mając na uwadze przedstawione rozważania, można byłoby przyjąć, iż omawiany przepis art. 30 ust. 2¹ ustawy o związkach zawodowych daje pracodawcy formalną podstawę do występowania do zakładowej organizacji związkowej o informacje o wszystkich osobach korzystających z jej ochrony. Podkreślił jednak, iż z punktu widzenia określonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych zasady adekwatności danych w stosunku do celów ich przetwarzania, istotne jest, aby pracodawca w swoich działaniach powstrzymywał się przed gromadzeniem danych o pracowniku „na zapas”, w sytuacji, gdy nie zamierza w stosunku do niego podejmować kroków, które uzasadniałyby konieczność zwrócenia się do związków zawodowych, o przekazanie informacji o ewentualnym korzystaniu przez niego z ich obrony. Skonstatował tym samym, iż brak jest uzasadnienia dla przekazania przez zakładową organizację, do której zwraca się pracodawca, wykazu wszystkich pracowników korzystających z jej obrony.²⁴³

W okresie objętym sprawozdaniem do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło również pismo jednego z przedsiębiorców telekomunikacyjnych, w którym zasygnalizowano wątpliwości związane ze stosowaniem przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, która zastąpiła poprzednią ustawę z dnia 21 lipca 2000 r.²⁴⁴ Przedsiębiorca telekomunikacyjny zwrócił się o wyjaśnienie sytuacji osób, które umowy o świadczenie usług telekomunikacyjnych zawarły w okresie poprzedzającym obowiązywanie „nowej” ustawy – Prawo telekomunikacyjne. Wcześniej ustawa nie formułowała obowiązku uzyskiwania zgody abonentów na umieszczenie ich danych w publicznie dostępnym spisie abonentów lub na udostępnianie ich za pośrednictwem służb informacyjnych operatora (przewidywała jedynie możliwość złożenia zastrzeżenia wobec takiego działania). Po zmianie przepisów taka zgoda jest niezbędna. W związku z tym przedsiębiorca pytał, czy ewentualnie można domniemywać fakt wyrażenia tejże zgody, jeżeli umowa o świadczenie usług telekomunikacyjnych zawarta była poprzednim w stanie prawnym.

²⁴³ GI-DOLiS-024/985/07

²⁴⁴ GI-DOLiS-024/977/07

Generalny Inspektor, rozstrzygając zasygnalizowane wątpliwości, wskazał przede wszystkim na brak w przepisach przejściowych obecnie obowiązującej ustawy – Prawo telekomunikacyjne unormowań odnoszących się do tej kwestii. Podkreślił jednak, iż z punktu widzenia przepisów ustawy o ochronie danych osobowych nie jest możliwe domniemanie, iż wobec braku dokonania tego rodzaju zastrzeżenia osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie, w tym udostępnianie. Ustawa o ochronie danych osobowych nie posługuje się konstrukcją domniemanie wyrażenia zgody. Organ do spraw ochrony danych osobowych wskazał na art. 7 pkt 5 ustawy o ochronie danych osobowych²⁴⁵ i zaznaczył, że zgoda na przetwarzanie danych osobowych tego, kto ją wyraża, powinna być przedmiotem odrębnego oświadczenia, albowiem w innym razie wyłącza to swobodę złożenia oświadczenia o treści zgody na przetwarzanie danych osobowych. O udzieleniu zgody na przetwarzanie danych przez osobę, której dane dotyczą, nie można zatem wnioskować z faktu niedokonania przez nią zastrzeżenia dotyczącego umieszczenia w publicznie dostępnym spisie abonentów jej danych osobowych. Podsumowując, w opisanej sytuacji, dla zapewnienia zgodnego z przepisami o ochronie danych osobowych przetwarzania danych, konieczne jest wystąpienie do abonentów, którzy podpisali umowę o świadczenie usług telekomunikacyjnych na podstawie już nieobowiązującej ustawy – Prawo telekomunikacyjne, w celu uzyskania ich zgody na zamieszczenie dotyczących ich danych w publicznie dostępnym spisie abonentów. GODO podkreślił, iż powyższe stanowisko zasadne jest tym bardziej, gdy weźmie się pod uwagę, że w myśl art. 67 ust. 3 obowiązującej ustawy – Prawo telekomunikacyjne, do usługi informacji o numerach telefonicznych oraz do sporządzania spisu abonentów i związanego z tym udostępniania danych stosuje się odpowiednio przepisy art. 161 i art. 169, przy czym art. 103 ust. 3 tej ustawy odnosi ten sam zapis do usługi ogólnokrajowej informacji o numerach abonentów oraz do sporządzania ogólnokrajowego spisu abonentów i związanego z tym udostępniania danych.²⁴⁶

Z kolei wątpliwości innego przedsiębiorcy telekomunikacyjnego wzbudziła możliwość przekazania przedsiębiorcy wyznaczonemu do świadczenia usługi ogólnokrajowej informacji o numerach telefonicznych, stosownie do art. 67 ust. 1 ustawy – Prawo telekomunikacyjne²⁴⁷, poza

²⁴⁵ Zgodnie z tym przepisem, pod pojęciem zgody osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

²⁴⁶ Art. 161 ust. 1 Prawa telekomunikacyjnego określa podstawy do przetwarzania danych osobowych i stanowi, iż przetwarzanie jest dopuszczalne, gdy dotyczy usługi świadczonej użytkownikowi lub też gdy jest niezbędne do jej wykonania. Ponadto w innych celach, niż wymienione, przetwarzanie będzie możliwe w przypadkach określonych w prawie telekomunikacyjnym. Art. 169 ust. 3 stanowi z kolei, iż zamieszczenie w spisie danych identyfikujących abonenta będącego osobą fizyczną może nastąpić po uprzednim wyrażeniu przez niego zgody na dokonanie tych czynności.

²⁴⁷ Zgodnie z tym przepisem, dostawca publicznie dostępnych usług telefonicznych udostępnia niezbędne dane innym przedsiębiorcom telekomunikacyjnym prowadzącym spisy abonentów oraz usługę informacji o numerach telefonicznych, w tym usługę ogólnokrajowego spisu abonentów oraz usługę informacji o numerach obejmującej wszystkich abonentów publicznych sieci telefonicznych na terytorium Rzeczypospolitej Polskiej, zwaną dalej „ogólnokrajową informacją o numerach telefonicznych”.

danymi, o których mowa w art. 169 ust. 1 tej ustawy²⁴⁸. Chodziło zwłaszcza o informacje o dokładnym adresie abonenta ,tj. także numer posesji i/lub numer lokalu, w którym znajduje się zakończenie sieci udostępnione abonentowi (w przypadku stacjonarnej publicznej sieci telefonicznej) przekazywane na podstawie wyrażonej przez abonenta zgody na, cyt.: „(...) przetwarzanie (...) danych osobowych w celu umieszczenia w publicznie dostępnym spisie abonentów danych identyfikujących Abonenta oraz na przekazanie ww. danych innym przedsiębiorcom w celu publikacji spisu lub świadczenia usługi informacji o numerach telefonicznych (...)”, przy czym określenie „ww. dane” obejmuje jedynie te, o których mowa w art. 169 ust. 2 cytowanej ustawy.

W kierowanych do tego przedsiębiorcy wyjaśnieniach GODO podkreślił, iż dostawca publicznie dostępnych usług telekomunikacyjnych ma obowiązek udostępnić niezbędne dane innym przedsiębiorcom telekomunikacyjnym prowadzącym spisy abonentów lub świadczącym usługę informacji o numerach telefonicznych, w tym usługę ogólnokrajowego spisu abonentów oraz usługę informacji o numerach obejmującej wszystkich abonentów publicznych sieci telefonicznych na terytorium Rzeczypospolitej Polskiej, zwaną w ustawie – Prawo telekomunikacyjne „ogólnokrajową informacją o numerach telefonicznych”.²⁴⁹ Jednocześnie zaznaczył, iż obowiązujące regulacje nie określają, jakie dane mogłyby być uznane za niezbędne w takiej sytuacji, wobec czego, mimo że Generalny Inspektor dostrzegał konieczność przekazania przedsiębiorcy telekomunikacyjnemu świadczącemu wspomniane usługi takiego katalogu danych, który umożliwiałby mu skuteczną weryfikację abonenta, a co za tym idzie - prawidłową realizację usługi, to jednocześnie wskazał, iż przy rozstrzyganiu przedmiotowej kwestii należy brać pod uwagę także pozostałe przepisy ustawy – Prawo telekomunikacyjne oraz ustawy o ochronie danych osobowych. I tak, zgodnie z art. 103 ust. 3 Prawa telekomunikacyjnego, do usługi ogólnokrajowej informacji o numerach abonentów oraz do sporządzania ogólnokrajowego spisu abonentów (prowadzonej przez przedsiębiorcę wyznaczonego, o którym mowa w ust. 1 i 2 tego przepisu) i związanego z tym udostępniania danych, stosuje się przepisy art. 161 i 169 ustawy. Pierwszy z tych przepisów legalizuje możliwość przetwarzania treści lub danych objętych tajemnicą telekomunikacyjną (w tym ich udostępniania) wówczas, gdy czynności te dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania, oraz zezwala na przetwarzanie w innych celach, o ile jest ono dopuszczalne na podstawie przepisów ustawowych. Określa ponadto, jaki zakres danych użytkownika będącego osobą fizyczną, może przetwarzać dostawca publicznie dostępnych usług telekomunikacyjnych. Drugi przepis w ust. 1 pkt 1 wskazuje zakres danych, jakie

²⁴⁸ Zgodnie z tym przepisem, dane osobowe zawarte w publicznie dostępnym spisie abonentów, wydawanym w formie książkowej lub elektronicznej, a także udostępniane za pośrednictwem służb informacyjnych przedsiębiorcy telekomunikacyjnego powinny być ograniczone do: 1) numeru abonenta lub znaku identyfikującego abonenta; 2) nazwiska i imienia abonenta; 3) nazwy miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione abonentowi - w przypadku stacjonarnej publicznej sieci telefonicznej albo miejsca zameldowania abonenta na pobyt stały - w przypadku ruchomej publicznej sieci telefonicznej.

²⁴⁹ Powołany wcześniej art. 67 ust. 1 ustawy Prawa telekomunikacyjnego.

mogą być umieszczane w publicznie dostępnym spisie abonentów, wydawanym w formie książkowej lub elektronicznej, a także udostępniane za pośrednictwem służb informacyjnych przedsiębiorcy telekomunikacyjnego. Stosownie zaś do ust. 3 i 4 art. 169 Prawa telekomunikacyjnego, zamieszczenie w spisie danych identyfikujących abonenta będącego osobą fizyczną, czy ewentualnie rozszerzenie katalogu zamieszczanych w nim danych, może nastąpić wyłącznie po uprzednim wyrażeniu przez abonenta zgody na dokonanie tych czynności. Generalny Inspektor wskazał, iż przekazanie przez dostawcę publicznie dostępnych usług telefonicznych danych osobowych użytkowników przedsiębiorcy wyznaczonemu, prowadzącemu usługę ogólnokrajowej informacji o numerach telefonicznych, uzależnione jest przede wszystkim od uzyskania zgody osoby, której dane dotyczą, na takie działanie. Tym samym późniejsze umieszczenie tych danych w spisie abonentów prowadzonym przez przedsiębiorcę wyznaczonego, jak też korzystanie z nich dla realizacji usługi informacji o numerach, również powinno odbywać się na podstawie omawianej zgody. Podkreślił, iż do zgody takiej ma zastosowanie art. 174 Prawa telekomunikacyjnego²⁵⁰, a w zakresie w nim nieuregulowanym, art. 7 pkt 5 ustawy o ochronie danych osobowych, w myśl którego przez zgodę osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Formuła zgody na przetwarzanie danych osobowych – jak zaznaczył – powinna stanowić odrębne oświadczenie osoby, której dane dotyczą, zaś z jej treści w sposób niebudzący wątpliwości powinno wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażający zgodę musi mieć bowiem pełną świadomość tego, na co się godzi. Wobec tego Generalny Inspektor stwierdził, iż trudno przyjąć, aby podmiot danych miał świadomość, że wyrażając zgodę na „przetwarzanie swoich danych osobowych w celu umieszczenia w publicznie dostępnym spisie abonentów danych identyfikujących abonenta oraz na przekazanie ww. danych innym przedsiębiorcom w celu publikacji spisu lub świadczenia usługi informacji o numerach telefonicznych”, zgadza się na przekazanie swoich danych także w zakresie numeru posesji czy lokalu, w którym zainstalowane jest zakończenie sieci udostępnione abonentowi. Organ do spraw ochrony danych osobowych skonstatował, iż nie wykluczając możliwości przekazania podmiotowi prowadzącemu omawianą usługę przez dostawcę publicznie dostępnych usług telefonicznych danych o abonencie także w zakresie jego dokładnego adresu, działanie takie byłoby możliwe jedynie na podstawie wyraźnej zgody osoby, której dane dotyczą, obejmującej wskazanie zakresu danych, jakie podlegałyby przekazaniu.²⁵¹

²⁵⁰ Zgodnie z jego treścią, jeżeli przepisy ustawy wymagają wyrażenia zgody przez abonenta lub użytkownika końcowego, zgoda ta: 1) nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; 2) może być wyrażona drogą elektroniczną, pod warunkiem jej utrwalenia i potwierdzenia przez użytkownika; 3) może być wycofana w każdym czasie, w sposób prosty i wolny od opłat.

²⁵¹ DOLiS-035-9/07

Przedmiotem analizy GIODO była też sprawa związana z planowanym wydzieleniem części jednego z banków w trybie art. 124c ust. 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.)²⁵² w związku z art. 529 § 1 pkt 4 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych [dalej: K.s.h.],²⁵³ tj. przez przeniesienie części majątku pierwszego (zwanego dalej „Bankiem A”) na drugi (zwanego dalej „Bankiem B”). Do Generalnego Inspektora zwrócono się o wydanie opinii w sprawie dopuszczalności wzajemnego udostępniania sobie przez oba banki danych osobowych klientów, po dniu wydzielenia, w rozumieniu art. 530 § 2 K.s.h.²⁵⁴

Generalny Inspektor, analizując zagadnienie, doszedł do wniosku, iż „Bank B” w tzw. okresie przejściowym (tzn. między dniem wydzielenia, o którym mowa w art. 530 § 2 K.s.h., a dniem ostatecznej migracji danych „przejętych” klientów „Banku A” do Systemu Teleinformatycznego „Banku B”) może, na podstawie art. 31 ustawy o ochronie danych osobowych²⁵⁵, powierzyć przetwarzanie danych tych klientów „Bankowi A”. Generalny Inspektor zgodził się z poglądem zaprezentowanym w treści skierowanego do niego pisma, iż w przypadku podziału spółki, zgodnie z art. 531 § 1 K.s.h., spółki przejmujące lub spółki nowo zawiązane powstałe w związku z podziałem, wstępują z dniem podziału bądź z dniem wydzielenia w prawa i obowiązki spółki dzielonej, określone w planie podziału. Stąd z dniem wydzielenia „Bank B”, jako podmiot decydujący o celach i środkach przetwarzania danych klientów „przejętych”, stanie się ich administratorem i będzie mógł powierzyć przetwarzanie tych danych innemu podmiotowi w trybie art. 31 ustawy o ochronie danych osobowych (w tym także „Bankowi A”). Generalny Inspektor zaznaczył jednak, iż jego wątpliwości budzi celowość powierzenia przez „Bank A” danych swoich klientów, którzy po dniu wydzielenia w dalszym ciągu pozostaną klientami jedynie tego Banku, „Bankowi B”, a zamiar taki jednoznacznie wynikał z treści nadesłanej korespondencji. Generalny Inspektor zwrócił uwagę na fakt, iż art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych nakłada na administratora danych obowiązek dołożenia należytej staranności w celu ochrony interesów osób, których dane dotyczą, a zwłaszcza zapewnienia, by były

²⁵² Stosownie do treści powołanego przepisu, banki w formie spółki akcyjnej podlegają podziałowi jedynie w sposób określony w art. 529 § 1 pkt 4 Kodeksu spółek handlowych z zastrzeżeniem, że przeniesienie części majątku banku dzielonego nastąpi na spółkę akcyjną będącą bankiem krajowym lub instytucją kredytową.

²⁵³ Zgodnie z tym przepisem, podział spółki kapitałowej może być dokonany przez przeniesienie części majątku spółki dzielonej na istniejącą spółkę lub na spółkę nowo zawiązaną (podział przez wydzielenie) - Dz. U. Nr 94, poz. 1037 z późn. zm.

²⁵⁴ Jak przepis ten stanowi, wydzielenie nowej spółki następuje w dniu jej wpisu do rejestru. W przypadku przeniesienia części majątku spółki dzielonej na istniejącą spółkę, wydzielenie następuje w dniu wpisu do rejestru podwyższenia kapitału zakładowego spółki przejmującej (dzień wydzielenia).

²⁵⁵ Przepis ten w ust. 1 wskazuje, że administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych przez niego administrowanych. Podmiot, któremu powierzono przetwarzanie takich danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie (ust. 2). Ponadto jest on obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w jej art. 39a. W zakresie przestrzegania tych przepisów podmiot ten ponosi odpowiedzialność jak administrator danych (ust. 3). W przypadku powierzenia przetwarzania danych odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową (ust. 4).

one zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 tego przepisu. Podkreślił, iż wynikająca z tego przepisu zasada celowości przetwarzania danych sprzeciwia się przetwarzaniu danych przez ich administratora w oderwaniu od celu tego procesu, a podstawowym celem dla jakiego „Bank A” przetwarza dane osobowe swoich klientów jest realizacja umów łączących te osoby z bankiem.²⁵⁶

Generalny Inspektor wypowiedział się również w kwestii możliwości przekazania przez podmiot gospodarczy, będący pracodawcą i działający na terytorium Rzeczypospolitej Polskiej, organowi ścigania Republiki Federalnej Niemiec, danych osobowych byłego pracownika, podejrzanego o popełnienie czynu zabronionego na obszarze tego państwa.²⁵⁷ Generalny Inspektor wskazał, że w aktualnie obowiązującym na terytorium Rzeczypospolitej Polskiej stanie prawnym brak jest podstaw do podejmowania powyższych działań. Zwrócił uwagę, że organy ścigania w sprawach tego typu powinny kierować się Europejską Konwencją o pomocy prawnej w sprawach karnych z dnia 20 kwietnia 1959 r. (Dz. U. z 1999 r. Nr 76, poz. 854 z późn. zm.), a dodatkowo, w relacjach Polska – RFN, na uwadze należy mieć umowę między Rzeczpospolitą Polską a Republiką Federalną Niemiec o uzupełnieniu i ułatwieniu stosowania Europejskiej konwencji o pomocy prawnej w sprawach karnych z dnia 20 kwietnia 1959 r. podpisaną w Berlinie z dnia 17 lipca 2003 r., których przepisy wskazują tryb pomocy i organy właściwe do występowania z wnioskami o jej udzielenie.²⁵⁸

Wśród pytań kierowanych do Generalnego Inspektora Ochrony Danych Osobowych znajdowały się także takie, które były ściśle związane ze stosowaniem samej ustawy o ochronie danych osobowych. Generalny Inspektor wyjaśniał nadawcom m.in. charakter tzw. instytucji współadministrowania.²⁵⁹ Wskazywał, że możliwa jest sytuacja, w której z jednym zbiorem danych związanych będzie dwóch lub nawet większa liczba administratorów danych. Stan taki może wystąpić wówczas, gdy zbiór pozostaje we wspólnej dyspozycji więcej niż jednego podmiotu. W tym przypadku mogą oni działać wspólnie (a więc decyzje dotyczące zbioru podejmować we wzajemnym uzgodnieniu, w tym także opartym na podziale kompetencji) albo samodzielnie (i wtedy każdy z nich posiadałby status samodzielnego administratora danych, łącznie z wiążącymi się z tym uprawnieniami i

²⁵⁶ GI-DOLiS-024/867/07

²⁵⁷ GI-DOLiS-024/620/07

²⁵⁸ Zgodnie z art. 1 ust. 1 w zw. z art. 15 ust. 1 Europejskiej Konwencji o pomocy prawnej w sprawach karnych, Strony zobowiązują się do udzielania sobie, zgodnie z jej postanowieniami i w jak najkrótszym czasie, możliwie najszerszej pomocy prawnej w sprawach przestępstwa, których ściganie należy, w chwili występowania z wnioskiem, do właściwych organów Strony wzywającej. Wnioski o udzielenie pomocy prawnej, jak również wszelkie informacje przekazywane z własnej inicjatywy będą kierowane w formie pisemnej przez Ministerstwo Sprawiedliwości Strony wzywającej do Ministerstwa Sprawiedliwości Strony wezwanej i podlegać zwrotowi w tej samej drodze. Art. 10 ust. 1 umowy między Rzeczpospolitą Polską a Republiką Federalną Niemiec o uzupełnieniu i ułatwieniu stosowania Europejskiej konwencji o pomocy prawnej w sprawach karnych stanowi zaś, że, cyt.: „(...) Jeżeli Umowa niniejsza nie stanowi inaczej, organy sądowe obu Umawiających się Stron porozumiewają się bezpośrednio. Nie wyłącza to możliwości pośrednictwa Ministerstwa Sprawiedliwości Rzeczypospolitej Polskiej z jednej strony i Federalnego Ministerstwa Sprawiedliwości lub ministerstw sprawiedliwości krajów związkowych Republiki Federalnej Niemiec z drugiej strony (...)”.

²⁵⁹ Np. GI-DOLiS-024/360/07.

obowiązkami). Generalny Inspektor zwracał przy tym uwagę, że tożsame stanowisko prezentowane jest w literaturze przedmiotu.²⁶⁰

Wątpliwość pytających budziła również kwestia dopuszczalności rozwiązania polegającego na wydawaniu upoważnień do przetwarzania danych osobowych, o których jest mowa w art. 37 ustawy o ochronie danych osobowych²⁶¹ – w przypadku powierzenia ich przetwarzania w trybie art. 31 ustawy o ochronie danych osobowych²⁶² – przez podmiot, któremu przetwarzanie danych zostało powierzone. Generalny Inspektor, wyjaśniając powstałe wątpliwości, zwrócił uwagę na ust. 3 art. 31. Stosownie do jego treści, podmiot, któremu administrator danych powierzył ich przetwarzanie, jest obowiązany przed rozpoczęciem tego procesu podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39 ustawy, czyli również te zawarte w omawianym art. 37 odnoszącym się do nadawania upoważnień. Wskazał, iż z regulacji tej można wywnioskować, że w przypadku powierzenia przetwarzania danych, podmiot, któremu administrator danych powierzył ich przetwarzanie, będzie miał możliwość samodzielnie wydawać upoważnienia, o których mowa, np. swoim pracownikom, którzy na jego rzecz będą brali udział w tym procesie. Zaznaczył jednocześnie, że uprawnienie tego ostatniego w powyższym przedmiocie nie wyłącza możliwości wydawania upoważnień takim osobom przez samego administratora danych.²⁶³

Ogólna liczba wpływających do Generalnego Inspektora Ochrony Danych Osobowych pism z prośbą o interpretację przepisów dotyczących przetwarzania danych osobowych, mimo ich zmniejszenia w porównaniu z latami ubiegłymi, w dalszym ciągu utrzymuje się na dość wysokim poziomie. Niemniej widoczny jest coraz większy stopień złożoności poruszanych w treści pism problemów dotyczących tej tematyki, co prowadzi do wniosku, że podstawowa wiedza z zakresu zasad ochrony danych osobowych dotarła do świadomości szerokiej grupy podmiotów biorących udział w procesie ich przetwarzania.

²⁶⁰ Np. J. Barta, R. Markiewicz, P. Fajgielski, *Ochrona danych osobowych. Komentarz*, Wydanie IV, Wolters Kluwer Polska – LEX, Kraków 2007, s. 379

²⁶¹ Zgodnie z tym przepisem, do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

²⁶² W świetle art. 31 ust. 1 ustawy o ochronie danych osobowych, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych. Podmiot, któremu powierzono przetwarzanie takich danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie (ust. 2). Ponadto jest on obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36 – 39 ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w jej art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych (ust. 3). W przypadku powierzenia przetwarzania danych, odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodne z tą umową (ust. 4).

²⁶³ Np. DOLiS-035-119/07, DOLiS-035/51/07

6.2. Działalność informacyjna

W celu zapewnienia powszechnego dostępu do informacji, Generalny Inspektor w 2007 r. tradycyjnie już, korzystając z pośrednictwa mediów (prasa, radio, telewizja, agencje informacyjne i portale internetowe) oraz wszelkich innych form propagowania wiedzy o ochronie danych osobowych organizował konferencje prasowe, udzielał wywiadów i odpowiadał na indywidualne pytania dziennikarzy. Na bieżąco zamieszczał i poszerzał informacje zawarte na głównej stronie internetowej (www.giodo.gov.pl) oraz w Biuletynie Informacji Publicznej. Duży krąg odbiorców informacji zapewniły również publikacje książkowe, szkolenia oraz konferencje o charakterze naukowym organizowane przez GIODO. W 2007 r. informacje do pojedynczych odbiorców trafiały zarówno w formie pism, jak i ustnych wyjaśnień udzielanych podczas dyżurów telefonicznych oraz indywidualnych spotkań pracowników GIODO z osobami zainteresowanymi tematyką ochrony danych osobowych.

W 2007 r. przekazywane przez GIODO materiały obejmowały m.in. interpretację przepisów ustawy o ochronie danych osobowych, wystąpienia Generalnego Inspektora do podmiotów, w których sygnalizowane były nieprawidłowości dotyczące stosowania przepisów o ochronie danych osobowych, i odpowiedzi, na kierowane do Biura pytania. Informacje dotyczyły również podejmowanych, w indywidualnych sprawach rozstrzygnięć oraz działalności GIODO zarówno na arenie międzynarodowej, jak i krajowej.

a) Stałe, codzienne kontakty z mediami

W 2007 r. Generalny Inspektor kontynuował stałą współpracę z prasą o zasięgu ogólnopolskim i lokalnym, zwłaszcza z „Rzeczpospolitą”, „Gazetą Prawną”, „Gazetą Samorządu i Administracji”, w których cyklicznie ukazują się rubryki poświęcone ochronie danych osobowych. Jednocześnie materiały dotyczące tej tematyki publikowane są regularnie w innych gazetach ogólnopolskich i lokalnych. Na ich łamach GIODO publikował swoje opinie i wystąpienia wydawane na podstawie rozstrzygnięć konkretnych spraw oraz wszelkie inne informacje dotyczące ochrony danych osobowych. Dodatkowo w wielu gazetach zamieszczane były wywiady poświęcone zagadnieniom z dziedziny ochrony danych osobowych, którymi interesowały się media.

Generalny Inspektor dzięki stałej współpracy z „Gazetą Samorządu i Administracji” co miesiąc publikował odpowiedzi na pytania związane z ochroną danych osobowych w kontekście problematyki samorządowej. Czytelnicy tego pisma mogli też za pośrednictwem redakcji kierować do GIODO wszelkie pytania dotyczące omawianej problematyki. Ponadto Generalny Inspektor Ochrony Danych Osobowych w 2007 r. podpisał z „GŚiA” umowę, zgodnie z którą do 6 kolejnych wydań gazety z 2008 r. (nr. 2-7) dołączana będzie – opracowana przez GIODO – broszura informacyjna z cyklu „ABC ochrony danych osobowych”. Wraz z pierwszą z nich dystrybuowana ma być również ulotka informacyjna dotycząca przystąpienia Polski do strefy Schengen.

Generalny Inspektor rozpoczął również współpracę z poczytnymi pismami kobiecymi, takimi jak „Tina” i „Chwila dla Ciebie”. Zagadnienia tam publikowane, ujęte w prosty i czytelny sposób, uświadamiają mniej wyrobionym prawniczo czytelnikom zagrożenia płynące z nieznamości podstawowych zasadach ochrony danych osobowych. Poprzez te publikacje GODO wskazywał czytelnikom, jakich danych mogą od nas żądać instytucje, m.in. takie jak bank, ZUS, BIK. Artykuły te odniosły też taki efekt, że czytelnicy tych pism zaczęli zwracać się z pytaniami bezpośrednio do Biura GODO.

GODO utrzymywał także stałe kontakty z innymi mediami, takimi jak stacje telewizyjne i rozgłośnie radiowe, którym udostępniał - zarówno na ich prośbę, jak i z własnej inicjatywy - wszelkie ważne z punktu widzenia bieżących spraw informacje związane tematycznie z ochroną danych osobowych.

Odpowiadał również na liczne pytania zadawane przez przedstawicieli prasy o zasięgu ogólnopolskim i lokalnym. Do najczęściej poruszanych w prasie zagadnień należały:

- wyrzucanie na śmietnik dokumentów zawierających dane osobowe,
- wprowadzanie przez niektóre instytucje praktyki podawania danych osobowych przez telefon,
- gromadzenie przez podmioty danych osobowych w celu tworzenia tzw. księgi wejść i wyjść,
- spamming,
- przekazywanie przez spółdzielnie czy przewoźników danych dłużników do Krajowego Rejestru Długów,
- podsłuchy w firmie,
- handel bazami danych,
- kradzież tożsamości,
- powszechnie stosowana przez urzędy skarbowe praktyka dostępu stażystów i praktykantów do danych osobowych podatników,
- projekt nowelizacji ustawy o ochronie danych osobowych,
- instalowanie monitoringu wraz z podsłuchami w szkołach,
- upublicznianie danych dłużników na stronach internetowych banków w związku ze sprzedażą wierzytelności,
- traktowanie numeru IP komputera jako danej osobowej.

Ze względu na konieczność wyjaśnienia pojawiających się wielu pytań i wątpliwości GODO systematycznie przekazywał do prasy materiały informacyjne. Dotyczyły one zwłaszcza takich zagadnień, jak:

- rejestracja zbioru danych dotyczących radnych,
- udostępnianie danych z ewidencji ludności i dowodów osobistych,

- obowiązki starosty jako administratora danych gromadzonych w związku z wykonywaniem zadań publicznych dotyczących rejestracji pojazdów i wydawania dokumentów stwierdzających uprawnienie do kierowania pojazdami,
- podawanie do publicznej wiadomości nazwisk osób korzystających z pomocy społecznej oraz rodzaju i zakresu przyznanego świadczenia,
- dostęp do informacji z dokumentów IPN (na kanwie nowelizacji ustawy lustracyjnej),
- zakres danych, jakie firma może gromadzić o swoim kliencie (na podstawie formularzy stosowanych przez sieć sklepów Żabka),
- udostępnianie informacji o studentach przez uczelnie wyższe,
- udostępnianie danych osobowych ze względu na interes publiczny,
- przebieg przygotowań Polski do wejścia do strefy Schengen,
- udostępnianie Centralnemu Biuru Antykorupcyjnemu bazy danych prowadzonych przez ZUS,
- kradzież tożsamości.

Warto wspomnieć, iż w 2007 r. wciąż budziła wątpliwość - sygnalizowana przez media - kwestia odmowy udostępnienia służbom ratowniczym (GOPR, TOPR) przez operatorów publicznych sieci telefonicznych danych lokalizacyjnych abonentów wywołujących połączenia z tymi numerami. W tej materii Generalny Inspektor podjął szeroką kampanię informacyjną, określając takie działanie jako niedopuszczalne.

Odnosić też należy objęcie przez GIODO patronatem merytorycznym akcji „Chroń swoją tożsamość”, która miała na celu uświadomienie zagrożeń płynących z braku dbałości o dane osobowe. Wyniki przeprowadzonych przez pracowników naukowych Uniwersytetu Wrocławskiego badań na śmietnikach wykazały bowiem, iż wyrzucane tam dokumenty są cennym łupem dla złodziei, którzy wykorzystują tak zdobyte informacje do kradzieży tożsamości osób, których te dane dotyczą. Tematyka ochrony danych osobowych w kontekście kradzieży tożsamości omawiana była przez Generalnego Inspektora w większości stacji radiowych i telewizyjnych oraz na łamach prasy ogólnopolskiej i lokalnej.

b) Inne formy współpracy z mediami

- **Debaty Generalnego Inspektora Ochrony Danych Osobowych we współpracy z „Gazetą Prawną”**

W „Gazecie Prawnej” GIODO kontynuował cykl debat, inicjując za ich pośrednictwem społeczną dyskusję poświęconą najistotniejszym problemom związanych z ochroną danych osobowych w różnych dziedzinach życia.

W 2007 r. odbyło się 6 takich dyskusji. Były to:

- „*Ochrona danych osobowych a prawo do prywatności*” (29 stycznia 2007 r.)

Debata odbyła się w związku z obchodami Dnia Ochrony Danych Osobowych Rady Europy i poświęcona była m.in. potrzebie nowelizacji ustawy o ochronie danych osobowych oraz potrzebie opracowania kodeksów dobrych praktyk przez podmioty przetwarzające dane osobowe. Rozmówcy podkreślali także konieczność podnoszenia świadomości społecznej na temat zagrożeń wynikających z korzystania przez różne firmy i instytucje z coraz większego zakresu informacji o obywatelach.

- „*Prawo do prywatności osób publicznych*” (28 lutego 2007 r.)

W dyskusji o prywatności osób publicznych przeważał pogląd iż, nawet osoby publiczne mają prawo do prywatności, która może być naruszana tylko w kontekście ujawnienia interesu publicznego i w związku z wykonywaniem mandatu. Podkreślono, że istnieją skuteczne instrumenty prawa cywilnego i karnego, które chronią dostęp do prywatności osób publicznych.

- „*Przetwarzanie danych o stanie zdrowia w elektronicznych bazach medycznych*” (20 lipca 2007 r.)

Podczas debaty poruszony został temat wdrażania zintegrowanego systemu gromadzenia i przetwarzania danych medycznych. Jego wprowadzenie mogłoby wpłynąć m.in. na podniesienie jakości usług zdrowotnych oraz obniżenie kosztów opieki zdrowotnej. Uczestnicy spotkania wyrażali swoje opinie m.in. na temat tego, jak chronić zgromadzone informacje o pacjentach oraz kto powinien mieć do nich dostęp.

- „*Bezpieczeństwo danych osobowych w sieci*” (27 sierpnia 2007 r.)

Podczas rozmowy poruszony został temat przetwarzania danych osobowych w Internecie. Dyskusja poświęcona była głównie bezpiecznemu korzystaniu z usług internetowych oraz możliwościom skutecznej ochrony danych osobowych w sieci.

- „*Prawo do prywatności w społeczeństwie nadzorowanym*” (22 października 2007 r.)

Dyskusja odbyła się w Sejmie w związku z organizowanymi przez GODO obchodami 10-lecia ustawy o ochronie danych osobowych. Wśród tematów omawianych przez uczestników debaty znalazły się te najczęściej poruszane przez media w kontekście opisywania działalności osób publicznych, m.in. czy ujawniać informacje z życia prywatnego osób publicznych, kiedy media mogą ingerować w ich prywatność oraz kto jest osobą publiczną.

- „*Schengen a ochrona danych osobowych*” (14 grudnia 2007 r.)

Debata poświęcona była wejściu Polski do strefy Schengen i związanej z tym roli GODO w Systemie Informacyjnym Schengen (SIS). Jej uczestnicy wypowiadali się na temat stosowania zabezpieczeń danych przetwarzanych w SIS oraz wstępnej - przeprowadzonej przez GODO - kontroli systemu.

W zainicjowanych przez GODO debatach prowadzonych we współpracy z „GP” i na jej łamach udział brali eksperci ze środowisk tematycznie związanych z tematem dyskusji.

- **Konferencje prasowe Generalnego Inspektora Ochrony Danych Osobowych**

W 2007 r. Zespół Prasowy przygotował i zorganizował 5 konferencji prasowych:

- *Konferencja „Ochrona Danych Osobowych – gwarancja czy zagrożenie prywatności”* (29 stycznia 2007 r.)

Odbyła się ona z okazji Dnia Ochrony Danych Osobowych i została zorganizowana w Wyższej Szkole Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego w Warszawie. Stała się ona okazją do dyskusji na tematy związane z ochroną danych osobowych w kontekście postępu gospodarczego i rozwoju nowych technologii, zwłaszcza informatycznych. Dyskutowano o tym, jak pogodzić korzystanie ze zdobyczy techniki ułatwiających codzienne życie z prawem do ochrony danych osobowych oraz o tendencjach coraz szerszego zakresu informacji o obywatelach gromadzonych przez różne instytucje publiczne i prywatne.

- *Konferencja poświęcona nielegalnym działaniom firm marketingowych pt. „Wygrałeś? – Uwważaj!”* (4 kwietnia 2007 r.)

Odbyła się w siedzibie Urzędu Ochrony Konkurencji i Konsumentów w Warszawie. W czasie jej trwania został poruszony problem stosowania przez firmy marketingowe nielegalnych metod mających na celu wyłudzenie pieniędzy od obywateli.

Zagadnienia mechanizmu działania firm wysyłkowych, wykorzystywania danych przez nieuczciwe firmy wysyłkowe oraz doświadczenia w ich ściganiu, a także informacje, do kogo zwrócić się o pomoc, zostały przedstawione pod kątem działalności współpracujących ze sobą: Urzędu Ochrony Konkurencji i Konsumentów, Generalnego Inspektora Ochrony Danych Osobowych, Policji oraz Miejskiego Rzecznika Konsumentów w Warszawie. Przedstawiciele tych instytucji, wyjaśniając mechanizm „naciągania” obywateli przez nieuczciwe firmy marketingowe, przestrzegali - przed płynącymi z tego typu praktyk - zagrożeniami.

- *Spotkanie z dziennikarzami podczas zorganizowanego przez GIODO szkolenia dla pracowników Sądu Apelacyjnego, Sądu Okręgowego, Urzędu Miasta Sopotu, Urzędów Miejskiego i Wojewódzkiego w Gdańsku* (21 maja 2007 r.)

- *Konferencja w centrum prasowym PAP z okazji „Tygodnia Twojej Tożsamości”* (9 października 2007 r.)

Generalny Inspektor, obejmując akcję merytorycznym patronatem, zasygnalizował wagę zagrożeń wynikających ze zjawiska kradzieży tożsamości. Podczas konferencji przedstawiony został również raport pracowników Uniwersytetu Wrocławskiego zawierający wyniki badań przeprowadzonych w 2007 r. na wysypiskach śmieci w Warszawie. GIODO poinformował, że przygotowana jest nowelizacja ustawy, która pozwalałaby m.in. Generalnemu Inspektorowi na

nakładanie kar finansowych za niedostateczną ochronę danych osobowych w czasie ich przetwarzania.

- *Konferencja w Biurze GIODO pt. „Czy nasze dane są bezpieczne w Systemie Informacyjnym Schengen?”* (17 grudnia 2007 r.)

Konferencja poświęcona została wejściu Polski do strefy Schengen i związanej z tym roli GIODO w Systemie Informacyjnym Schengen (SIS). W czasie konferencji przekazane zostały wszelkie materiały informacyjne związane z wymienioną tematyką, w tym ulotka informacyjna dotycząca SIS.

- **Dyżury telefoniczne Generalnego Inspektora w dzienniku „Rzeczpospolita”**

W ramach upowszechniania informacji o ochronie danych osobowych, na łamach prasy ogólnopolskiej, Generalny Inspektor Ochrony Danych Osobowych kontynuował cykl dyżurów telefonicznych. Odbyły się one w Biurze GIODO za pośrednictwem redakcji „Rzeczpospolitej”. Osoby zainteresowane ochroną danych osobowych mogły bezpośrednio, telefonicznie zadać pytania dyżurującemu Generalnemu Inspektorowi i jego pracownikom. Najczęściej dotyczyły one problematyki ochrony danych osobowych z dziedziny prawa pracy, jak np.:

- monitoringu w miejscu pracy,
- zakresu informacji o kandydatach do pracy i pracownikach gromadzonych przez pracodawców,
- upoważnień do przetwarzania danych,
- skanowania linii papilarnych osób zatrudnionych w firmie,
- zabezpieczenia dokumentacji pracowniczej,
- księgi wejść i wyjść w zakładzie pracy.

Inne zagadnienia, o które pytali telefonujący, miały związek z przetwarzaniem danych osobowych w celach marketingu produktów i usług administratorów danych, rejestrowaniem zbiorów i prawami osób, których dane dotyczą. Wyjaśnienia udzielane na pytania czytelników publikowane były następnie na łamach „Rzeczpospolitej”.

Warto podkreślić, że dzięki coraz częstszemu publikowaniu przez media informacji dotyczących ochrony danych osobowych rośnie świadomość wagi tych zagadnień, zarówno wśród społeczeństwa, jak i u administratorów danych. Jednocześnie doniesienia medialne niejednokrotnie stały się podstawą do podjęcia przez Generalnego Inspektora Ochrony Danych Osobowych odpowiednich interwencji.

c) Publikacje GODO

Generalny Inspektor Ochrony Danych Osobowych rozpoczął we współpracy z Wydawnictwem Sejmowym druk cyklu broszur informacyjnych na temat ochrony danych osobowych. Są one przekazywane parlamentarzystom, dziennikarzom, eurodeputowanym oraz osobom, z którymi GODO współpracuje i dla których przeprowadza szkolenia. W 2007 r. ukazały się następujące publikacje:

- „ABC ochrony danych osobowych”,
- „ABC rejestracji zbiorów danych osobowych” ,
- „ABC wybranych zagadnień z ustawy o ochronie danych osobowych”,
- „ABC zasad kontroli przetwarzania danych osobowych”,
- „ABC zasad przekazywania danych osobowych do państw trzecich”,
- „ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych”.

d) Szkolenia, staże

W celu realizacji działalności edukacyjnej GODO organizował nieodpłatne **szkolenia**, które odbywały się systematycznie od stycznia do grudnia 2007 r. z przerwą wakacyjną. Stanowiły one swego rodzaju odpowiedź na zgłaszane przez zainteresowane podmioty zapotrzebowanie na wiedzę z zakresu ochrony danych osobowych.

Na szkoleniach przeprowadzonych w 2007 r. poruszane były różne kwestie związane ze stosowaniem przepisów o ochronie danych osobowych, zwłaszcza odnoszące się do takich zagadnień, jak:

- przesłanki dopuszczalności przetwarzania danych osobowych i ich praktyczne stosowanie,
- zasady udostępniania danych osobowych,
- przetwarzanie danych osobowych w systemach teleinformatycznych,
- obowiązki administratorów danych osobowych,
- warunki, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych,
- rejestracja zbiorów danych osobowych,
- informacje o sposobie korzystania z systemu e-GODO,
- zasady funkcjonowania przepisów o ochronie danych osobowych w odniesieniu do innych regulacji prawnych, jak prawo do prywatności czy prawo do informacji.

Generalny Inspektor Ochrony Danych Osobowych przeprowadził szkolenia m.in. dla: sędziów Sądu Okręgowego i Sądu Apelacyjnego w Gdańsku, archiwistów i komorników sądowych, marszałków województw oraz przedstawicieli samorządu terytorialnego województwa mazowieckiego i pomorskiego, Samorządowych Kolegiów Odwoławczych, Urzędu Komisji

Nadzoru Finansowego, Spółdzielczej Kasy Oszczędnościowo-Kredytowej, Ministerstwa Spraw Zagranicznych, Narodowego Banku Polskiego, Służby Celnej, Kancelarii Prezesa Rady Ministrów, Kancelarii Sejmu i Senatu oraz przedsiębiorców Polskiej Konfederacji Pracodawców Prywatnych „Lewiatan” i polskich posłów do parlamentu w Brukseli.

W 2007 r. odbyło się 60 takich szkoleń (zob. załącznik nr 6).

W Biurze Generalnego Inspektora Ochrony Danych Osobowych w lipcu i sierpniu 2007 r. organizowane były też **praktyki** dla studentów wydziału prawa, podczas których zapoznawali się oni z zagadnieniami dotyczącymi ochrony danych osobowych oraz ze specyfiką pracy w Biurze GIODO. Oprócz zadań wykonywanych w poszczególnych departamentach Biura GIODO uczestniczyli także w specjalnych - prowadzonych przez kadre kierowniczą oraz pracowników Biura - szkoleniach organizowanych cyklicznie dla wszystkich nowo zatrudnionych pracowników.

Projekt wymiany realizowany w ramach Programu Leonardo da Vinci

W 2007 r., w ramach Programu Leonardo da Vinci, rozpoczęła się realizacja projektu *„Nowe kompetencje osób odpowiedzialnych za wykonywanie przepisów ochrony danych osobowych”*, czas trwania którego przewidziano na 17 września 2007 r. – 30 czerwca 2008 r. Zakłada on 1-2-tygodniowe pobyty pracowników Biura GIODO w organach ochrony danych osobowych w 6 krajach: Czechach, Finlandii, Francji, Irlandii, Niemczech i Wielkiej Brytanii.

Dzięki niemu uczestnicy wyjazdów będą mieli możliwość pogłębienia wiedzy, pozyskania nowych informacji związanych ze stosowaniem prawa z zakresu ochrony danych osobowych przez inne organy zajmujące się tą problematyką, wymiany doświadczeń dotyczących funkcjonowania organów ochrony danych osobowych w kraju partnera, zapoznania się z systemem wdrażania prawodawstwa unijnego w wybranych obszarach objętych programem wymiany, a także wzmocnienia kompetencji językowych.

e) Konferencje zorganizowane przez Generalnego Inspektora oraz udział GIODO w konferencjach organizowanych przez inne podmioty

Dzień Ochrony Danych Osobowych

Rok 2007 zaczął się od bardzo ważnego wydarzenia w dziedzinie ochrony danych osobowych. Otóż Polska, po raz pierwszy, uczestniczyła w obchodach **Dnia Ochrony Danych Osobowych**. O ustanowieniu 28 stycznia świętem ochrony danych osobowych zdecydował Komitet Ministrów Rady Europy, biorąc pod uwagę, że tego dnia obchodzona jest rocznica otwarcia do podpisu Konwencji 108 Rady Europy z dnia 28 stycznia 1981 r. w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych - najstarszego aktu prawnego o zasięgu międzynarodowym, kompleksowo regulującego zagadnienia związane z ochroną danych osobowych. W ramach obchodów Dnia Ochrony Danych Osobowych odbyły się:

- **Konferencja „Ochrona Danych Osobowych – gwarancja czy zagrożenie prywatności” (29 stycznia 2007 r.)** - zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych oraz Rektora Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, prof. zw. dr hab. Andrzeja K. Koźmińskiego, a objęta patronatem przez Marszałka Sejmu Rzeczypospolitej Polskiej - Marka Jurka. Na konferencji poruszane były tematy związane z ochroną danych osobowych w kontekście postępu gospodarczego i rozwoju nowych technologii, zwłaszcza informatycznych. Dyskutowano o tym, jak pogodzić korzystanie ze zdobyczy techniki ułatwiających codzienne życie z prawem do ochrony danych osobowych, oraz o coraz szerszym zakresie informacji o obywatelach gromadzonych przez różne instytucje publiczne i prywatne.

- **Spotkanie Generalnego Inspektora z eurodeputowanymi w Brukseli (31 stycznia 2007 r.)** – odbyło się ono w siedzibie Parlamentu Europejskiego, w ramach posiedzenia Klubu Polskiego, podczas którego wystąpienia wygłosili Michał Serzycki, Generalny Inspektor Ochrony Danych Osobowych oraz Andrzej Lewiński, Zastępca Generalnego Inspektora Ochrony Danych Osobowych. Wykład na temat ustawy o ochronie danych osobowych poprowadziła Bogusława Pilc, Dyrektor Departamentu Inspekcji Biura Generalnego Inspektora Ochrony Danych Osobowych.

- **Spotkanie w Stałym Przedstawicielstwie Rzeczypospolitej Polskiej przy Unii Europejskiej w Brukseli (31 stycznia 2007 r.)** – zorganizowane przez Generalnego Inspektora Ochrony Danych Osobowych i Pana Piotra Wojtczaka, Radcę Ministra *Chargé d'affaires a.i.* Wzięły w nim udział osoby zajmujące się problematyką ochrony prywatności i danych osobowych w instytucjach unijnych oraz Radzie Europy, polscy eurodeputowani, przedstawiciele polskich placówek dyplomatycznych w Belgii oraz dziennikarze.

Z kolei zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych **Międzynarodowa Konferencja „Prawo do prywatności w społeczeństwie nadzorowanym” (22-23 października 2007 r.)** upamiętnić miała 10. rocznicę uchwalenia ustawy o ochronie danych osobowych. Towarzyszyły jej warsztaty „Prywatność a media”, zorganizowane we współpracy z Komisją Europejską, które pozwoliły na przedyskutowanie aktualnych kwestii ochrony prywatności i danych osobowych w kontekście działalności dziennikarskiej i publicystycznej.

Happening – Polska w Schengen (13 grudnia 2007 r.)

Z okazji wstąpienia Polski do Strefy Schengen w Wyższej Szkole Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego w Warszawie odbył się happening, w którym uczestniczyli m.in. przedstawiciele Biura Generalnego Inspektora Ochrony Danych Osobowych. W specjalnie utworzonym punkcie informacyjnym można było zapoznać się z materiałami dotyczącymi ochrony danych osobowych i roli Generalnego Inspektora w związku z funkcjonowaniem Systemu Informacyjnego Schengen. Przedstawiciele Biura GIODO zorganizowali prezentację multimedialną, przeprowadzili konkurs wiedzy o Schengen dla studentów, udzielali odpowiedzi na pytania osób zainteresowanych oraz

rozdawali materiały informacyjne (ulotki, płyty CD) na temat prawa o ochronie danych osobowych, zasadach ochrony prywatności w Systemie Informacyjnym Schengen oraz zasadach funkcjonowania Biura GIODO.

f) Informacja telefoniczna

Kolejnym istotnym instrumentem polityki informacyjnej jest możliwość zwracania się do GIODO z pytaniami dotyczącymi

Zasad ochrony danych osobowych wynikających zarówno wprost z ustawy o ochronie danych osobowych, jak i z innych przepisów prawa regulujących to zagadnienie.

Zainteresowani mogą:

- otrzymać indywidualne pisemne odpowiedzi na przesyłane pytania,
- uzyskać wyjaśnienia telefoniczne od prawników zatrudnionych u Generalnego Inspektora,
- osobiście spotkać się z pracownikami Biura, w siedzibie Biura GIODO.

g) Internet

Od momentu założenia w 1999 r. strony internetowej www.giodo.gov.pl obserwuje się stały wzrost jej odwiedzalności.

Strona jest na bieżąco aktualizowana i wzbogacana o nowe artykuły, a także kontrolowana pod kątem zgodności z obowiązującym stanem prawnym.

W 2007 r. dokonano na niej wielu zmian. Wiązało się to zwłaszcza z koniecznością dostosowania zawartej na niej strony Biuletynu Informacji Publicznej GIODO do wymagań nowego rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10, poz. 68), które zaczęło obowiązywać na początku 2007 r. W związku z tym, że jego przepisy obligowały Generalnego Inspektora do udostępnienia wielu informacji stanowiących informację publiczną, postanowiono przekształcić stronę internetową GIODO w stronę internetową Biuletynu Informacji Publicznej GIODO.

Ponadto w 2007 r. dodana została nowa kategoria: „Edukacja”, a w niej kolejne dwie podkategorie: „Szkolenia” i „Konkursy”. W „Szkoleniach” zamieszczony jest wykaz wszystkich szkoleń przeprowadzonych przez GIODO i jego pracowników w obecnej kadencji, która rozpoczęła się 13 lipca 2006 r. Z kolei podkategoria „Konkursy” zawiera informacje o przeprowadzanych przez GIODO konkursach, zasadach udziału w nich i nagrodach. Takie przedsięwzięcia mają na celu zwrócenie uwagi na tematykę ochrony danych osobowych oraz zachęcanie młodych ludzi (studentów oraz dzieci w wieku szkolnym) do rozwijania wiedzy z tej dziedziny.

Stronę internetową wzbogaca się na bieżąco, poprzez systematyczne zamieszczanie treści kolejnych decyzji oraz wystąpień Generalnego Inspektora do różnych podmiotów publicznych. W zakładce „Pytania i odpowiedzi” zamieszczono wiele nowych interpretacji problemów związanych z ochroną danych osobowych.

W kategorii „Prasa” – „Inne artykuły” zamieszczono liczne publikacje prasowe z 2007 r., które dziennikarze tworzyli na podstawie opinii GIODO. W kategorii „Publikacje GIODO” zamieszczone zostały broszury z cyklu „ABC”.

Wdrożenie Elektronicznej Skrzynki Podawczej (ESP)

Nowym elementem systemu informatycznego GIODO, wprowadzonym w roku 2007, była Elektroniczna Skrzynka Podawcza. Jej wdrożenie spowodowane było m.in. koniecznością dostosowania systemu informatycznego Biura GIODO do wymogów Rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno–technicznych doręczania dokumentów elektronicznych podmiotom publicznym. Kupione w związku z tym oprogramowanie zintegrowane zostało ze stroną podmiotową Biuletynu Informacji Publicznej GIODO. W efekcie na stronie internetowej umieszczono formularz główny do przekazywania pism drogą elektroniczną oraz 5 wyspecjalizowanych formularzy tematycznych o nazwach:

- Wniosek o wydanie zaświadczenia o zarejestrowaniu zbioru danych osobowych,
- Skarga na nieprawidłowości w procesie przetwarzania danych osobowych,
- Wniosek o wyjaśnienie zakresu stosowania przepisów o ochronie danych osobowych,
- Wniosek o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego,
- Wyjaśnienie w sprawie.

h) Inne informacje

Porozumienie między GIODO a Polską Federacją Rynku Nieruchomości (23 maja 2007 r.)

Generalny Inspektor Ochrony Danych Osobowych podpisał z Polską Federacją Rynku Nieruchomościami [dalej: PFRN] porozumienie o stałej współpracy na rzecz upowszechniania prawa do ochrony danych osobowych i prawa do prywatności oraz o tworzeniu kodeksu dobrych praktyk. Wydarzenie to miało miejsce na XIII Kongresie Polskiej Federacji Rynku Nieruchomości, która odbyła się 23 listopada 2007 r. w Pałacu Kultury i Nauki w Warszawie.

Projekt „Ochrona danych osobowych – moje prawa, moje zadania”

Projekt ten zakłada prowadzenie dwóch specjalistycznych modułów szkoleniowych w formule interaktywnych stron internetowych:

Moduł I – informacyjny, zawierający informacje obejmujące m.in. przegląd prawodawstwa krajowego i wspólnotowego związanego z ochroną danych osobowych,

Moduł II – szkoleniowy, zawierający 3 specjalistyczne kursy *e-learningowe* adresowane do trzech grup beneficjentów (osoby fizyczne, podmioty sektora prywatnego i publicznego).

Celem projektu jest zwiększenie wiedzy nt. polskiego i unijnego prawa dotyczącego ochrony danych osobowych oraz umiejętności praktycznego jej stosowania wśród wybranych grup docelowych.

I edycja konkursu plastycznego, pt. Prywatność wokół mnie”

Na konkurs zorganizowany przez Generalnego Inspektora dla uczniów warszawskich szkół podstawowych przysłanych zostało 39 prac z 7 szkół:

- | | |
|---|------------|
| - Szkoły Podstawowej Nr 255, ul. Kamionkowska 36/44 | - 2 prace |
| - Szkoły Podstawowej Nr 16, ul. Wilczy Dół 4 | - 3 prace |
| - Szkoły Podstawowej Nr 12 im. Powstańców Śląskich,
ul. Górnośląska 45 | - 9 prac |
| - Zespołu Szkolno-Przedszkolnego Nr 3, ul. Przyczółkowa 27 | - 22 prace |
| - Szkoły Podstawowej Nr 42, ul. Balkonowa 2/4 | - 1 praca |
| - Szkoły Podstawowej Nr 341, ul. Oławska 3 | - 1 praca |
| - Szkoły Podstawowej im. I Batalionu Saperów
Kościuszkowskich w Izabelinie ul. Szkolna 1 | - 1 praca |

Wystawa prac plastycznych nadesłanych na I edycję konkursu „Prywatność wokół mnie” została zorganizowana w Sali Kolumnowej Sejmu RP podczas międzynarodowej Konferencji „Prawo do prywatności w społeczeństwie nadzorowanym”, która odbyła się 22 i 23 października 2007 r.

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, tak jak w latach poprzednich, wśród różnych form działalności międzynarodowej podstawowe znaczenie miała współpraca Generalnego Inspektora z europejskimi rzecznikami ochrony danych osobowych na forum Unii Europejskiej. Odnosiła się ona zarówno do zagadnień związanych z przetwarzaniem danych osobowych zarówno w I, jak 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. Grupa Robocza Art. 29 przyjęła wiele dokumentów zawierających opinie oraz wytyczne dotyczące m.in. takich kwestii, jak pojęcie danych osobowych, elektroniczne bazy danych medycznych czy zbieranie danych osobowych pasażerów linii lotniczych w celach zwalczania przestępczości.

Częścią Grupy Roboczej Art. 29 są różnego rodzaju podgrupy powoływane w celu analizy szczegółowych zagadnień dotyczących ochrony danych osobowych oraz przygotowywania dokumentów na posiedzenia plenarne.

W 2007 r. Generalny Inspektor brał udział w pracach Wspólnego Organu Nadzorczego nad Europolem. Organ ten zajmuje się nadzorem nad przetwarzaniem danych osobowych w ramach Europejskiego Urzędu Policji oraz 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, którego Generalny Inspektor również jest członkiem.

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

W 2007 r. 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.

Generalny Inspektor brał udział w pracach dotyczących ochrony danych osobowych na forum Rady Europy, w tym zwłaszcza w pracach Komitetu Konsultacyjnego ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Przedstawiciel GIODO uczestniczył w 23 posiedzeniu plenarnym Komitetu, które odbyło się 15 i 16 marca 2007 r.

W działalności Generalnego Inspektora tradycyjnie dużą rolę odgrywa współpraca dwustronna, która polega m.in. na wymianie informacji, pomocy przy prowadzeniu postępowań administracyjnych, 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 lipcu 2007 r. w Warszawie gościli przedstawiciele czeskiego oraz bułgarskiego organu ochrony danych osobowych, a w październiku 2007 r. przedstawiciele litewskiego organu ochrony danych. Wizyty te stały się okazją do przedstawienia gościom funkcjonowania polskiego organu ochrony danych osobowych oraz wzajemnej wymiany doświadczeń dotyczących wdrażania przepisów o ochronie danych osobowych. Również Generalny Inspektor gościł z wizytą w czeskim urzędzie ochrony danych osobowych.

Generalny Inspektor oraz pracownicy Biura GIODO uczestniczyli także w konferencjach i seminariach o charakterze międzynarodowym. Do najważniejszych z nich należy zaliczyć te wymienione poniżej.

Między 25 a 28 września 2007 r. Generalny Inspektor brał udział w odbywającej się w Toronto Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności pt. „Horyzonty Prywatności – *Terra Incognita*”. Wśród poruszonych na niej tematów należy wymienić, takie jak: ochrona prywatności w kontekście zapewnienia bezpieczeństwa publicznego oraz globalizacji, prywatność a nanotechnologia, aspekty prawne rozwoju technologii, biobanki i przetwarzanie danych genetycznych. Ponadto na sesji zamkniętej rzeczników ochrony danych osobowych przyjęto Rezolucję w sprawie konieczności stworzenia globalnych standardów bezpieczeństwa danych pasażerów, Rezolucję w sprawie rozwoju standardów międzynarodowych, Rezolucję w sprawie współpracy międzynarodowej, Rezolucję Grupy Roboczej do spraw organizacji konferencji oraz Rezolucję w sprawie akredytacji nowych członków Konferencji (Słowenia, Macedonia, Nowa Finlandia i Labrador).

Z kolei 10 i 11 maja 2007 r. Generalny Inspektor brał udział w Wiosennej Konferencji Europejskich Organów Ochrony Danych, która odbyła się w Larnace na Cyprze. W czasie jej trwania poruszono m.in. problematykę dotyczącą ochrony danych osobowych w III filarze UE, narodowych baz danych medycznych oraz elektronicznej karty medycznej, ochrony danych osobowych wobec działalności mediów. W drugim dniu obrad przyjęto deklarację w sprawie decyzji ramowej o ochronie danych osobowych w III filarze UE oraz dokument poświęcony zasadzie dostępności. Na konferencji podjęto również decyzje w sprawie przyszłości afiliowanej przy niej Grupy Roboczej do spraw Policji, która - rozszerzając zakres swojego działania - zmieniła nazwę na Grupę Roboczą do spraw Policji i Wymiaru Sprawiedliwości.

Od 4 do 6 czerwca 2007 r. Generalny Inspektor brał udział w IX Spotkaniu Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej w Zadarze. Podczas tego spotkania poruszono m.in. następujące tematy: ochrona danych osobowych w III filarze UE; przejrzystość procesu przetwarzania danych, elektroniczne karty medyczne, wideonadzór, ochrona danych osobowych a dostęp do informacji publicznej. Ponadto organizację kolejnego X spotkania powierzono polskiemu organowi ochrony danych osobowych.

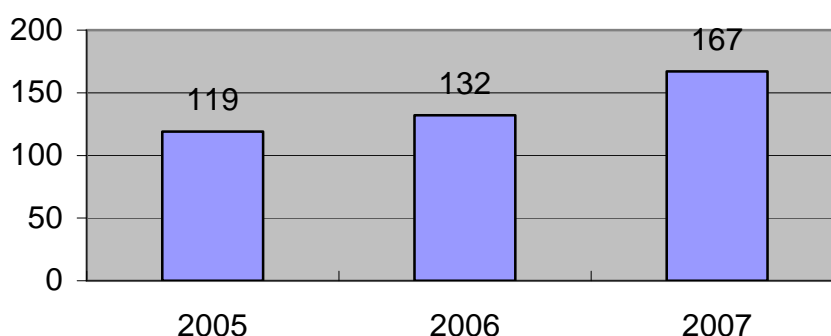
„Tendencje ochrony danych w społeczeństwie informacyjnym” to tytuł odbywającej się 13 i 14 listopada 2007 r. w Wilnie międzynarodowej konferencji, w której uczestniczył Zastępca Generalnego Inspektora. W czasie jej trwania Zastępca Dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej Biura GIODO przedstawił prezentację poświęconą systemowi E-GIODO – Elektronicznej Platformie Komunikacji z Generalnym Inspektorem.

Część II. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2007 roku

Oceniając wyniki przeprowadzonych **kontroli** należy stwierdzić, że większość kontrolowanych jednostek miała problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych przed ich udostępnieniem bądź zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także z prawidłowym opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych i polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Nieprawidłowości w tym zakresie stwierdzono zwłaszcza podczas kontroli podmiotów udzielających świadczeń zdrowotnych.

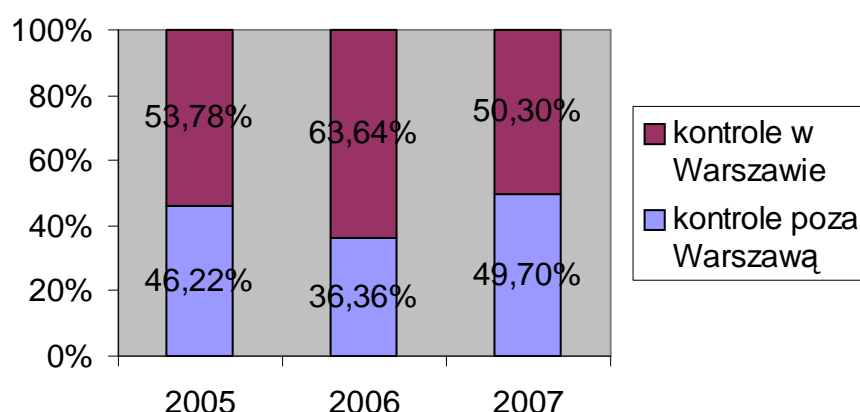
Liczne uchybienia występowały również w procesie przetwarzania danych osobowych przy użyciu **systemów informatycznych**. Trudności z prawidłowym wypełnieniem obowiązków określonych w przepisach rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, miały podmioty ze wszystkich sektorów opisanych w Sprawozdaniu. Dużo mniej problemów nastroczało natomiast prawidłowe wykonanie podstawowych obowiązków określonych w przepisach o ochronie danych osobowych. Nieprawidłowości w tym zakresie dotyczyły m.in. niedopełnienia obowiązku zgłoszenia prowadzonych zbiorów do rejestracji Generalnemu Inspektorowi oraz zbierania danych osobowych w szerszym zakresie niż wynika to z przepisów prawa.

W 2007 r. przeprowadzonych zostało 167 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych. To największa liczba od 2005 r. (patrz Wykres 22).



Wykres 22: *Porównanie liczby kontroli przeprowadzonych w latach 2005–2007.*

Z kolei Wykres 23 przedstawia procentowe zastawienie kontroli przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych na terenie Warszawy oraz poza nią.



Wykres 23: *Porównanie procentowe kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2005–2007.*

Najwięcej kontroli przeprowadzonych zostało z urzędu (113). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot je inicjujący:

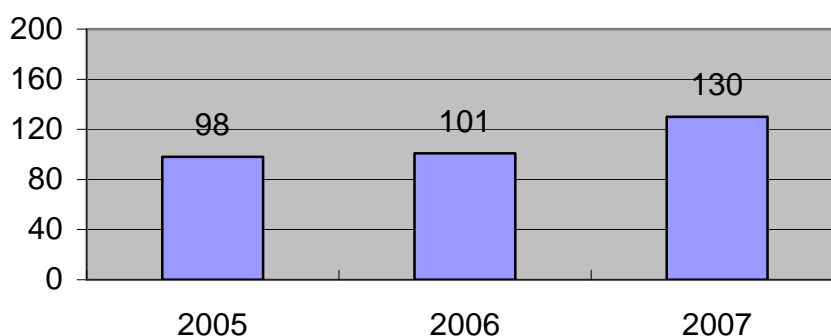
Inicjatywa kontroli	Liczba kontroli
Z urzędu	113
Departament Orzecznictwa, Legislacji i Skarg	32
Departament Rejestracji Zbiorów Danych Osobowych	7
Prokuratura	1
Komenda Główna Policji	2
Prezes Naczelnej Rady Lekarskiej	1
W związku z inną kontrolą	11

Najczęściej czynnościom kontrolnym poddawane były podmioty z sektorów administracji publicznej, służby zdrowia oraz instytucji finansowych. Jednak największą grupę jednostek kontrolowanych stanowiły podmioty zaliczone do sektora „Inne”, obejmującego te podmioty, które ze względu na charakter prowadzonej działalności nie mogły zostać zakwalifikowane do innej kategorii.

W okresie sprawozdawczym szczególny nacisk położony został na przeprowadzenie tzw. **kontroli sektorowych**, którymi objęto jednostki samorządu terytorialnego (25 kontroli), podmioty przetwarzające dane osobowe uczestników funduszy inwestycyjnych (16 kontroli), podmioty udzielające świadczeń zdrowotnych (24 kontrole) oraz archiwa państwowe (8 kontroli). 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 danego sektora.

Ponadto w 2007 r. sprawdzano, czy podmioty, wobec których Generalny Inspektor wydał decyzje nakazujące usunięcie uchybień w procesie przetwarzania danych osobowych, przywróciły stan zgodny z prawem. W tym celu Generalny Inspektor Ochrony Danych Osobowych przeprowadził 12 kontroli sprawdzających wykonanie decyzji administracyjnych. Wykazały one, że wszystkie skontrolowane ponownie podmioty wykonały wydane wobec nich decyzje. W 2007 r. Generalny Inspektor w związku z przeprowadzonymi kontrolami wydał łącznie 130 decyzji.



Wykres 24: *Porównanie liczby decyzji wydanych w związku z kontrolami przeprowadzonymi w latach 2005–2007.*

Należy także wskazać, że w 2007 r., w związku z wejściem Polski do strefy Schengen, zadania Generalnego Inspektora Ochrony Danych Osobowych zostały rozszerzone o kontrolę procesu przetwarzania danych osobowych przy użyciu Krajowego Systemu Informatycznego służącego do przekazywania oraz dostępu do danych gromadzonych w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej. Zadania Generalnego Inspektora w tym zakresie określone zostały w ustawie z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz w Systemie Informacji Wizowej (Dz. U. Nr 165, poz. 1170) i obejmują sprawowanie kontroli nad tym, czy wykorzystywanie danych nie narusza praw osób, których dane te dotyczą, oraz przeprowadzenie tzw. kontroli wstępnej Krajowego Systemu Informatycznego w celu sprawdzenia, czy spełnia on wymogi określone w art. 36–39 ustawy o ochronie danych osobowych i 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.

Podczas przeprowadzanych kontroli Generalny Inspektor Ochrony Danych Osobowych spotykał się z różnorodnymi rozwiązaniami technologicznymi w procesie przetwarzania danych

osobowych obejmującymi, z jednej strony, bardzo zaawansowane systemy informatyczne oparte na skomplikowanym mechanizmie bazodanowym, a z drugiej - powszechnie dostępne aplikacje biurowe. W przypadku rozbudowanych systemów informatycznych stwierdzono, że kontrolowane jednostki coraz częściej stosują globalne podejście do rozwiązywania problemów bezpieczeństwa przetwarzania danych osobowych, co powoduje, że obowiązki wynikające z przepisów o ochronie danych osobowych realizowane są coraz lepiej. Jest to związane z tym, że wdrożone zostały procedury wyznaczające sposób i zasady postępowania w zakresie bezpieczeństwa, co w połączeniu z zaawansowanymi rozwiązaniami technicznymi oraz z zastosowaniem mechanizmów i narzędzi zarządzania uprawnieniami użytkowników systemów informatycznych znacząco przyczyniło się do podniesienia poziomu ochrony danych osobowych.

Podkreślić również należy, że kontrole przeprowadzone w 2007 r. wykazały dalszy wzrost wykorzystywania technologii internetowych w procesie przetwarzania danych osobowych. Jednocześnie jednak stwierdzono, że osoby odpowiedzialne za przetwarzanie danych w podmiotach wykorzystujących technologie internetowe wykazywały dużą świadomość ryzyka związanego z transmisją danych w Internecie. Skutkowało to zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzanym danym, np. mechanizmów kryptograficznej ochrony danych osobowych. Natomiast w przypadku systemów informatycznych zainstalowanych na pojedynczych stanowiskach, niepodłączonych do sieci komputerowej, kluczową rolę odgrywały zabezpieczenia fizyczne obszaru przetwarzania danych oraz zabezpieczenia logiczne stacji komputerowych, np. przypisania użytkownikom odrębnych identyfikatorów. Część kontroli wykazała jednak, że ww. systemy nie zapewniały automatycznego odnotowania informacji o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane.

Duże znaczenie dla bezpieczeństwa danych osobowych miało także zapewnienie, aby dostęp do danych przyznawany był wyłącznie osobom upoważnionym i zaznajomionym z obowiązującymi w danym podmiocie zasadami bezpiecznego przetwarzania danych, w tym - z przepisami prawa. Określenie w taki sposób dostępu do danych minimalizowało ryzyko wystąpienia tzw. błędów ludzkich, gdyż świadomość pracowników, nie tylko co do już istniejących, ale także pojawiających się nowych zagrożeń, przekładała się bezpośrednio na wzrost ich poczucia odpowiedzialności za przetwarzane dane. Ponadto świadomość ta umacniana była poprzez stałe szkolenia pracowników w zakresie zagadnień związanych z bezpieczeństwem.

W ramach zadań kontrolnych związanych z oceną **zabezpieczeń technicznych** przeprowadzone zostały 161 kontrole, w tym 22 należące 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. Jedenaście z kontroli częściowych miało charakter sprawdzający wykonanie zaleceń pokontrolnych. W sumie skontrolowano **625 systemów informatycznych** wykorzystywanych do przetwarzania danych osobowych.

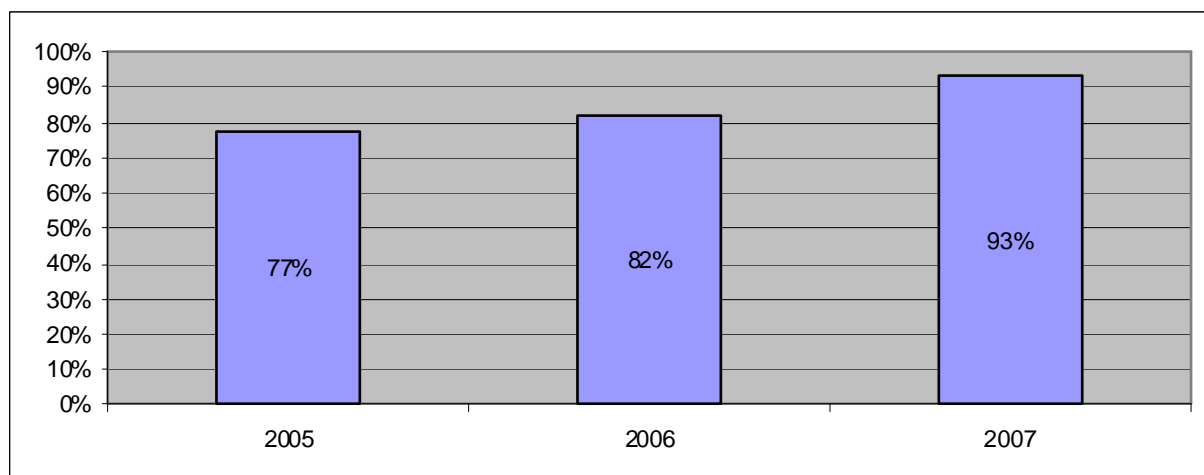
Jak wynika z poniższego zestawienia, od 2005 r. rośnie liczba skontrolowanych systemów informatycznych. I tak:

- w roku 2005 odbyło się 116 kontroli, obejmujących 456 systemów informatycznych,
- w roku 2006 odbyły się 124 kontrole, obejmujące 485 systemów informatycznych,
- w roku 2007 odbyło się 161 kontroli, obejmujących 625 systemów informatycznych.

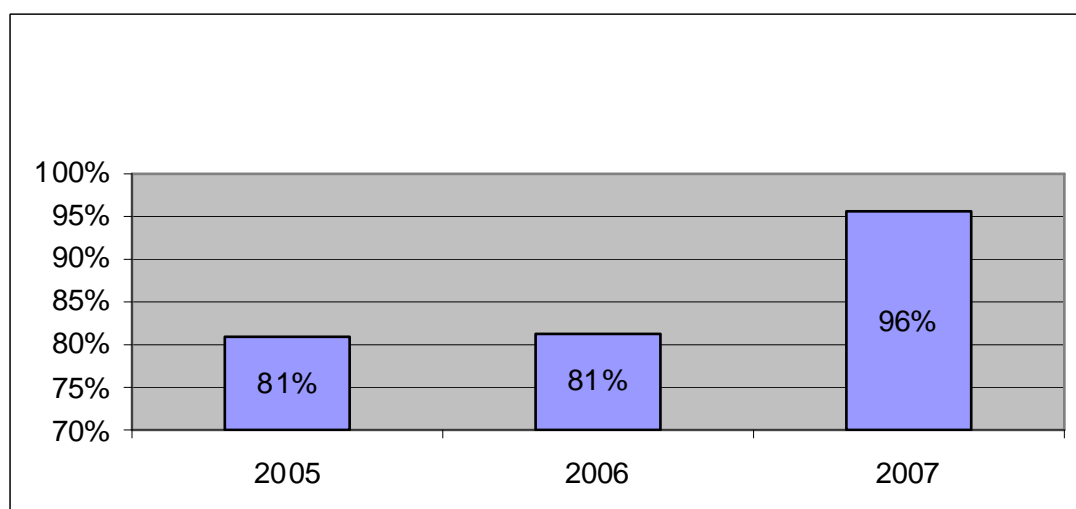
W większości kontrolowanych jednostek zaobserwowano tendencje do łączenia lub zastępowania odrębnych systemów informatycznych służących do przetwarzania danych o podobnym charakterze w jeden zintegrowany system modułowy. Wprowadzenie tego typu rozwiązań wykorzystujących nowoczesne technologie skutkowało spełnieniem wymogów ustawy i rozporządzenia. Wspomniane tu rozwiązania techniczne niejako wymuszały globalne podejście administratorów danych do zagadnień bezpieczeństwa, co powodowało, że również wymagania wynikające z ustawy o ochronie danych osobowych realizowane były w większości przypadków właściwie. Dodatkowo wdrożenie procedur sankcjonujących w sposób jednoznaczny postępowanie w zakresie bezpieczeństwa, w połączeniu z zaawansowanymi rozwiązaniami w obszarze ochrony fizycznej, spowodowało, że zabezpieczenie przetwarzanych danych utrzymywało się na odpowiednio wysokim poziomie. W jednostkach, w których wdrożono wspomniane rozwiązania, liczba nieprawidłowości dotyczących systemów informatycznych była znikoma lub uchybień takich nie stwierdzono w ogóle. Natomiast tam, gdzie wykorzystywano systemy informatyczne funkcjonujące jeszcze przed wejściem w życie ustawy, najczęstsze uchybienia w procesie przetwarzania danych osobowych dotyczyły braku w systemach informatycznych funkcjonalności umożliwiających odnotowanie daty pierwszego wprowadzenia danych, identyfikatora użytkownika wprowadzającego dane oraz stworzenie i wydrukowanie raportu zawierającego ww. informacje.

Stopień wypełnienia wymogów formalnych i organizacyjnych odnoszących się do warunków, jakim powinny odpowiadać urządzenia i systemy informatyczne używane do przetwarzania danych osobowych, przedstawiono na *Wykresach 25-29*. Poszczególne zestawienia obrazują procentowe wyniki kontroli w odniesieniu do ogólnej liczby kontroli w danym roku lub ogólnej liczby kontrolowanych w danym roku systemów informatycznych. Przy ich tworzeniu 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 danych lub do obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, oceniano w skali procentowej w stosunku do

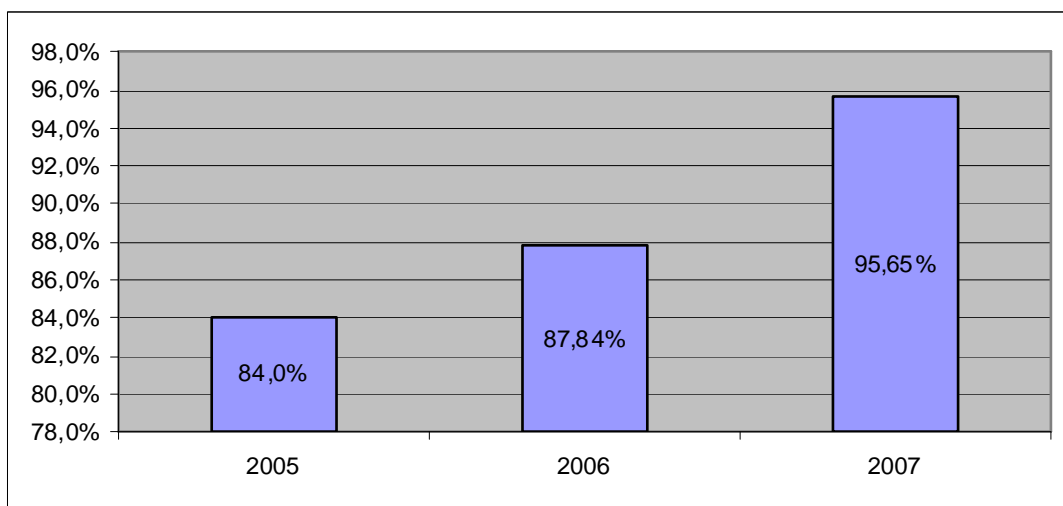
liczby kontrolowanych podmiotów. Z kolei w przypadku stopnia wypełnienia wymogów formalnych i organizacyjnych jednostkę statystyczną stanowił kontrolowany podmiot, zaś w zestawieniach odnoszących się do stopnia realizacji technicznych warunków przetwarzania danych - kontrolowany system lub kontrolowany 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 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.



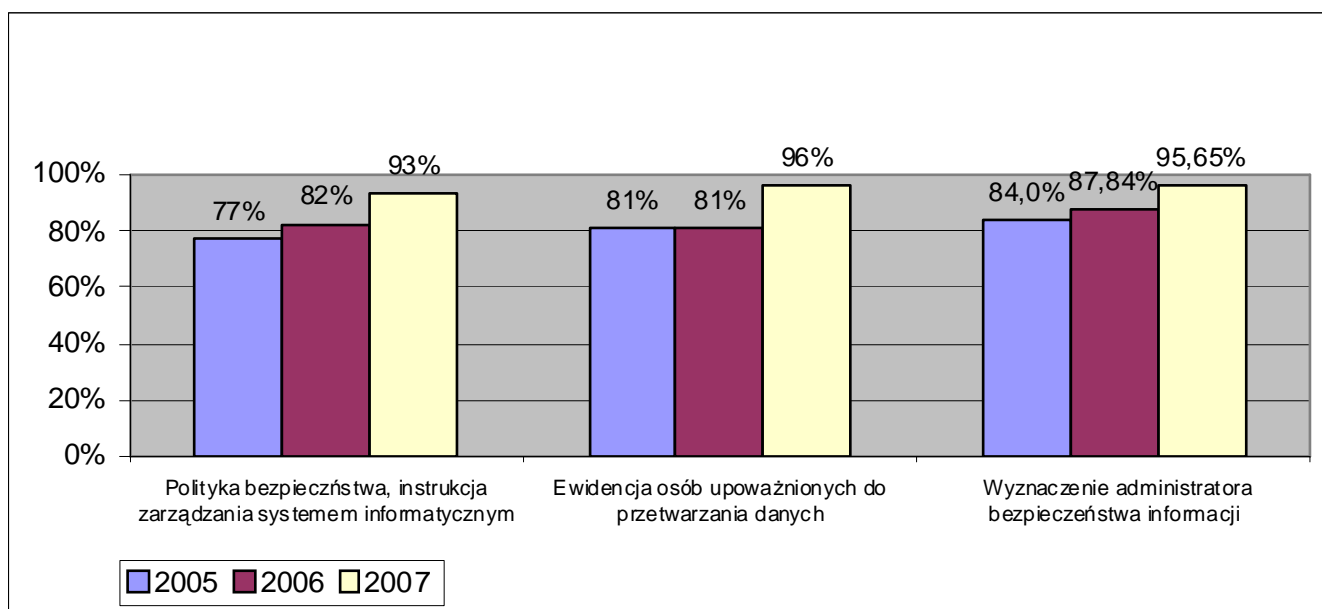
Wykres 25: *Stopień realizacji wykonania obowiązku opracowania dokumentacji polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w latach 2005-2007.*



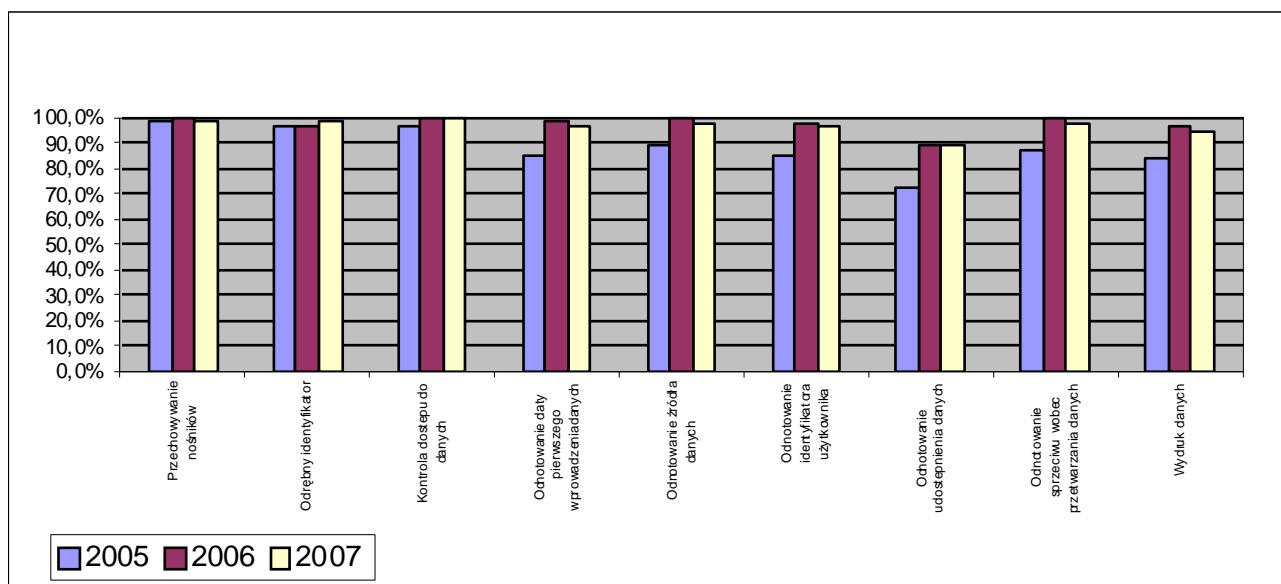
Wykres 26: *Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w latach 2005-2007.*



Wykres 27: *Stopień realizacji obowiązku wyznaczenia administratora bezpieczeństwa informacji w latach 2005-2007.*



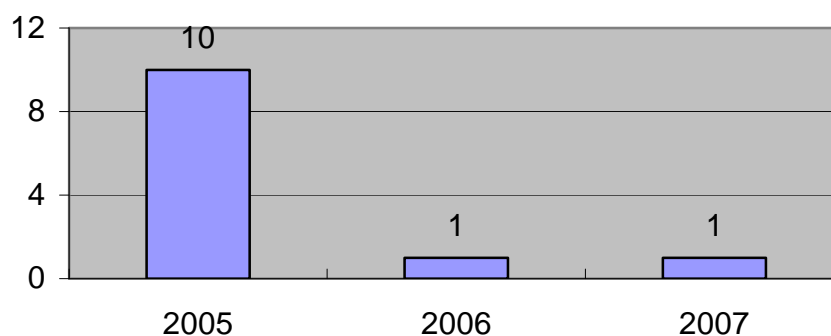
Wykres 28: *Stopień wypełnienia wymogów formalnych i organizacyjnych, jakim powinny odpowiadać urzędy i systemy informatyczne używane do przetwarzania danych osobowych, w latach 2005-2007.*



Wykres 29: *Stopień realizacji wymogów technicznych w latach 2005–2007.*

Kontrolowane jednostki nie wykonywały obowiązków określonych w przepisach o ochronie danych osobowych najczęściej z powodu błędnej ich interpretacji oraz niekonsekwentnego stosowania. Częstą przyczyną, głównie w przypadku podmiotów z sektora służby zdrowia, był również brak środków finansowych niezbędnych do pokrycia kosztów związanych z wdrożeniem odpowiednich rozwiązań informatycznych. W niektórych przypadkach odnotowano jednak niewłaściwe podejście osób odpowiedzialnych za przetwarzanie danych osobowych do problematyki ochrony danych, a nawet lekceważenie przepisów prawa. Świadczy o tym zwłaszcza niewykonywanie przez te osoby obowiązków, które nie pociągają za sobą nadmiernych kosztów finansowych, np. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych czy wyznaczenie administratora bezpieczeństwa informacji.

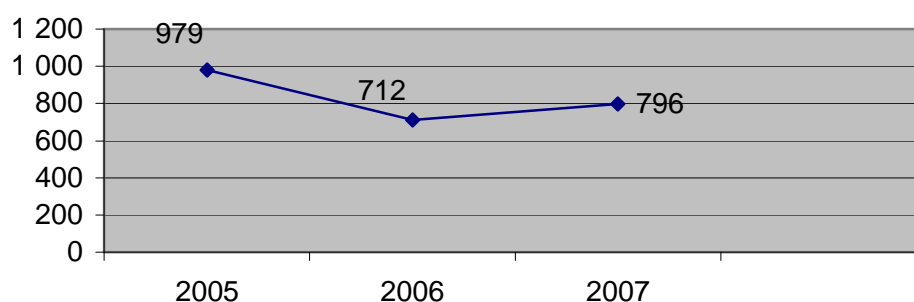
Na podkreślenie zasługuje fakt, że w większości przypadków stwierdzone w czasie kontroli uchybienia były usuwane przez jednostki kontrolowane w toku postępowania. Natomiast do jednostkowych należały sytuacje składania przez te jednostki wniosków o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora oraz zaskarżania decyzji do Wojewódzkiego Sądu Administracyjnego w Warszawie lub Naczelnego Sądu Administracyjnego.



Wykres 30: *Skargi wniesione do Wojewódzkiego Sądu Administracyjnego oraz Naczelnego Sądu Administracyjnego w związku z kontrolami przeprowadzonymi w latach 2005–2007.*

Na podstawie ustaleń z kontroli przeprowadzonych w 2007 r. należy stwierdzić, że w porównaniu z latami ubiegłymi osoby odpowiedzialne za przetwarzanie danych osobowych wykazały większą świadomość zagrożeń związanych z przetwarzaniem danych osobowych, a tym samym świadomość konieczności zapewnienia odpowiednich środków organizacyjnych i technicznych zapewniających ich ochronę. Konsekwencją było większe wyczulenie na prawidłowe dopełnienie obowiązków wynikających z przepisów o ochronie danych osobowych, co oczywiście nie oznacza, że obowiązki te wykonywane były zawsze w sposób właściwy. Niestety, spostrzeżenia te nie dotyczą wszystkich kontrolowanych podmiotów. Zdarzały się bowiem jednostki, w których nie wykonywano większości obowiązków wynikających z przepisów o ochronie danych osobowych.

W 2007 r. nieznacznie, w porównaniu z poprzednimi latami, wzrosła liczba **skarg**, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych, co obrazuje Wykres 31.



Wykres 31: *Zestawienie liczby skarg, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w latach 2005-2007.*

Ich ocena pod kątem znajomości i efektywności stosowania 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 rozpatrywanych w 2007 r. skargach najczęściej pojawiały się zarzuty nielegalnego przetwarzania (pozyskania i posiadania) danych osobowych zarówno przez podmioty publiczne (organy samorządu terytorialnego, organy administracji centralnej), jak i podmioty z sektora prywatnego. W grupie spraw dotyczących podmiotów publicznych najczęściej kwestionowano przetwarzanie danych osobowych w ramach prowadzonego przez organ postępowania administracyjnego bez zgody osoby, której dane dotyczyły i udostępniania danych między różnymi podmiotami administracji publicznej w związku z konkretnym postępowaniem administracyjnym. Najczęściej w takich przypadkach skargi okazywały się niezasadne. Wynikało to z błędnego przekonania osób skarżących, że brak ich zgody na takie działanie świadczyć ma o jego bezprawności. GODO stwierdzał natomiast, że w takich przypadkach, przetwarzając dane osobowe, organy działały na podstawie innych przepisów prawa i dlatego, mimo braku wspomianej zgody, takie postępowanie w świetle ustawy o ochronie danych osobowych było dopuszczalne.

W omawianym okresie sprawozdawczym znacznie **zmałała liczba skarg dotyczących organów administracji publicznej**. Świadczy to nie tylko o coraz lepszej znajomości przepisów ustawy wśród pracowników tych organów, ale również o ich właściwym stosowaniu.

W stopniu porównywalnym do poprzednich lat pojawiał się problem niewłaściwego zabezpieczenia danych osobowych i to zarówno wśród podmiotów z sektora publicznego, jak i prywatnego. W większości przypadków Generalny Inspektor stwierdził, iż przyczyną naruszeń przepisów w tym zakresie nie były uchybienia w kwestiach technicznych zabezpieczeń przetwarzania danych, lecz ignorowanie przepisów przez pracowników zatrudnionych przy przetwarzaniu danych. W takich przypadkach GODO, korzystając ze swoich ustawowych kompetencji, oprócz wydania stosownej decyzji administracyjnej, kierował również wnioski o wszczęcie postępowania dyscyplinarnego. Wiele skarg dotyczyło udostępnienia danych w związku z dochodzeniem roszczeń pieniężnych (na podstawie cesji wierzytelności lub zlecenia prowadzenia postępowania windykacyjnego). W tych przypadkach najwięcej spraw odnosiło się do podmiotów z sektora bankowości oraz operatorów telekomunikacyjnych. Większość skarg okazywała się jednak bezzasadna. W przypadku powierzenia danych wynikało to z błędnego przekonania osób skarżących, iż brak ich zgody na takie powierzenie danych innym podmiotom jest okolicznością wyłączającą legalność udostępnienia. W rzeczywistości znajdowało to podstawy w art. 31 ustawy o ochronie danych osobowych. W sytuacjach udostępnienia danych w wyniku cesji wierzytelności GODO przyjmował, że dłużnik nie mógł uwolnić się od spełnienia zobowiązania z powołaniem się na nielegalne, bo bez jego zgody, udostępnienie danych. W tej kwestii utrwaliła się linia orzecznicza rozpoczęta

rozstrzygnięciem NSA w składzie 7 sędziów²⁶⁴, który ustalił sposób interpretacji przepisów art. 23 ust. 1 ustawy w związku z treścią art. 509 § 1 oraz art. 385¹ § 1 i art. 385³ pkt 5 K.c. NSA wskazał ostatecznie na zastosowanie w takim przypadku przesłanki z art. 23 ust. 1 pkt 5 ustawy, argumentując m.in., że odnosi się ona wprost do administratora danych osobowych lub odbiorcy danych, którzy, aby zrealizować prawnie dopuszczalne cele, muszą udostępniać dane osobowe. Pod warunkiem wszakże, że nie naruszy to praw i wolności osoby, której dane dotyczą. NSA, a w późniejszym okresie również WSA w Warszawie²⁶⁵, uznawały, że prawnie usprawiedliwiony cel administratora danych, o którym mowa w art. 23 ust. 1 pkt 5 ustawy, może być oparty na przepisach prawa cywilnego. Za taki prawnie usprawiedliwiony cel ustawa uznaje dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej (art. 23 ust. 4 pkt 2 ustawy).

Przedmiotem skarg czyniono także niespełnienie, spełnianie w ograniczonym zakresie bądź spełnienie po upływie ustawowego 30-dniowego terminu, obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych. Administratorami, do których najczęściej adresowano takie skargi, były podmioty wykorzystujące dane osobowe do prowadzenia marketingu własnych produktów oraz podmioty świadczące usługi drogą elektroniczną. Oceniając treść wpływających skarg z perspektywy lat ubiegłych należy dodać, że problem ignorowania przez administratorów danych wspomnianego obowiązku informacyjnego nie ustał. Najczęściej w takich przypadkach administratorzy danych wskazywali, iż obowiązek ten jest bezprzedmiotowy, bowiem informacje w zakresie wskazanym w wymienionym przepisie są już znane osobie, która z wnioskiem o ich udzielenie występowała (np. w związku z zawarciem umowy cywilnoprawnej z administratorem). Tymczasem obowiązek informacyjny determinowany złożonym przez osobę zainteresowaną wnioskiem powinien być bezwzględnie spełniany, jeżeli jest kierowany do administratora danych nie częściej, niż co 6 miesięcy (art. 32 ust. 5 ustawy). W omawianym okresie pojawił się również problem naruszenia zasady celowości przetwarzania (pozyskiwania) przez spółdzielnie mieszkaniowe danych osobowych ich członków. Do tego rodzaju sytuacji dochodziło podczas pozyskiwania danych osobowych w zakresie szerszym, niż przewidują to przepisy prawa regulujące działalność spółdzielni. Natomiast dane te miały być ewentualnie wykorzystane w przyszłości w postępowaniu o zapłatę zaległości czynszowych. Takie zbieranie danych „na zapas” GIODO ocenił jako niedopuszczalne i podjął odpowiednie działania skierowane na wyeliminowanie powyższych praktyk.

W omawianym okresie istotą część spraw stanowiły te dotyczące przetwarzania danych osobowych osób publicznych w toku przygotowywania i publikowania informacji o takich osobach w materiałach prasowych. Analizowano wówczas dwie kwestie, tj. legalność udostępniania przez podmioty

²⁶⁴ Wyrok z dnia 6 czerwca 2005 r. (sygn. akt I OPS 2/05)

²⁶⁵ Np. wyrok WSA w Warszawie z dnia 27 stycznia 2006 r. (sygn. akt II SA/Wa 2077/05), wyrok WSA w Warszawie z dnia 31 marca 2006 r. (sygn. akt II SA/Wa 2396/04)

publiczne informacji o swoich pracownikach (osobach publicznych) dziennikarzom w kontekście ustawy o dostępie do informacji publicznej oraz legalność publikowania (ujawniania) tych danych w materiałach prasowych.

GIODO przyjął, że udostępnienie przez instytucję publiczną informacji (danych osobowych) ściśle związanych ze sprawowaną przez konkretnego pracownika funkcją publiczną i stanowiących w związku z tym informację publiczną w rozumieniu ustawy o dostępie do informacji publicznej, dziennikarzowi przygotowującemu materiał prasowy, stanowi realizację prawa dostępu obywateli do tego typu informacji i jako takie wypełnia przesłankę legalnego przetwarzania danych osobowych z pkt. 4 i 5 art. 23 ust. 1 ustawy o ochronie danych osobowych. Odnosząc się natomiast do kwestii zachowania rzetelności przy publikowaniu danych w materiale prasowym, w każdej z tego typu spraw GODO stwierdzał zastosowanie art. 3a ust. 2 ustawy o ochronie danych osobowych wyłączającego możliwość oceny tego zagadnienia w kontekście regulacji ww. ustawy. GODO w każdym tego typu przypadku wskazywał na odpowiednie przepisy ustawy Prawo prasowe, które zapewniają ochronę osobom, których prawa zostałyby naruszone wskutek publikacji prasowej.

W odniesieniu do zawiadomień o podejrzeniu popełnienia przestępstwa kierowanych przez Generalnego Inspektora Ochrony Danych Osobowych do organów ścigania w dalszym ciągu utrzymuje się duży współczynnik przypadków kończenia postępowań przygotowawczych bez sformułowania aktu oskarżenia. Podobnie jak w latach ubiegłych najczęściej odmawiano wszczęcia postępowania przygotowawczego bądź wszczęte umarzano, przywołując art. 17 § 1 pkt. 2 i 3 Kodeksu postępowania karnego, tj. wskazując, że czyn, o którym zawiadamiał GODO, nie zawierał znamion czynu zabronionego albo jego społeczna szkodliwość była znikoma. Z analizy treści uzasadnień takich postanowień nasuwał się jednak wniosek, iż podobnie do lat poprzednich, organy ścigania wykazywały się nieznajomością przepisów o ochronie danych osobowych oraz bezzasadną oceną przypadków złamania tej ustawy jako czynów o znikomej społecznej szkodliwości.

Inną z przesłanek umorzenia postępowań wykazywanych jako podstawa umorzenia (odmowy wszczęcia) postępowania było przedawnienie karalności czynu zagrożonego karą z ustawy o ochronie danych osobowych. W roku sprawozdawczym 2007 tylko w pięciu przypadkach postępowania przygotowawcze zakończyły się skierowaniem aktu oskarżenia do sądu.

Z kolei analiza przesyłanych w 2007 r. 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 – niezmiennie, od wielu lat obowiązywania prawa o ochronie danych osobowych, zainteresowane są pozyskiwaniem coraz szerszych uprawnień z zakresu przetwarzania danych. Niepokojące jest więc to, że wniosek z tej analizy od lat pozostaje bez zmian.

Podsumowując uchybienia popełnione w projektach aktów prawnych przesyłanych Generalnemu Inspektorowi do zaopiniowania w okresie objętym sprawozdaniem należy wskazać, że większość z nich dotyczy chęci pozyskiwania przez różnego rodzaju podmioty coraz większego zakresu danych, nieadekwatnego do celów ich przetwarzania lub takiego formułowania przepisów, z których wynika dowolność zakresu przetwarzanych danych w zależności od swobodnego uznania administratora. Zdarza się też i tak, iż projektodawcy wprowadzają do aktów prawnych przepisy, których wejście w życie naruszałoby wręcz porządek konstytucyjny.

Niemniej zauważalna jest tendencja do coraz częstszego uwzględniania zgłaszanych przez Generalnego Inspektora zastrzeżeń do poszczególnych projektów, tak w drodze prowadzonej korespondencji, jak i w wyniku uczestnictwa w posiedzeniach konferencji uzgodnieniowych i komisji prawnych.

W 2007 r. do Generalnego Inspektora wpłynęło 12 wniosków o **udzielenie zgody na przekazanie danych osobowych do państwa trzeciego**. Ponieważ duża liczba międzynarodowych transferów danych odbywa się w ramach Europejskiego Obszaru Gospodarczego, nie ma 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 (wymienionych w art. 47 ust. 1, 2 lub 3 ustawy o ochronie danych osobowych), przy zastosowaniu których zgoda Generalnego Inspektora nie jest wymagana. Należy także zauważyć niewielką świadomość istnienia szerokich możliwości zastosowania uregulowanych prawem wspólnotowym standardowych klauzul umownych, które mogą stanowić podstawę wyrażenia zgody przez Generalnego Inspektora.²⁶⁶

Generalny Inspektor jest uprawniony do udzielenia zgody na przekazanie danych osobowych do państwa trzeciego, pod warunkiem zapewnienia przez administratora danych odpowiedniego

²⁶⁶ Komisja Europejska, na mocy art. 26 ust. 4 dyrektywy 95/46/WE, jest uprawniona do uznania w drodze decyzji, że określone standardowe klauzule umowne zapewniają odpowiednią ochronę danych osobowych oraz praw i wolności jednostek. Decyzje te wymagają, aby państwa członkowskie nie odmawiały uznania zabezpieczeń ustanowionych w standardowych 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 standardowych 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 standardowe klauzule umowne mające zastosowanie do przekazywania danych osobowych w przypadku powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy o ochronie danych osobowych.

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) standardowe klauzule umowne przyjęte przez Komisję Europejską,
- b) wiążące reguły korporacyjne.²⁶⁷

W roku sprawozdawczym 2007 do Generalnego Inspektora wpływały wnioski, w których administratorzy danych powoływali się na zastosowanie standardowych klauzul umownych ustanowionych przez Komisję Europejską (jest to rozwiązanie preferowane przez większość organów ochrony danych osobowych w Unii) lub zmodyfikowanych standardowych klauzul umownych. 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.

Zadeklarowanie przez wnioskodawcę zastosowania standardowych klauzul umownych określonych decyzjami Komisji Europejskiej powoduje konieczność porównania przez Generalnego Inspektora przyjętych przez wnioskodawcę rozwiązań z treścią wzorcowych klauzul umownych. Ponadto Generalny Inspektor bada również okoliczności planowanego transferu danych (w tym również przyjęte przez odbiorcę danych organizacyjne i techniczne środki zabezpieczeń).

Z punktu widzenia **rejestracji zbiorów danych osobowych** nie można kategorycznie stwierdzić, iż rok 2007 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 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 lub nieścisłości występujących w zgłoszonych wnioskach. Pozytywnym aspektem

²⁶⁷ 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.

postępowań wyjaśniających jest edukacja. Administratorzy danych otrzymują w ten sposób fachowe wskazówki, a co za tym idzie szansę dostosowania prowadzonej działalności do wymogów określonych właściwymi przepisami prawa.

Niezmiennie więc rejestrację zbiorów utrudniają uchybienia w części zgłoszenia dotyczącej informacji o sposobie wypełnienia warunków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy o ochronie danych osobowych. Niejednokrotnie także deklarowany poziom bezpieczeństwa przetwarzania danych w systemie informatycznym nie spełniał wymogów określonych w rozporządzeniu wykonawczym do ustawy o ochronie danych osobowych.

Przepisy o ochronie danych osobowych określają elementy, które pozwalają scharakteryzować zbiór danych osobowych. Są to m.in.: cel, dla którego zbiór ten jest tworzony, podstawa prawna upoważniająca do prowadzenia zbioru oraz zakres danych przetwarzanych w zbiorze. Informacje te, dotyczące konkretnego zbioru, administrator danych powinien zawrzeć w formularzu zgłoszenia. Zatem jedno zgłoszenie do rejestracji powinno dotyczyć tylko jednego zbioru danych. W praktyce reguła ta przysparza administratorom danych wiele trudności. W 2007 r. charakterystycznym przykładem były zgłoszenia pochodzące od podmiotów publicznych, które realizują zdania z zakresu oświaty. Prowadzą one swoją działalność na podstawie wielu przepisów kompetencyjnych, przede wszystkim ustawy o systemie informacji oświatowej²⁶⁸ oraz ustawy o systemie oświaty.²⁶⁹ Nie dostrzegają jednak, iż każda ze wskazanych ustaw jest jednocześnie podstawą prawną do tworzenia odrębnego zbioru danych osobowych, który dotyczy innej kategorii osób i skutkuje przetwarzaniem innego zakresu danych. W rezultacie zgłoszenie nadesłane do rejestracji faktycznie dotyczy kilku zbiorów danych osobowych. Postępowania wyjaśniające w takich sprawach mają więc na celu spowodowanie, aby administrator danych prawidłowo dokonał zgłoszenia zbiorów, czyli zgłosił każdy z nich na odrębnym formularzu. Tylko wówczas można mówić, że wykonał, ciążący na nim z mocy art. 40 ustawy o ochronie danych osobowych, obowiązek zgłoszenia zbioru do rejestracji.

W okresie sprawozdawczym zanotowano wzrost dokonanych przez jednostki samorządu terytorialnego (gminy i powiaty) zgłoszeń do rejestracji zbiorów danych osobowych oraz wzrost zgłoszeń składanych w trybie art. 41 ust. 2 ustawy informujących o zmianach w zarejestrowanych zbiorach (zwykle zgłoszonych do rejestracji w 1999 r.). Gminy i powiaty coraz częściej występowały do Generalnego Inspektora Ochrony Danych Osobowych z wnioskami o wykreślenie zbiorów danych osobowych z rejestru. Można zatem mówić o wzroście wiedzy na temat obowiązków wynikających z ustawy o ochronie danych osobowych dotyczącej faktu, iż zmiany w obowiązujących przepisach, zwłaszcza zmiany kompetencyjne, powinny znaleźć odzwierciedlenie w rejestrze zbiorów danych

²⁶⁸Ustawa z dnia 19 lutego 2004 r. o systemie informacji oświatowej (Dz. U. Nr 49, poz. 463 z późn. zm.)

²⁶⁹ Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.)

osobowych. Obligują one bowiem administratorów danych działających w sferze publicznej do nieustannego monitorowania procesu przetwarzania danych osobowych i aktualizowania pierwotnie dokonanych zgłoszeń, tak aby były zgodnie z aktualnym stanem faktycznym i prawnym.

W 2007 r. Generalny Inspektor Ochrony Danych Osobowych rozpatrywał liczne zgłoszenia zmian pochodzące od podmiotów prywatnych zajmujących się działalnością finansową. Najczęściej były one związane z przekształceniem własnościowym. W postępowaniach wyjaśniających należało ustalić, na czym polegała reorganizacja i jakie ma przełożenie na prowadzenie zbiorów danych osobowych, przede wszystkim zaś, czy doszło do zmiany administratora danych. Większość rozpatrywanych spraw kończyła się wykreśleniem zbioru z rejestru w związku z zaprzestaniem przetwarzania danych przez dotychczasowego administratora i rejestracją nowego zbioru prowadzonego przez inny podmiot.

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 i bardzo dynamicznym. I to zarówno w odniesieniu do podmiotów ze sfery publicznej, jak i sektora prywatnego.

Mimo obserwowanej dynamiki napływu zgłoszeń zbiorów danych do rejestracji, przed Generalnym Inspektorem Ochrony Danych Osobowych w dalszym ciągu stoi zadanie aktywizowania administratorów danych, by dopełnili obowiązku rejestracyjnego. W tym celu GODO przesyła m.in. do podmiotów nadzorujących takich administratorów danych stosowne upomnienia.

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

Zarówno analiza wpływających do GODO skarg, jak i ustaleń pokontrolnych oraz doświadczeń wynikających z 10-letniego okresu obowiązywania ustawy o ochronie danych osobowych – mimo poddawania jej przepisów nowelizacjom (w tym dwu znaczącym, w 2001 i w 2004 r.) – wskazuje na potrzebę wprowadzenia kolejnych zmian, które miałyby na celu zagwarantowanie pełniejszej realizacji zasad ochrony danych osobowych. Dlatego podjęte zostały prace nad nowelizacją ustawy, której założeniem jest zmiana – mało efektywnych, jak wynika z dotychczasowych doświadczeń – rozwiązań dotyczących prawnokarnej ochrony danych osobowych. Wprowadzenie skutecznych środków egzekwowania przestrzegania zasad określonych w ustawie jest obowiązkiem wynikającym z regulacji unijnych. Art. 24 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 obliguje państwa członkowskie do podjęcia działań zmierzających do zapewnienia pełnej realizacji praw i obowiązków, które zostały w niej

określone. Jednak jest on wiążący jedynie co do celu, jaki należy osiągnąć. Wybór wiodącej do tego drogi pozostawia zaś poszczególnym państwom członkowskim.

Wydawało się, że przyjęte pierwotnie i obowiązujące dotychczas przepisy o odpowiedzialności karnej za naruszenie zasad określonych w ustawie o ochronie danych osobowych okażą się wystarczające w egzekwowaniu prawa. Niestety, system ten się nie sprawdził. Nie stanowi przesady stwierdzenie, iż przepisy ustawy w obowiązującym brzmieniu nie przyznają Generalnemu Inspektorowi Ochrony Danych Osobowych wystarczająco skutecznych instrumentów, które, po pierwsze, służyłyby egzekwowaniu prawa, po drugie zaś, byłyby gwarantem tego, że administratorzy danych, którzy uporczywie naruszają przepisy ustawy, nie respektując przy tym praw osób, których dane dotyczą, poniosą konsekwencje takich działań.

Ponadto istotnym warunkiem skuteczności ochrony danych osobowych jest również należyte wypełnianie przez administratorów danych swoich obowiązków. Skoro bowiem administrator decyduje o celach i środkach przetwarzania danych, powinien mieć również świadomość ciążącej na nim odpowiedzialności za niezgodne z prawem działanie. Tymczasem brak skutecznego instrumentu w walce z nierzetelnymi administratorami danych powoduje, iż niejednokrotnie lekceważą oni – formułowane przez Generalnego Inspektora w decyzjach administracyjnych – nakazy i zakazy bądź uniemożliwiają podejmowanie działań, do których upoważnia go ustawa, dopuszczając się tym samym świadomego naruszenia przepisów prawa. W wielu przypadkach przyczyną ignorancji jest dodatkowo brak właściwej reakcji organów ścigania rozpatrujących sprawy dotyczące popełnienia przestępstw wymienionych w ustawie o ochronie danych osobowych. Często praktyką jest, iż zawiadomienia o popełnieniu przestępstwa przez podmioty uporczywie uchylające się od swoich obowiązków związanych ze sprawowaniem pieczy nad powierzonymi im danymi osobowymi są umarzane z powodu znikomej społecznej szkodliwości lub braku cech przestępstwa. U osób i firm dopuszczających się naruszenia prawa ochrony danych osobowych umacnia to poczucie bezkarności.

Dlatego w celu zapewnienia **rzeczywistej ochrony danych osobowych** niezbędne jest wyposażenie Generalnego Inspektora w skuteczniejsze niż dotychczas instrumenty umożliwiające wyegzekwowanie od podmiotów naruszających przepisy ustawy o ochronie danych osobowych przestrzegania prawa.

Doświadczenia wielu państw europejskich wskazują, że rozwiązaniem podnoszącym poziom takiej ochrony - także wśród podmiotów, które wcześniej uporczywie działały niezgodnie z obowiązującymi przepisami - jest przyznanie organowi ds. ochrony danych osobowych możliwości nakładania kar pieniężnych.

Warto też zauważyć, że przyznanie Generalnemu Inspektorowi Ochrony Danych Osobowych **prawa występowania do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej**

albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych oraz zobligowanie adresatów takich wniosków do zajęcia stanowiska w ściśle określonym terminie służyć będzie skuteczniejszej realizacji zasad ochrony danych osobowych. Dotychczas GIODO nie miał takich uprawnień, dysponuje nimi natomiast – w sprawach objętych zakresem swojego działania – wiele innych podmiotów, np. Rzecznik Praw Obywatelskich, Rzecznik Praw Dziecka czy Rzecznik Ubezpieczonych.

Z kolei dla upowszechniania wiedzy dotyczącej ochrony danych osobowych istotne znaczenie ma podjęta przez Generalnego Inspektora organizacja systematycznych **szkoleń** dla przedstawicieli kluczowych jednostek administracji publicznej, izb i samorządów zawodowych wszystkich sektorów, a także pracowników wymiaru sprawiedliwości. Działalność ta prowadzona jest zgodnie z potrzebami i oczekiwaniami uczestników. Program zajęć ułożony jest w taki sposób, by zdobywana w czasie ich trwania wiedza była jak najbardziej przydatna w pracy zawodowej. Ważne jest także, aby dzięki szkoleniom dotrzeć do różnych środowisk, nawiązać i umocnić współpracę z nimi, a także, aby przy aktywnym wsparciu organu ds. ochrony danych osobowych, zmotywować i zaktywizować dane środowisko do samodzielnego podejmowania działań w sferze ochrony danych osobowych - tak, jak to miało miejsce w odniesieniu do podmiotów zarządzających rynkiem nieruchomości, z którym Generalny Inspektor podpisał w 2007 r. porozumienie o stałej współpracy na rzecz upowszechniania zasad ochrony danych osobowych. Podobny efekt przyniosła współpraca ze Stowarzyszeniem Marketingu Bezpośredniego, które po szkoleniach GIODO opracowało kodeks dobrych praktyk przetwarzania danych osobowych w tym sektorze. Został on pozytywnie zaopiniowany przez pracowników GIODO.

Dla **edukacji społecznej** niezwykle istotne jest stałe rozszerzanie i umacnianie współpracy Generalnego Inspektora z instytucjami oświatowymi i środowiskami naukowymi. W tym celu podejmowanych jest wiele przedsięwzięć, by przy wykorzystaniu różnych form przekazu, przeniknąć z informacją o prawach i obowiązkach wynikających z ustawy o ochronie danych osobowych do świadomości Polaków oraz polskich instytucji publicznych i prywatnych. GIODO organizuje konferencje, szkolenia, warsztaty, wygłasza referaty w szkołach wyższych, udziela wywiadów, publikuje i odbywa dyżury telefoniczne. Jest też autorem koncepcji promowania prac magisterskich i innych opracowań o tematyce związanej z danymi osobowymi. Planuje rozpocząć II edycję broszur z cyklu ABC ochrony danych osobowych, odnoszących się do takich zagadnień, jak przetwarzanie danych osobowych w sektorze bankowym, medycznym, ubezpieczeniowym, telekomunikacyjnym i marketingowym, a także bezpieczeństwa danych osobowych w sieci.

Tego rodzaju działania Generalnego Inspektora są o tyle ważne, że w świetle dotychczasowych ustaleń, 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 ich udostępnieniem 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 nieumieszczanie w deklaracji opcjonalności jej wyrażenia. Dlatego tak bardzo istotne jest, aby przed podpisaniem dokumentu czy deklaracji bardzo uważnie przeczytać formularz i zastanowić się nad jego treścią.

Edukacji najmłodszych miała służyć I edycja konkursu plastycznego dla uczniów szkół podstawowych pod tytułem „Prywatność wokół mnie”. Celem konkursu plastycznego było zachęcenie uczniów do zainteresowania się problematyką ochrony danych osobowych, podniesienie wśród dzieci świadomości na temat ochrony prywatności oraz zmobilizowanie do twórczego przedstawienia swoich przemyśleń związanych z tą problematyką.

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 Polski w dniu 21 grudnia 2007 r. do systemu Schengen było bardzo ważne ze względu na fakt, iż System ten doprowadził do zniesienia kontroli wobec obywateli polskich na granicach wewnętrznych Unii Europejskiej. Ale z drugiej strony - zadania Generalnego Inspektora Ochrony Danych Osobowych zostały przez to rozszerzone o kontrolę procesu przetwarzania danych osobowych przy użyciu Krajowego Systemu Informatycznego, służącego do przekazywania oraz dostępu do danych gromadzonych w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej.

Kolejnym ważnym zadaniem stojącym przed Generalnym Inspektorem będzie zorganizowanie w Polsce, w 2008 roku, X Spotkania Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej. Decyzję o powierzeniu organizacji tego jubileuszowego spotkania polskiemu organowi do spraw ochrony danych należy traktować jako wyraz uznania dla jego pozycji i roli na tym forum.

Trzeba zaznaczyć, że coroczne Spotkania Rzeczników Ochrony Danych Osobowych z Europy Środkowo-Wschodniej zainicjowane zostały w 2001 roku przez polskiego Generalnego Inspektora

Ochrony Danych Osobowych.²⁷⁰ 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 między rzecznikami ochrony danych osobowych w tym regionie.

Podsumowując, w 2007 r. Generalny Inspektor Ochrony Danych Osobowych podjął wiele działań zmierzających do stworzenia **kompleksowego systemu edukacyjno-szkoleniowego**. Obejmowały one zarówno kontynuację dotychczasowych szkoleń różnych podmiotów, jak i nowe przedsięwzięcia w związku z wyzwaniem społeczeństwa informacyjnego, stojącego wobec problemu nowych technologii. Na to zagadnienie zwróciła także uwagę Grupa Robocza Art. 29²⁷¹ w swoim „Programie prac na lata 2008-2009”. Wśród najpilniejszych zadań, jakie Grupa Robocza Art. 29 przewidziała na nadchodzący rok, były następujące kwestie:

- wpływu nowych technologii na ochronę prywatności i danych osobowych,
- zapewnienia ochrony danych przy przekazywaniu ich do państw trzecich,
- skuteczniejsze wdrażanie 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.

Co ciekawe, intencją regulacji przewidzianych powyższą dyrektywą miało być zabezpieczenie jednolitego 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.

Waga ochrony danych osobowych wzrasta z rozwojem nowych technologii, handlu elektronicznego oraz postępującej informatyzacji instytucji prywatnych i publicznych. Zauważalna jest tendencja do poszerzania zakresu gromadzonych danych osobowych przez różne podmioty, tworzenie coraz to nowych baz danych i ich łączenie, zapewnianie dostępu do nich coraz liczniejszym grupom

²⁷⁰ Więcej o współpracy rzeczników ochrony danych z państw Europy Środkowej i Wschodniej zob. na stronie internetowej: <http://www.ceecprivacy.org>

²⁷¹ Grupa Robocza Art. 29 powołana została na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych osobowych i prywatności. Zadania grupy określa art. 30 wspomnianej dyrektywy: a) badanie wszelkich kwestii dotyczących stosowania krajowych środków przyjętych na mocy dyrektywy 95/46/WE, tak, aby przyczyniać się do jednolitego stosowania tych środków, b) przekazywanie Komisji opinii na temat stopnia ochrony we Wspólnocie i państwach trzecich, c) doradzanie Komisji w sprawie wszelkich proponowanych zmian tejże dyrektywy, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych środków wspólnotowych dotyczących tych praw i wolności, d) wydawanie opinii na temat kodeksów postępowania opracowywanych na poziomie wspólnotowym. Zadania te mają zastosowanie także w odniesieniu do sektora łączności elektronicznej (art. 15 ust. 3 dyrektywy 2002/58/WE).

osób, a także coraz powszechniejsze świadczenie usług drogą elektroniczną. Z jednej strony można przyjąć, że służy to wygodzie obywatela, który dzięki temu może oczekiwać kompleksowej i szybkiej obsługi (e-administracja). Ale z drugiej, stwarza ryzyko nadużyć, a w konsekwencji zagraża elementarnemu prawu jednostki, która oczekuje od Państwa ochrony swej prywatności i danych osobowych.

I chociaż rozwoju cywilizacji nie da się zahamować, to poprzez wypracowanie pewnych standardów i mechanizmów kontroli nad tym procesem, można wyeliminować lub przynajmniej zminimalizować jego niepożądane skutki. I przed takim właśnie zadaniem na rok 2008, stanął Generalny Inspektor Ochrony Danych Osobowych. Zapewnienie skutecznej ochrony danych w kontekście nowych technologii, zwłaszcza związanych z Internetem, łącznością elektroniczną, e-administracją, biometrią czy zarządzaniem tożsamością – to obecnie bardzo poważne wyzwania dla polskiego organu ds. ochrony danych osobowych. Wyzwania, które wymaga szeregu – nierzadko długofalowych – przedsięwzięć i związanych z ich realizacją nakładów finansowych. Ważne jest bowiem, aby nowe technologie służyły, a nie szkodziły człowiekowi i społeczeństwu.

Tymczasem od wielu lat w budżecie Biura GIODO nie były zagwarantowane środki na działalność edukacyjną, która jest priorytetem wśród licznych innych zadań. Dlatego Generalny Inspektor musi teraz bardzo aktywnie poszukiwać dodatkowych środków na ten cel. Korzysta więc z funduszy unijnych, i to zarówno w kwestii finansowania, np. szkoleń pracowników Biura GIODO, na które są przewidziane pewne środki w budżecie Biura (projekt wymiany pracowników w ramach Programu Leonardo da Vinci), jak i pozyskuje fundusze unijne w celu edukacji społeczeństwa w ramach programu „Ochrona danych osobowych – moje prawa, moje zadania”, którego bezpośrednim rezultatem będzie uruchomienie interaktywnej strony internetowej (tzw. platforma e-learningowa). Korzysta więc z każdej możliwości zwiększenia budżetu na realizację swoich zadań w sferze edukacji społecznej.

Niemniej dla pełnej realizacji działań w tym zakresie najwłaściwsze byłoby zagwarantowanie niezbędnych środków w budżecie Generalnego Inspektora.

ZAŁĄCZNIKI:

Załącznik nr 1 Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2007 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego.

I.p.	Podmiot, do którego skierowano wystąpienie	Data wystąpienia i sygnatura sprawy	Przedmiot wystąpienia
1.	Minister Finansów	10.01.2007 r. GI-DOLiS-024/57/07	Wystąpienie o dokonanie wykładni przepisu art. 299b ustawy Ordynacja podatkowa, dotyczącego przesłanek ujawnienia informacji stanowiących tajemnicę skarbową.
2.	Minister Pracy i Polityki Społecznej	30.01.2007 r. GI-DOLiS-024/37/07	Wniosek o podjęcie działań legislacyjnych w celu zmiany załącznika nr 1 do rozporządzenia Ministra Gospodarki i Pracy z dnia 26 listopada 2004 r. w sprawie rejestracji bezrobotnych i poszukujących pracy i dostosowanie treści zawartego w nim „Wzoru karty rejestracyjnej bezrobotnego” do przepisów ustawy o ochronie danych osobowych.
3.	Minister Zdrowia	8.02.2007 r. GI-DIS-K-411/39/06	Rozważenie możliwości podjęcia działań w celu uregulowania w przepisach prawa trybu przekazywania ze szkół danych osobowych uczniów do zakładów opieki zdrowotnej w celu sprawowania profilaktycznej opieki zdrowotnej.
4.	Wiceprezes Rady Ministrów	14.02.2007 r. GI-DOLiS-023/18/07	Wniosek o zwrócenie szczególnej uwagi na konieczność przestrzegania przepisów ustawy o ochronie danych osobowych w procesie tworzenia i stosowania prawa.
5.	Burmistrz Miasta Brodnicy	16.04.2007 r. Gi-DOLiS-430/21/06	Wystąpienie dotyczące podjęcia niezbędnych działań mających na celu zapewnienie zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa.
6.	Wójt Gminy Czarna Dąbrówka	14.03.2007 r. GI-DOLiS-24/83/07	Wystąpienie o dostosowanie procesu przetwarzania danych osobowych w trakcie postępowań administracyjnych do wymogów ustawy o ochronie danych osobowych.
7.	Minister Spraw Wewnętrznych i Administracji	12.04.2007 r. GI-DP-024/1037/06/2218/07	Wystąpienie o podjęcie prac legislacyjnych mających na celu stworzenie podstaw prawnych funkcjonowania Integrującej Platformy Elektronicznej, służącej przetwarzaniu danych osobowych przez organy administracji właściwe w sprawach geodezji i kartografii.
8.	Minister Spraw Zagranicznych	30.04.2007 r. GI-DOLiS-024/484/07	Wystąpienie o podjęcie działań legislacyjnych w celu zmiany załączników 1, 2 i 3 do rozporządzenia Ministra Spraw Zagranicznych z dnia 28 sierpnia 2002 r. w sprawie udzielania przez konsula Rzeczypospolitej Polskiej pomocy finansowej oraz trybu postępowania przy jej udzielaniu, w celu ich dostosowania do przepisów ustawy o ochronie danych osobowych.
9.	Minister Rozwoju Regionalnego	25.05.2007 r. GI-GOLiS-024/565/07	Wystąpienie o podjęcie prac dostosowujących tryb przyznawania stypendiów dla uczniów pochodzących z rodzin znajdujących się w trudnej sytuacji materialnej,

			uczniów z obszarów wiejskich i uczniów z małych miast oraz studentów z obszarów marginalizowanych (w szczególności wiejskich i restrukturyzacji przemysłu) i znajdujących się w trudnej sytuacji materialnej, do przepisów ustawy o ochronie danych osobowych.
10.	Komornik Sądowy Rewiru II przy Sądzie Rejonowym w Mikołowie	5.06.2007 r. GI-DOLiS-430/142/07	Wniosek o zaprzestanie praktyki umieszczania w obwieszczeniach o licytacji nieruchomości – ogłaszanych w poczytnych gazetach – danych osobowych dłużników w zakresie ich imion i nazwisk.
11.	Wojewoda Warmińsko – Mazurski	20.06.2007 r. GI-DOLiS-430/32/06	Wniosek o podjęcie niezbędnych działań dyscyplinujących wobec Wójta Gminy Świątki mających na celu zapewnienie zgodności przetwarzania danych osobowych mieszkańców gminy Świątki z przepisami ustawy o ochronie danych osobowych.
12.	Główny Inspektor Farmaceutyczny	26.06.2007 r. GI-DIS-K-411/59/07 GI-DIS-K-411/65/07 GI-DIS-K-411/68/07 GI-DIS-K-411/69/07 GI-DIS-K-411/74/07	Wyrażenie opinii, czy na gruncie przepisów ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne dopuszczalne jest zawieranie przez apteki umów z DOZ S.A. z siedzibą w Łodzi, których przedmiotem jest uczestniczenie w programie marketingowym o nazwie „Dbam o zdrowie”.
13.	Minister Rozwoju Regionalnego	9.07.2007 r. GI-DOLiS-024/731/07	Wniosek o podjęcie działań legislacyjnych mających na celu uregulowanie warunku niekaralności za przestępstwo umyślne lub przestępstwo skarbowe, który powinien spełniać kandydat na eksperta powoływanego w celu oceny projektów realizowanych w ramach programów operacyjnych, w ustawie z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. Nr 227, poz. 1658).
14.	Minister Spraw Wewnętrznych i Administracji	3.08.2007 r. GI-DOLiS-024/704/07	Wystąpienie o rozważenie możliwości podjęcia prac zmierzających do zmiany art. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.) w celu zapewnienia należytego poziomu ochrony danych wrażliwych świadków i pokrzywdzonych uczestniczącym w postępowaniu karnym.
15.	Minister Sprawiedliwości	27.08.2007 r. GI-DOLiS-430/487/07	Wystąpienie o przeprowadzenie czynności wyjaśniających w sprawie nieprawidłowości w procesie przetwarzania danych osobowych byłych pracowników Huty Szkła „Julia”.
16.	Prezes Krajowej Rady Komorników	27.08.2007 r. GI-DOLiS-024/666/07	Wystąpienie o dokonanie oceny praktyk kancelarii komorniczych polegających na wysyłaniu do pracodawców zajęć wynagrodzenia za pracę dłużników bez wstępnego sprawdzenia, czy dana osoba jest rzeczywiście zatrudniona u tego pracodawcy.
17.	Burmistrz Miasta Milanówka	29.08.2007 r. GI-DOLiS-024/742/07	Wystąpienie o zaprzestanie praktyki przez organy gminy w sporządzanych i przesyłanych właściwym osobom pismach, pełnego wykazu imion, nazwisk i adresów zamieszkania innych osób, do wiadomości których pisma te zostały przekazane.
18.	Komendant Komendy Miejskiej Policji w Toruniu	13.09.2007 r. GI-DOLiS-024/993/07	Poinformowanie, iż umieszczanie numerów IP komputerów na stronie internetowej Komendy Miejskiej Policji w Toruniu, za pomocą których użytkownicy sieci umieszczali swoje posty, bez ich zgody jest niezgodne z ustawą o ochronie danych osobowych.
19.	Zastępca Szefa Kancelarii	20.09.2007 r. GI-DOLiS-024/991/07	Wystąpienie o zbadanie prawidłowości regulacji zawartej w art. 81 ust. 3 ustawy z dnia 15 grudnia 2000 r. o

	Prezydenta RP		spółdzielniach mieszkaniowych (Dz. U. z 2003 r. Nr 119, poz. 1116 z późn. zm.).
20.	Minister Sprawiedliwości	10.10.2007 r. GI-DS-430/768/04	Wystąpienie w celu zasygnalizowania nieprawidłowości w prowadzeniu przez prokuraturę postępowań zawiadomień złożonych przez Generalnego Inspektora Ochrony Danych Osobowych.
21.	Minister Edukacji Narodowej	31.10.2007 r. DOLiS-035-93/07	Wystąpienie z uwagą, iż instalowanie na terenie szkół i placówek oświatowych urządzeń umożliwiających rejestrowanie rozmów budzi zasadnicze wątpliwości co do zgodności z Konstytucją RP.
22.	Przewodniczący Komisji Infrastruktury i Inwestycji Rady m.st. Warszawy	31.10.2007 r. DOLiS-035-94/07	Wystąpienie z informacją, iż planowane przez Zakład Transportu Miejskiego w Warszawie wprowadzenie nowych kart miejskich uprawniających do określonego rodzaju przejazdu, na których zamieszczana będzie – poza innymi – także informacja o numerze PESEL poszczególnych podróżnych budzi wątpliwości pod kątem zgodności z ustawą o ochronie danych osobowych.
23.	Rektor Akademii Medycznej w Gdańsku	5.11.2007 r. GI-DOLiS-430/15/06	Wystąpienie o usunięcie uchybień w procesie przetwarzania danych osobowych poprzez wprowadzenie zasady dopuszczenia do przetwarzania danych wyłącznie przez osoby legitymujące się stosownym upoważnieniem, o którym mowa w art. 37 ustawy o ochronie danych osobowych.
24.	Wojewoda Wielkopolski	15.11.2007 r. GI-DOLiS-024/990/07	Wystąpienie o podjęcie niezbędnych działań mających na celu zapewnienie właściwej ochrony danych osobowych zawartych w dokumentacji urzędowej.
25.	Minister Sprawiedliwości	22.11.2007 r. GI-DS-430/552/05	Zasygnalizowanie nieprawidłowości w prowadzeniu przez prokuraturę postępowania przygotowawczego.
26.	Minister Spraw Wewnętrznych i Administracji	23.11.2007 r. GI-DOLiS-430/103/07	Wystąpienie o zaprzestanie przetwarzania danych osobowych kandydatów związanych ze środowiskami mniejszości narodowych, etnicznych oraz mniejszości posługujących się językiem regionalnym, ubiegających się o mandaty z list komitetów wyborczych niezarejestrowanych przez organizacje mniejszości narodowych i etnicznych w wyborach samorządowych.

Załącznik nr 2 Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2007 do podmiotów prywatnych.

I.p.	Podmiot, do którego skierowano wystąpienie	Data wystąpienia i sygnatura sprawy	Przedmiot wystąpienia
1.	Atlanta Company Sp. z o.o.	12.02.2007 r. GI-DS-430/529/06	Wystąpienie dotyczące zaprzestania praktyki ujawniania danych osobowych wraz z wysokością zadłużenia w miejscach powszechnie dostępnych.
2.	Bank Ochrony Środowiska S.A.	16.02.2007 r. GI-DP-024/1976/06	Wystąpienie o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych osobowych osób zainteresowanych uzyskaniem informacji dotyczącej działalności banku za pośrednictwem zamieszczonego na stronie internetowej banku formularza do wymogów z ustawy o ochronie danych osobowych.
3.	Spółka Wodna "Boży Stok"	28.02.2007 r. GI-DOLiS-430/5/07	Wystąpienie dotyczące realizacji obowiązku rejestracji zbioru danych osobowych, o którym mowa w art. 40 ustawy o ochronie danych osobowych.
4.	Polkomtel S.A.	5.03.2007 r. GI-DOLiS-024/275/07	Wystąpienie o podjęcie działań mających na celu zapobieżenie w przyszłości przypadkom odmowy udostępnienia służbom ustawowo upoważnionym do niesienia pomocy danych lokalizacyjnych abonentów wywołujących połączenia z numerami alarmowymi z powołaniem się na przepisy ustawy o ochronie danych osobowych.
5.	Polska Telefonia Komórkowa Sp. z o.o.	5.03.2007 r. GI-DOLiS-024/275/07	Wystąpienie o podjęcie działań mających na celu zapobieżenie w przyszłości przypadkom odmowy udostępnienia służbom ustawowo upoważnionym do niesienia pomocy danych lokalizacyjnych abonentów wywołujących połączenia z numerami alarmowymi z powołaniem się na przepisy ustawy o ochronie danych osobowych.
6.	Redaktor Naczelny „Gazety Wyborczej”	7.03.2007 r. GI-DOLiS-430/140/07/1454	Wystąpienie o podjęcie działań mających na celu zapobieżenie sytuacjom publikowania w materiałach prasowych danych osobowych z naruszeniem przepisów ustawy Prawo prasowe.
7.	Zarząd Wspólnoty Mieszkaniowej „WIT – KOL”	12.03.2007 r. GI-DOLiS-430/88/06/1554/07	Wystąpienie dotyczące zaprzestania praktyki ujawniania danych osobowych w treści ogłoszeń ujawnianych na tablicach ogłoszeń w budynkach należących do Wspólnoty Mieszkaniowej.
8.	Syigma Bank Polska S.A.	14.03.2007 r. GI-DP-024/317/07	Wystąpienie o zmianę treści klauzul zgody na przetwarzanie danych osobowych umieszczonych we wniosku o kredyt odnawialny.
9.	Syndyk masy upadłości Spółdzielni Mieszkaniowej „Natalia” w Grudziądzu	22.03.2007 r. GI-DOLiS-430/43/06	Wystąpienie dotyczące zaprzestania praktyki ujawniania danych osobowych poprzez umieszczanie w miejscu powszechnie dostępnym informacji o zamiarze zgłoszenia zawiadomienia przestępstwa przez konkretną osobę oraz niezastosowania wystarczających środków, aby zapewnić ochronę przetwarzanych danych.
10.	Zarząd Wspólnoty Mieszkaniowej „Poduszkowiec” w Pruszkowie	17.04.2007 r. GI-DOLiS-430/40/07	Wystąpienie dotyczące zaprzestania praktyki ujawniania danych osobowych członków Wspólnoty w miejscach powszechnie dostępnych.
11.	Neckermann Polska Biuro Podróży Sp. z o.o.	8.05.2007 r. GI-DOLiS-430/6/07	Wystąpienie dotyczące zmiany treści formularzy stosowanych przez Spółkę oraz „warunków umów o świadczenie usług turystycznych i warunki płatności Neckermann Polska Biuro Podróży Sp. z o.o.” na zgodne z przepisami ustawy o ochronie danych osobowych.
12.	Arcybiskup Kazimierz Nycz Metropolita Warszawski	29.05.2007 r. GI-DOLiS-024/609/07	Opinia w sprawie przetwarzania danych osobowych przez Kościół Katolicki.

13.	Regionalne Wodociągi i Kanalizacja Sp. z o.o. w Ustroniu Miejskim	6.06.2007 r. GI-DOLiS-430/28/06	Wystąpienie o zaprzestanie stosowania praktyki umieszczania na kopertach pism (faktur) w sposób powodujący udostępnienie danych osobowych nabywcy usług świadczonych przez Spółkę osobom nieupoważnionym.
14.	J. Zając, H. Wawrzyńczyk A&J Partners s.c.	5.07.2007 r. GI-DOLiS-430/89/06	Wystąpienie o zaprzestanie praktyki udostępniania MOPS danych osobowych bez podstawy prawnej.
15.	IMP Sp. z o.o.	13.07.2007 r. GI-DOLiS-430/137/07	Wystąpienie o zmianę formuły zgody na przetwarzanie danych osobowych.
16.	Spółdzielnia Mieszkaniowa „Mokotów” w Warszawie	27.08.2007 r. GI-DOLiS-430/318/07	Wystąpienie o zaprzestanie praktyki gromadzenia danych osobowych członków Spółdzielni dla potrzeb ewentualnego postępowania egzekucyjnego.
17.	Telekomunikacja Polska S.A.	16.10.2007 r. GI-DOLiS-430/514/07	Wystąpienie o podjęcie działań mających na celu zabezpieczenie przetwarzanych przez Spółkę danych.
18.	Przedsiębiorstwo Gospodarki Komunalnej Sp. z o.o.	7.11.2007 r. GI-DOLiS-430/412/07	Wystąpienie o zaprzestanie przechowywania przez Przedsiębiorstwo aktów notarialnych.

Załącznik nr 3 Wykaz kontroli przeprowadzonych w 2007 r.

L. p.	Data i sygnatura kontroli	Podmiot kontrolowany i miejsce kontroli	Inicjatywa kontroli	Rozstrzygnięcie oraz/lub data i sygnatura decyzji
1.	8-10.01.2007 r. GI-DIS-K-411/1/07	Wittchen Sp. z o. o. Z siedzibą w Łomiankach k/Warszawy – Kiełpin, ul. Ogrodowa 27/29	Departament Orzecznictwa, Legislacji i Skarg	24.05.2007 r. decyzja GI-DEC-DIS-19/07
2.	8-10.01.2007 r. GI-DIS-K-411/2/07	AIG Towarzystwo Funduszy Inwestycyjnych S.A. z siedzibą w Warszawie, ul. Przemysłowa 26	z urzędu	usunięto uchybienia
3.	8-10.01.2007 r. GI-DIS-K-411/3/07	Commercial Union Polska Towarzystwo Funduszy S.A. z siedzibą w Warszawie, ul. Prosta 70	z urzędu	nie stwierdzono uchybień
4.	8-10.01.2007 r. GI-DIS-K-411/4/07	Millennium Towarzystwo Funduszy Inwestycyjnych S.A. z siedzibą w Warszawie, Al.. Jerozolimskie 123 A	z urzędu	nie stwierdzono uchybień
5.	11-15.01.2007 r. GI-DIS-K-411/5/07	Obsługa Funduszy Inwestycyjnych Sp. z o.o. z siedzibą w Warszawie, ul. Cybernetyki 21	w związku z kontrolą GI-DIS-K-411/3/07	nie stwierdzono uchybień
6.	10-16.01.2007 r. GI-DIS-K-411/6/07	Proservice Agent Transferowy Sp. z o.o. z siedzibą w Warszawie, ul. Puławska 436	w związku z kontrolą GI-DIS-K-411/2/07	15.05.2007 r. decyzja GI-DEC-DIS-17/07
7.	10-12 i 15.01.2007 r. GI-DIS-K-411/7/07	Bank Millennium S.A. z siedzibą w Warszawie, Al.. Jerozolimskie 123 A	w związku z kontrolą GI-DIS-K-411/4/07	nie stwierdzono uchybień
8.	12.01.2007 r. GI-DIS-K-411/8/07	Osiedle Kampinos Sp. z o.o. z siedzibą w Warszawie, ul. Marszałkowska 111	Departament Orzecznictwa Legislacji i Skarg	sprawa przekazana do Departamentu Orzecznictwa Legislacji i Skarg
9.	15-19.01.2007 r. GI-DIS-K-411/9/07	Towarzystwo Funduszy Inwestycyjnych Allianz Polska S. A. z siedzibą w Warszawie, ul. Rodziny Hiszpańskich 1	z urzędu	16.01.2008 r. decyzja DIS/DEC-20/1061/08 decyzja DIS/DEC-21/1065/08 decyzja DIS/DEC-22/1067/08 decyzja DIS/DEC-23/1068/08 decyzja DIS/DEC-24/1069/08 decyzja DIS/DEC-25/1070/08
10.	15-16.01.2007 r. GI-DIS-K-411/10/07	Opera Towarzystwo Funduszy Inwestycyjnych S.A. z siedzibą w Warszawie, Rondo ONZ 1	z urzędu	29.06.2007 r. decyzja GI-DEC-DIS-30/07 decyzja GI-DEC-DIS-31/07
11.	22-26.01.2007 r. GI-DIS-K-411/11/07	Urząd Skarbowy w Braniewie z siedzibą w Braniewie, ul. Jana Matejki 6	z urzędu	nie stwierdzono uchybień
12.	29.01-2.02.2007 r. GI-DIS-K-411/12/07	Schenker Sp. z o.o. z siedzibą w Warszawie,	Departament Orzecznictwa	30.08.2007 r. decyzja GI-DEC-DIS-69/07

		ul. Ordona 2 A	Legislacji i Skarg	
13.	29-30.01.2007 r. GI-DIS-K-411/13/07	Legg Mason Towarzystwo Funduszy Inwestycyjnych S.A. z siedzibą w Warszawie, Pl. Piłsudskiego 2	z urzędu	usunięto uchybienia
14.	29.01-2.02.2007 r. GI-DIS-K-411/14/07	BRE Bank S.A. z siedzibą w Warszawie ul. Senatorska 18 miejsce kontroli – mBank Wydział Bankowości Detalicznej w Łodzi, Al. Piłsudskiego 3	z urzędu	nie stwierdzono uchybień
15.	5-8.02.2007 r. GI-DIS-K-411/15/07	ING Towarzystwo Funduszy Inwestycyjnych S.A. z siedzibą w Warszawie, Pl. Trzech Krzyży 10/14	z urzędu	29.05.2007 r. decyzja GI-DEC-DIS-22/07
16.	7-9.02.2007 r. GI-DIS-K-411/16/07	Copernicus Capital Towarzystwo Funduszy Inwestycyjnych S.A. z siedzibą w Warszawie, ul. Królewska 16	z urzędu	10.07.2007 r. decyzja GI-DEC-DIS-43/07 decyzja GI-DEC-DIS-44/07 decyzja GI-DEC-DIS-45/07
17.	6-9.02.2007 r. GI-DIS-K-411/17/07	Towarzystwo Funduszy Inwestycyjnych PZU S.A. z siedzibą w Warszawie, Al. Jana Pawła II 24	z urzędu	10.07.2007 r. decyzja GI-DEC-DIS-32/07 decyzja GI-DEC-DIS-33/07 decyzja GI-DEC-DIS-34/07 decyzja GI-DEC-DIS-35/07 decyzja GI-DEC-DIS-36/07 decyzja GI-DEC-DIS-37/07 decyzja GI-DEC-DIS-38/07 decyzja GI-DEC-DIS-39/07 decyzja GI-DEC-DIS-40/07
18.	7-8.02.2007 r. GI-DIS-K-411/18/07	Intrum Justitia Towarzystwo Funduszy Inwestycyjnych S.A. z siedzibą w Warszawie, ul. Domaniewska 41	z urzędu	nie stwierdzono uchybień
19.	12-16.02.2007 r. GI-DIS-K-411/20/07	Kredyt Bank S.A. z siedzibą w Warszawie, ul. Kasprzaka 2/8	z urzędu	usunięto uchybienia
20.	12-16.02.2007 r. GI-DIS-K-411/21/07	Centrum Informtyki Grupy PZU S.A. z siedzibą w Warszawie, ul. Matuszewskiej 14	z urzędu	usunięto uchybienia
21.	12-16.02.2007 r. GI-DIS-K-411/22/07	IPSOS Polska Sp. z o.o. z siedzibą w Warszawie, ul. Puławska 39	Departament Orzecznictwa Legislacji i Skarg	18.01.2008 r. decyzja DIS/DEC-29/1175/08
22.	8-9.02.2007 r. GI-DIS-K-411/23/07	Intrum Justitia Sp. z o.o. z siedzibą w Warszawie, ul. Domaniewska 41	z urzędu	nie stwierdzono uchybień
23.	19-23.02.2007 r. GI-DIS-K-411/24/07	Komisja Nadzoru Finansowego z siedzibą w Warszawie, Pl. Powstańców Warszawy 1	Departament Rejestracji Zbiorów Danych Osobowych	17.08.2007 r. decyzja GI-DEC-DIS-65/07
24.	19-20.02.2007 r. GI-DIS-K-411/25/07	Dachlux sc 1 Spółka jawna Łysoniewski, K. Jedynak z siedzibą w Warszawie – Falenicy ul. Tyszowiecka 8	z urzędu	13.07.2007 r. decyzja GI-DEC-DIS-46/07
25.	26.02-01.03.2007 r. GI-DIS-K-411/26/07	Bankowy Ośrodek Doradztwa i Edukacji Sp. z o.o. z siedzibą	Departament Orzecznictwa, Legislacji i Skarg	23.11.2007 r. decyzja DIS-DEC-121/07

		w Poznaniu, ul. Norwida 14		
26.	26.02-2.03.2007 r. GI-DIS-K-411/27/07	Pekao Financial Services Sp. z o.o. z siedzibą w Warszawie, ul. Marynarska 19 A	z urzędu	30.08.2007 r. decyzja GI-DEC-DIS-70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97/07
27.	26.02-2.03.2007 r. GI-DIS-K-411/28/07	Cetelem Bank S.A. z siedzibą w Warszawie, ul. Kijowska 1	z urzędu	nie stwierdzono uchybień
28.	26-28.02.2007 r. GI-DIS-K-411/29/07	Towarzystwo Ubezpieczeń i Reasekuracji Warta S.A. z siedzibą w Warszawie, ul. Chmielna 85/87	Prokuratura Rejonowa Warszawa Mokotów	1.06.2007 r. decyzja GI-DEC-DIS-23/07
29.	5-9.03.2007 r. GI-DIS-K-411/30/07	Grupa Finansowo – Inwestycyjna Sp. z o.o. z siedzibą w Legnicy, ul. Rataja 14/1 Miejsce wykonywania działalności: Legnica, ul. Rzeczypospolitej 116	z urzędu	nie przetwarza danych osobowych
30.	5-9.03.2007 r. GI-DIS-K-411/31/07	Jerzy Eigner prowadzący działalność gospodarczą pod nazwą „Polisa Jerzy Eigner” z siedzibą w Legnicy, ul. Piastowska 20 A Miejsce wykonywania działalności: Legnica, ul. Rzeczypospolitej 116	KGP w Oświęcimiu	20.07.2007 r. decyzja GI-DEC-DIS-48/07
31.	5-9.03.2007 r. GI-DIS-K-411/32/07	Gmina Aleksandrów Kujawski – Urząd Miasta w Aleksandrowie Kujawskim z siedzibą w Aleksandrowie Kujawskim, ul. Słowackiego 8	z urzędu	26.06.2007 r. decyzja GI-DEC-DIS-25/07
32.	12-16.03.2007 r. GI-DIS-K-411/33/07	Gmina Legionowo – Urząd Miasta Legionowo z siedzibą w Legionowie, ul. J. Piłsudskiego 3.	z urzędu	28.05.2007 r. decyzja GI-DEC-DIS-20/07
33.	12-16.03.2007 r. GI-DIS-K-411/34/07	Powiat Bielski – Starostwo Powiatowe w Bielsku Podlaskim z siedzibą w Bielsku Podlaskim ul. Mickiewicza 46	z urzędu	25.07.2007 r. decyzja GI-DEC-DIS-51/07
34.	12-16.03.2007 r. GI-DIS-K-411/35/07	Gmina Bielsk Podlaski – Urząd Miasta w Bielsku Podlaskim z siedzibą w Bielsku Podlaskim, ul. Kopernika 1.	z urzędu	28.08.2007 r. decyzja GI-DEC-DIS-68/07
35.	12-16.03.2007 r. GI-DIS-K-411/36/07	Powiat Aleksandrowski – Starostwo Powiatowe w Aleksandrowie Kujawskim z siedzibą w Aleksandrowie Kujawskim, ul. Słowackiego 8.	z urzędu	10.07.2007 r. decyzja GI-DEC-DIS-41/07
36.	19-21.03.2007 r. GI-DIS-K-411/37/07	Syigma Banque Societe Anonyme Oddział w Polsce z siedzibą w Warszawie, Al. Jerozolimskie 92	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
37.	19-22.03.2007 r. GI-DIS-K-411/38/07	IPSOS Observer Sp. z o.o. z siedzibą w Warszawie, ul. Puławska 39/4	z urzędu	15.01.2008 r. decyzja DIS-DEC-15/895/08
38.	21-23.03.2007 r.	Fundacja „KAMELOT”	z urzędu	nie stwierdzono uchybień

	GI-DIS-K-411/39/07	z siedzibą w Łodzi, ul. Jaracza 41 lok. 38		
39.	21.03.2007 r. GI-DIS-K-411/40/07	Polkomtel S.A. z siedzibą w Warszawie, ul. Postępu 3	Departament Orzecznictwa, Legislacji i Skarg	26.09.2007 r. decyzja GI-DEC-DIS-105/07
40.	26-30.03.2007 r. GI-DIS-K-411/41/07	Gmina Gliwice – Urząd Miejski w Gliwicach z siedzibą w Gliwicach, ul. Zwycięstwa 21	z urzędu	24.07.2007 r. decyzja GI-DEC-DIS-50/07
41.	26-28.03.2007 r. GI-DIS-K-411/42/07	Żagiel S.A. z siedzibą w Lublinie, ul. Tomasza Zana 39 A	z urzędu	
42.	26-30.03.2007 r. GI-DIS-K-411/43/07	Euro Providus S.A. z siedzibą we Wrocławiu, ul. Oławskiej 17 Miejsce kontroli – Oddział Euro Providus S.A. w Częstochowie, ul. Dąbrowskiego 7	z urzędu	25.07.2007 r. decyzja GI-DEC-DIS-53/07
43.	2-6.04.2007 r. GI-DIS-K-411/44/07	Powiat Puławski – Starostwo Powiatowe w Puławach z siedzibą w Puławach, Al. Królewska 19	z urzędu	1.08.2007 r. decyzja GI-DEC-DIS-55/07
44.	2-6.04.2007 r. GI-DIS-K-411/45/07	Gmina Miasta Puławy – Urząd Miasta w Puławach z siedzibą w Puławach, ul. Lubelska 5	z urzędu	8.08.2007 r. decyzja GI-DEC-DIS-60/07
45.	2-6.04.2007 r. GI-DIS-K-411/46/07	Powiat Legionowski – Starostwo Powiatowe w Legionowie z siedzibą w Legionowie, ul. Sikorskiego 11	z urzędu	13.08.2007 r. decyzja GI-DEC-DIS-62/07
46.	10-13.04.2007 r. GI-DIS-K-411/47/07	Polska Agencja Rozwoju Przedsiębiorczości z siedzibą w Warszawie, ul. Pańska 81/83	Departament Orzecznictwa, Legislacji i Skarg	30.11.2007 r. decyzja DIS-DEC-125/421/07
47.	16-20.04.2007 r. GI-DIS-K-411/48/07	Województwo Kujawsko – Pomorskie – Urząd Marszałkowski Województwa Kujawsko – Pomorskiego z siedzibą w Toruniu, Pl. Teatralny 2	z urzędu	10.07.2007 r. decyzja GI-DEC-DIS-42/07
48.	16-20.04.2007 r. GI-DIS-K-411/49/07	Gmina Iława – Urząd Gminy w Iławie z siedzibą w Iławie, ul. Gen. Andersa 2 A	z urzędu	26.06.2007 r. decyzja GI-DEC-DIS-26/07
49.	16-20.04.2007 r. GI-DIS-K-411/50/07	Starostwo Powiatowe w Gliwicach z siedzibą w Gliwicach, ul. Zygmunta Starego 17	z urzędu	13.07.2007 r. decyzja GI-DEC-DIS-47/07
50.	16-20.04.2007 r. GI-DIS-K-411/51/07	Powiat Iławski – Starostwo Powiatowe w Iławie z siedzibą w Iławie, ul. Andersa 2 A	z urzędu	8.08.2007 r. decyzja GI-DEC-DIS-61/07
51.	16-20.04.2007 r. GI-DIS-K-411/52/07	Powiat Legionowski – Starostwo Powiatowe w Legionowie z siedzibą w Legionowie, ul. Sikorskiego 11	z urzędu	13.08.2007 r. decyzja GI-DEC-DIS-62/07
52.	23-27.04.2007 r. GI-DIS-K-411/53/07	Niepubliczny Zakład Opieki Zdrowotnej „Remedium” s.c. J. Cynkier, A. Cynkier z siedzibą w Rawie	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień

		Mazowieckiej, ul. Konstytucji 3 Maja 9 B		
53.	23-27.04.2007 r. GI-DIS-K-411/54/07	Gmina Urszulin – Urząd Gminy Urszulin z siedzibą w Urszulinie, ul. Kwiatowa 35	Departament Orzecznictwa, Legislacji i Skarg	27.06.2007 decyzja GI-DEC-DIS-29/07
54.	23-27.04.2007 r. GI-DIS-K-411/55/07	Klaudia Maria Rosadzińska prowadząca działalność gospodarczą pod firmą „Pollana” z siedzibą w Sierosławiu, ul. Kręta 1 A	Departament Orzecznictwa, Legislacji i Skarg	2007-08-30, decyzja GI-DEC-DIS-67/07
55.	25.04.2007 r. GI-DIS-K-411/56/07	Sofralux Sp. z o.o. z siedzibą w Warszawie, ul. Czeska 5	z urzędu	27.06.2007 r. decyzja GI-DEC-DIS-27/07
56.	24-25.04.2007 r. GI-DIS-K-411/57/07	Gabriela Magnon – Jabłońska prowadząca działalność gospodarczą pod nazwą „Diparlux” z siedzibą w Warszawie, ul. Czeska 5	z urzędu	27.06.2007 r. decyzja GI-DEC-DIS-28/07
57.	7-11.05.2007 r. GI-DIS-K-411/58/07	Gmina Miejska Starogard Gdański – Urząd Miejski w Starogardzie Gdańskim z siedzibą w Starogardzie Gdańskim, ul. Gdańska 6	z urzędu	8.08.2007 r. decyzja GI-DEC-DIS-58/07
58.	10-11.05.2007 r. GI-DIS-K-411/59/07	„Apteka ONZ – Kujawa Tadeusz Marek, Kujawa Anna Małgorzata, Kujawa Michał Tadeusz” s.c. z siedzibą w Józefowie przy ul. Orlej 20, miejsce kontroli – Apteka ONZ w Warszawie przy Al. Jana Pawła II 15	z urzędu	nie stwierdzono uchybień
59.	14-18.05.2007 r. GI-DIS-K-411/60/07	Województwo Łódzkie – Urząd Marszałkowski w Łodzi z siedzibą w Łodzi, Al. Piłsudskiego 8	z urzędu	31.08.2007 r. decyzja GI-DEC-DIS-98/07
60.	14-18.05.2007 r. GI-DIS-K-411/61/07	Powiat Starogardzki – Starostwo Powiatowe w Starogardzie Gdańskim z siedzibą w Starogardzie Gdańskim, ul. Kościuszki 17	z urzędu	8.08.2007 r. decyzja GI-DEC-DIS-59/07
61.	14-18.05.2007 r. GI-DIS-K-411/62/07	Powiat Myślenicki – Starostwo Powiatowe w Myślenicach z siedzibą w Myślenicach, ul. Mikołaja Reja 13	z urzędu	1.08.2007 r. decyzja GI-DEC-DIS-54/07
62.	14-18.05.2007 r. GI-DIS-K-411/63/07	Urząd Celny I w Warszawie – Oddział Celny I Pocztowy z siedzibą w Warszawie, ul. Łączyny 8	Departament Orzecznictwa, Legislacji i Skarg	usunięto uchybienia
63.	14-18.05.2007 r. GI-DIS-K-411/64/07	Techland Sp. z o.o. z siedzibą w Ostrowie Wielkopolskim, ul. Żółkiewskiego 3	z urzędu	13.03.2008 r. decyzja DIS/DEC-178/6683/08
64.	18.05.2007 r. GI-DIS-K-411/65/07	Izmar Sp. z o.o. z siedzibą w Warszawie, ul. Marszałkowska 138 Miejsce kontroli – Apteka, ul. Hoża 41	z urzędu	20.09.2007 r. decyzja GI-DEC-DIS-103/07

65.	21-24.05.2007 r. GI-DIS-K-411/66/07	Nordea Otwarty Fundusz Emerytalny – Nordea Powszechne Towarzystwo Emerytalne S.A. z siedzibą w Warszawie, Al. Jana Pawła II 27	z urzędu	3.08.2007 r. decyzja GI-DEC-DIS-56/07 decyzja GI-DEC-DIS-57/07
66.	21-25.05.2007 r. GI-DIS-K-411/67/07	Sobiesław Zasada Łódź Sp. z o.o. z siedzibą w Łodzi, ul. Aleksandrowska 11	na wniosek DRZDO/403/24/07	14.11.2007 r. decyzja DIS-DEC-116/421/07
67.	28.05-1.06.2007 r. GI-DIS-K-411/68/07	Polska Grupa Farmaceutyczna S.A. z siedzibą w Łodzi, ul. Zbąszyńska 1	z urzędu	nie stwierdzono uchybień
68.	28.05-1.06.2007 r. GI-DIS-K-411/69/07	DOZ + S.A. z siedzibą w Łodzi, ul. Zbąszyńska 3	z urzędu	nie stwierdzono uchybień
69.	30.05-1.06.2007 r. GI-DIS-K-411/70/07	Ministerstwo Rozwoju Regionalnego z siedzibą w Warszawie, ul. Wspólna 2/4	w związku z kontrolą GI-DIS-K-411/47/07	nie stwierdzono uchybień
70.	28.05-1.06.2007 r. GI-DIS-K-411/71/07	Miasto i Gmina Wieliczka – Urząd Miasta i Gminy Wieliczka z siedzibą w Wieliczce, ul. Powstania Warszawskiego 1	z urzędu	20.09.2007 r. decyzja GI-DEC-DIS-102/07
71.	25.05.2007 r. GI-DIS-K-411/72/07	BRE Bank S.A. z siedzibą w Warszawie ul. Senatorska 13	w związku z kontrolą GI-DIS-K-411/22/07	materiał dowodowy zostanie wykorzystany w postępowaniu prowadzonym przez IPSOS Polska Sp. z o. o. w W-wie (GI-DIS-K-411/22/07);
72.	31.05.2007 r. GI-DIS-K-411/73/07	Link4 Towarzystwo Ubezpieczeń S.A. z siedzibą w Warszawie, Al. Jerozolimskie 92	w związku z kontrolą GI-DIS-K-411/22/07	18.01.2008 r. decyzja DIS/DEC-28/1168/08
73.	29.05.2007 r. GI-DIS-K-411/74/07	Polska Grupa Farmaceutyczna Sp. z o.o. z siedzibą w Warszawie, ul. Marywilska 42 B	z urzędu	nie stwierdzono uchybień
74.	1.06.2007 r. GI-DIS-K-411/75/07	Piotr Kotulski prowadzący działalność gospodarczą pod nazwą „CENTRUM NLP” z siedzibą w Warszawie, ul. Skierniewicka 21/15	Departament Orzecznictwa, Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
75.	4-6.06.2007 r. GI-DIS-K-411/76/07	BRE Bank S.A. z siedzibą w Warszawie, ul. Senatorska 18	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
76.	11-15.06.2007 r. GI-DIS-K-411/77/07	Województwo Świętokrzyskie – Urząd Marszałkowski Województwa Świętokrzyskiego z siedzibą w Kielcach, Al. IX Wieków Kielc 3	z urzędu	14.11.2007 r. decyzja DIS-DEC-113/421/07
77.	11-15.06.2007 r. GI-DIS-K-411/78/07	Gmina Oleśnica – Urząd Miasta Oleśnica z siedzibą w Oleśnicy, Rynek Ratusz	z urzędu	7.09.2007 r. decyzja GI-DEC-DIS-101/07
78.	11-15.06.2007 r. GI-DIS-K-411/79/07	Powiat Oleśnicki – Starostwo Powiatowe w Oleśnicy z siedzibą w Oleśnicy, ul. Słowackiego 10	z urzędu	2007-08-17, decyzja GI-DEC-DIS-66/07
79.	11-15.06.2007 r. GI-DIS-K-411/80/07	Gmina Miasta Konin – Urząd Miasta w Koninie	z urzędu	3.10.2007 r. decyzja DIS-DEC-107/421/07

		z siedzibą w Koninie, Pl. Wolności 1		
80.	11-15.06.2007 r. GI-DIS-K-411/81/07	Powiat Koniński – Starostwo Powiatowe w Koninie z siedzibą w Koninie, AL. 1 – go Maja 9	z urzędu	nie stwierdzono uchybień
81.	18-22.06.2007 r. GI-DIS-K-411/82/07	Gospodarstwo Pomocnicze przy Śląskim Centrum Zdrowia Publicznego z siedzibą w Katowicach, ul. Dworcowa 17	z urzędu	nie stwierdzono uchybień
82.	18.06.2007 r. GI-DIS-K-411/83/07	Logistep Polska s. c. Krzysztof Gajewski, Nestor Nalewajk z siedzibą w Warszawie, Pl. Czerwca 1976 r. 2/308 Miejsce kontroli – Ożarów Mazowiecki, ul. Poznańska 215	z związku z kontrolą GI-DIS-K- 411/64/07	nie stwierdzono uchybień
83.	18-19.06.2007 r. GI-DIS-K-411/84/07	Gmina Konstancin Jeziorna – Urząd Miasta i Gminy Konstancin – Jeziorna z siedzibą w Konstancinie – Jeziorna, ul. Warszawska 32	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
84.	20-22.06.2007 r. GI-DIS-K-411/85/07	Śląska Izba Lekarska z siedzibą w Katowicach, ul. Grażyńskiego 49 A	z urzędu (pismo ŚIL/3791/07)	16.08.2007 r. decyzja GI-DEC-DIS-64/07
85.	25-26.06.2007 r. GI-DIS-K-411/86/07	Fundacja Pomocy Ludzie Ludziom – Dom Samotnej Matki z siedzibą w Biłgoraju k. Bełchatowa Rogowiec, gm. Kleszczów	z urzędu	nie stwierdzono uchybień
86.	25-29.06.2007 r. GI-DIS-K-411/87/07	Wojewódzki Urząd Pracy w Katowicach z siedzibą w Katowicach, ul. Powstańców 41 A	Departament Orzecznictwa, Legislacji i Skarg	1.02.2008 r. decyzja DIS/DEC-86/2633/08
87.	25-29.06.2007 r. GI-DIS-K-411/88/07	Województwo Dolnośląskie – Urząd Marszałkowski Województwa Dolnośląskiego z siedzibą we Wrocławiu, ul. Wybrzeże Juliusza Słowackiego 12 – 14	z urzędu	14.11.2007 r. Decyzja DIS-DEC-112/421/07
88.	22-28.06.2007 r. GI-DIS-K-411/89/07	ING Nationale – Nederlanden Polska S. A. z siedzibą w Warszawie, ul. Ludna 2	Departament Orzecznictwa, Legislacji i Skarg	7.04.2008 r. decyzja DIS/DEC- 223/8734,8735/08
89.	27-29.06.2007 r. GI-DIS-K-411/90/07	Samodzielny Publiczny Zespół Zakładów Lecznictwa Otwartego Warszawa – Żoliborz z siedzibą w Warszawie, ul. Szajnoch 8 Miejsce kontroli – Przychodnia Rejonowa z siedzibą w Warszawie, ul. Felińskiego 8	z urzędu	nie stwierdzono uchybień
90.	9-11.07.2007 r. GI-DIS-K-411/91/07	Przychodnia Specjalistyczna „Anpol Centrum” s. c. z siedzibą w Warszawie,	z urzędu	nie stwierdzono uchybień

		ul. Mokotowska 35 A		
91.	9-13.07.2007 r. GI-DIS-K-411/92/07	Wojewódzki Szpital Psychiatryczny im. prof. Tadeusza Bilikiewicza w Gdańsku z siedzibą w Gdańsku, ul. Srebrniki 1	Departament Orzecznictwa, Legislacji i Skarg	26.10.2007 r. decyzja DIS-DEC-110/421/07
92.	9-13.07.2007 r. GI-DIS-K-411/93/07	Daniel Ślusarz prowadzący dział. gosp. pod firmą „Taurus Daniel Ślusarz” z siedzibą w Legnicy, Al. Rzeczypospolitej 116	w związku z kontrolą GI-DIS-K- 411/31/07	23.11.2007 r. decyzja DIS-DEC-123/421/07
93.	9-13.07.2007 r. GI-DIS-K-411/94/07	Bartłomiej Ślusarz prowadzący dział. gosp. pod firmą „Viktoria Bartłomiej Ślusarz” z siedzibą w Legnicy, Al. Rzeczypospolitej 116	w związku z kontrolą GI-DIS-K- 411/31/07	23.11.2007 r. decyzja DIS-DEC-122/421/07
94.	9-12.07.2007 r. GI-DIS-K-411/95/07	Tacoma Polska Sp. z o. o. z siedzibą w Wałbrzychu, ul. Limanowskiego 7 lok. 6 Miejsce kontroli – Biuro Tacoma Polska Sp. z o. o. z siedzibą we Wrocławiu, ul. Kazimierza Wielkiego 27 A	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
95.	16-20.07.2007 r. GI-DIS-K-411/96/07	Instytut Reumatologii im. prof. dr hab. med. Eleonory Reicher w Warszawie z siedzibą w Warszawie, ul. Spartańska 1	z urzędu	nie stwierdzono uchybień
96.	16-18.07.2007 r. GI-DIS-K-411/97/07	Centrum Medyczne Damiana Sp. z o. o. Niepubliczny ZOZ w Warszawie z siedzibą w Warszawie, ul. Wałbrzyska 45 Miejsce kontroli – Przychodnia Wałbrzyska w Warszawie, ul. Wałbrzyska 46	z urzędu	14.11.2007 r. decyzja DIS-DEC-118/421/07
97.	23-27.07.2007 r. GI-DIS-K-411/98/07	Instytut Matki i Dziecka z siedzibą w Warszawie, ul. Kasprzaka 17 A	z urzędu	12.11.2007 r. decyzja DIS-DEC-111/421/07
98.	24-27.07.2007 r. GI-DIS-K-411/99/07	Instytut Gruźlicy i Chorób Płuc z siedzibą w Warszawie, ul. Płocka 26	z urzędu	nie stwierdzono uchybień
99.	25-27.07.2007 r. GI-DIS-K- 411/100/07	Instytut Psychosomatyczny Sp. z o. o. NZOZ w Warszawie z siedzibą w Warszawie przy ul. Poleczki 49 Miejsce kontroli – Centrum Medyczne Instytutu Psychosomatycznego w Warszawie, ul. Mokotowska 3/6	z urzędu	nie stwierdzono uchybień
100.	6-10.08.2007 r. GI-DIS-K-411/101/07	Gmina Miasta Gliwice – Urząd Miejski w Gliwicach z siedzibą w Gliwicach, ul. Zwycięstwa 21	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
101.	6-10.08.2007 r. GI-DIS-K-411/102/07	Gmina Miasta Sosnowiec – Urząd Miejski w Sosnowcu z siedzibą w Sosnowcu,	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień

		Al. Zwycięstwa 20		
102.	6-08.08.2007 r. GI-DIS-K-411/103/07	Krajowe Centrum Osteoporozy z siedzibą w Warszawie, ul. Wł. Syrokomli 32	z urzędu	nie stwierdzono uchybień
103.	8-10.08.2007 r. GI-DIS-K-411/104/07	Centrum Profilaktyki i Terapii Niepubliczny Zakład Opieki Zdrowotnej z siedzibą w Warszawie, ul. Grójecka 126	z urzędu	5.10.2007 r. decyzja DIS-DEC-109/421/07
104.	8-09.08.2007 r. GI-DIS-K-411/105/07	Samodzielny Zespół Publicznych Zakładów Lecznictwa Otwartego Warszawa – Wola z siedzibą w Warszawie, ul. Obozowa 63/65	z urzędu	5.10.2007 r. decyzja DIS-DEC-108/421/07
105.	27-31.08.2007 r. GI-DIS-K-411/106/07	Remes Sp. z o.o. z siedzibą w Opalenicy ul. 5 Stycznia 35	Departament Orzecznictwa, Legislacji i Skarg	23.01.2008 r. decyzja DIS/DEC-44/1640/08
106.	20-24.08.2007 r. GI-DIS-K-411/107/07	Centrum Rehabilitacji im. prof. M. Weissa „STOCER” Samodzielny Publiczny Zakład Opieki Zdrowotnej z siedzibą w Konstancinie – Jeziornie, ul. Wierzejewskiego 12	z urzędu	14.11.2007 r. decyzja DIS-DEC-114/421/07
107.	20-22.08.2007 r. GI-DIS-K-411/108/07	Warszawskie Centrum Alergologii „ALERGO – MED” z siedzibą w Warszawie, ul. Lewicka 4	z urzędu	nie stwierdzono uchybień
108.	27.08.2007 r. GI-DIS-K-411/109/07	IT Polpager S. A. z siedzibą w Warszawie, ul. Pawia 55	z urzędu	wykonano decyzję GI-DEC-DIS-10/07
109.	27-29.08.2007 r. GI-DIS-K-411/110/07	Szpital Grochowski im. dr med. R. Masztaka – SP ZOZ z siedzibą w Warszawie przy ul. Grenadierów 51/59 Miejsce kontroli – Przychodnia Przyszpitalna przy Szpitalu im. R. Masztaka ul. Grenadierów 51/59 w Warszawie	z urzędu	6.12.2007 r. decyzja DIS-DEC-126/421/07
110.	27-30.08.2007 r. GI-DIS-K-411/111/07	Samodzielny Zespół Publicznych ZOZ dla Szkół Wyższych z siedzibą w Warszawie przy ul. Mochnackiego 10 Miejsce kontroli – Oddział Szpitalny dla Szkół Wyższych przy ul. Mochnackiego 10 w Warszawie	z urzędu	23.01.2008 r. decyzja DIS/DEC-51/1641/08
111.	27-28.08.2007 r. GI-DIS-K-411/112/07	DIP Sp. z o. o. – Przychodnia Lekarzy Specjalistów BEST – MED z siedzibą w Warszawie, Al. Jerozolimskich 87	z urzędu	14.11.2007 r. decyzja DIS-DEC-115/421/07
112.	4-6.09.2007 r. GI-DIS-K-411/113/07	Prezes Urzędu Ochrony Konkurencji i Konsumentów w Warszawie z siedzibą w Warszawie, Pl. Powstańców Warszawy 1	Departament Rejestracji Zbiorów Danych Osobowych	Wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych

113.	5-6.09.2007 r. GI-DIS-K-411/114/07	Centrum Medyczne „ARKA” Niepubliczny Zakład Opieki Zdrowotnej w Warszawie z siedzibą w Warszawie, ul. Kasprzaka 7	z urzędu	14.11.2007 r. decyzja DIS-DEC-117/421/07
114.	10-14.09.2007 r. GI-DIS-K-411/115/07	Samodzielny Publiczny Zespół ZOZ SOLEC – Szpital na Solcu w Warszawie z siedzibą w Warszawie, ul. Solec 93	z urzędu	18.01.2008 r. decyzja DIS/DEC-27/1161/08
115.	10-14.09.2007 r. GI-DIS-K-411/116/07	Gmina Siemianowice Śląskie – Urząd Miasta w Siemianowicach Śląskich z siedzibą władz w Siemianowicach Śląskich, ul. Jana Pawła II 10	z urzędu	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
116.	17-21.09.2007 r. GI-DIS-K-411/117/07	Samodzielny Zespół Publicznych Zakładów opieki Zdrowotnej im. prof. dr Jana Bogdanowicza z siedzibą w Warszawie, ul. Niekańska 4/24	z urzędu	22.02.2008 r. decyzja DIS/DEC-135/4608/08
117.	17-21.09.2007 r. GI-DIS-K-411/118/07	GFI s. c. z siedzibą w Legnicy, Al. Rzeczypospolitej 116	w związku z kontrolą GI-DIS-K-411/93 i 94/07	14.01.2008 r. decyzja DIS/DEC-13/657/08
118.	17-21.09.2007 r. GI-DIS-K-411/119/07	Jerzy Eigner prowadzący dział. gosp. pod nazwą „Polisa Jerzy Eigner” z siedzibą w Legnicy, ul. Piastowska 20 A Miejsce wykonywania dział.: Legnica, ul. Rzeczypospolitej 116	w związku z kontrolą GI-DIS-K- 411/31/07	usunięto uchybienia
119.	18-21.09.2007 r. GI-DIS-K-411/120/07	Niepubliczny Zakład Opieki Zdrowotnej „Carolina Medical Center” z siedzibą w Warszawie, ul. Broniewskiego 89	z urzędu	29.01.2008 r. decyzja DIS/DEC-69/2151/08
120.	17-21.09.2007 r. GI-DIS-K-411/121/07	General Electric Polska Sp. z o.o. z siedzibą w Kłodzku, ul. Piłsudskiego 5	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
121.	17-21.09.2007 r. GI-DIS-K- 411/122/07	Samodzielny Publiczny Szpital Kliniczny im. prof. Witolda Orłowskiego Centrum Medycznego Kształcenia Podyplomowego z siedzibą w Warszawie, ul. Czerniakowska 231	z urzędu	21.12.2007 r. decyzja DIS-DEC-129/421/07
122.	19-21.09.2007 r. GI-DIS-K- 411/123/07	Kancelaria Prawnicza OBIG Sp. z o.o. z siedzibą w Warszawie, ul. Filtrowa 69 lok. 32	z urzędu	nie stwierdzono uchybień
123.	24-26.09.2007 r. GI-DIS-K- 411/124/07	Krajowa Izba Lekarska – Weterynaryjna z siedzibą w Warszawie, Al. Przyjaciół 1	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
124.	24-25.09.2007 r. GI-DIS-K- 411/125/07	Bank Gospodarki Żywnościowej S.A. z siedzibą w Warszawie, ul. Kasprzaka 10/16	z urzędu	nie stwierdzono uchybień

125.	26-27.09.2007 r. GI-DIS-K-411/126/07	Przychodnia Specjalistyczna NZOZ CEMKO z siedzibą w Warszawie, ul. Baśniowa 3	z urzędu	nie stwierdzono uchybień
126.	25-28.09.2007 r. GI-DIS-K-411/127/07	Niepubliczny Zakład Opieki Zdrowotnej BOPOL z siedzibą w Warszawie, Al. Jerozolimskie 123 A	z urzędu	22.01.2008 r. decyzja DIS/DEC-43/1542/08
127.	8-12.10.2007 r. DIS-K-421/128/07	Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Miejski nr 1 z siedzibą w Sosnowcu, ul. Zegadłowicza 3	z urzędu	7.02.2008 r. decyzja DIS/DEC-106/3122/08
128.	8-10.10.2007 r. DIS-K-421/129/07	Biuro Nieruchomości „IBIS” Bogumiła Augustyn z siedzibą w Słupsku, ul. Tuwima 12/3	z urzędu	nie stwierdzono uchybień
129.	9-10.10.2007 r. DIS-K-421/130/07	Stowarzyszenie Collegium Invisible z siedzibą w Warszawie, ul. Krakowskie Przedmieście 3/12	z urzędu	14.01.2008 r. decyzja DIS/DEC-12/656/08
130.	15-18.10.2007 r. DIS-K-421/131/07	Niepubliczny Zakład Opieki Zdrowotnej „MegaMed” Sp. z o.o. z siedzibą w Bełchatowie, ul. Czapliniecka 93/95	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
131.	15-19.10.2007 r. DIS-K-421/132/07	Prokuratura Rejonowa w Dębicy z siedzibą w Dębicy, ul. Rzeszowska 23	z urzędu	27.11.2007 r. decyzja DIS-DEC-124/421/07
132.	15-17 i 19.10.2007 r. DIS-K-421/133/07	Przedsiębiorstwo Usługowo – Handlowe „W – Ż” Sp. z o.o. z siedzibą w Gdańsku, ul. Grunwaldzka 493	Departament Rejestracji Zbiorów Danych Osobowych	26.03.2008 r. decyzja DIS/DEC-200/7714/08
133.	18.10.2007 r. DIS-K-421/134/07	Zakład Pogrzebowy „Concordia” s.c. z siedzibą w Gdyni, ul. Powstania Styczniowego 4A	Departament Orzecznictwa, Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
134.	15-19.10.2007 r. DIS-K-421/135/07	Ministerstwo Finansów z siedzibą w Warszawie, ul. Świętokrzyska 12	z urzędu	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
135.	15-19.10.2007 r. DIS-K-421/136/07	Zakład Ubezpieczeń Społecznych z siedzibą w Warszawie, ul. Czerniakowska 16	z urzędu	Pismo informujące o wynikach kontroli
136.	25-26 i 29- 30.10.2007 r. DIS-K-421/137/07	Archiwum Państwowe Miasta Stołecznego Warszawy z siedzibą w Warszawie przy ul. Krzywe Koło 7 Miejsce kontroli – Oddział w Grodzisku Mazowieckim, ul. Poniatowskiego 14	z urzędu	nie stwierdzono uchybień
137.	26 i 29-31.10.2007 r. DIS-K-421/138/07	Archiwum Państwowe Miasta Stołecznego Warszawy z siedzibą w Warszawie przy ul. Krzywe Koło 7 Miejsce kontroli – Oddział w Otwocku, ul. Górna 7	z urzędu	nie stwierdzono uchybień
138.	29-31.10 i 5-9.11.2007 r.	Przedsiębiorstwo Państwowe „Porty Lotnicze”	z urzędu	2.04.2008 r. decyzja DIS/DEC-210/8375/08

	DIS-K-421/139/07	z siedzibą w Warszawie, ul. Żwirki i Wigury 1		
139.	12-16.11.2007 r. DIS-K-421/140/07	Dom Dziecka w Gdańsku z siedzibą w Gdańsku, ul. Brzezi 55	Departament Orzecznictwa, Legislacji i Skarg	2.04.2008 r. decyzja DIS/DEC-209/8372/08
140.	12-16.11.2007 r. DIS-K-421/141/07	Maria Cierech, Krzysztof Grabarski Wspólnicy s.c. „Mare Plus” z siedzibą w Gdyni, ul. Legionów 94 A	Departament Orzecznictwa Legislacji i Skarg	w toku
141.	13-14.11.2007 r. DIS-K-421/142/07	EURO – NET Sp. z o.o. z siedzibą w Warszawie, ul. Muszkieterów 15	Departament Orzecznictwa, Legislacji i Skarg	w toku
142.	12-16.11.2007 DIS-K-421/143/07	Bank BPH S.A. z siedzibą w Krakowie Al. Pokoju 1	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
143.	19-23.11.2007 r. DIS-K-421/144/07	Adam Drabiński prowadzący działalność gospodarczą pod firmą „Regionalna Agencja Rozwoju Rynku” z siedzibą w Bydgoszczy, ul. Świętojańska 10/16	Departament Orzecznictwa, Legislacji i Skarg	10.06.2008 r. decyzja DIS/DEC- 350/14494/08
144.	19-20.11.2007 r. DIS-K-421/145/07	Zarząd Transportu Miejskiego z siedzibą w Warszawie, ul. Senatorska 37	z urzędu	14.01.2008 r. decyzja DIS/DEC-14/658/08
145.	27-30.11.2007 r. DIS-K-421/146/07	LG Electronics Mława Sp. z o. o. z siedzibą w Mławie, ul. LG Electronics 7	Departament Orzecznictwa, Legislacji i Skarg	22.02.2008 r. decyzja DIS/DEC-134/4605/08
146.	19-23.11.2007 r. DIS-K-421/147/07	Archiwum Państwowe w Łodzi z siedzibą w Łodzi, Pl. Wolności 1	z urzędu	7.04.2008 r. decyzja DIS/DEC-222/8731/08
147.	27-29.11.2007 r. DIS-K-421/148/07	Kancelaria Prawno – Finansowa Pro & Lex Marta Raszewska i Partnerzy z siedzibą w Kole ul. Włocławska 7	Departament Orzecznictwa, Legislacji i Skarg	5.02.2008 r. decyzja DIS/DEC-88/2841/08
148.	26-28.11.2007 r. DIS-K-421/149/07	Archiwum Państwowe w Łodzi z siedzibą w Łodzi przy Pl. Wolności 1 Miejsce kontroli – Oddział w Sieradzu, ul. Polskiej Organizacji Wojskowej 5	z urzędu	7.04.2008 r. decyzja DIS/DEC-222/8731/08
149.	27-30.11.2007 r. DIS-K-421/150/07	„LIDER” Sp. z o.o. z siedzibą w Inowrocławiu, ul. Staropoznańska 188	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
150.	27-30.11.2007 r. DIS-K-421/151/07	Archiwum Państwowe m. st. Warszawy z siedzibą w Warszawie przy ul. Krzywe Koło 7 Miejsce kontroli – Ekspozytura w Milanówku, ul. Okrzei 1	z urzędu	nie stwierdzono uchybień
151.	5-6.12.2007 r. DIS-K-421/152/07	Schenker Sp. z o.o. z siedzibą w Warszawie, ul. Ordona 2 A	z urzędu	wykonano decyzję GI-DEC-DIS-69/07/632
152.	5-6.12.2007 r. DIS-K-421/153/07	Telepizza Poland Sp. z o.o. z siedzibą w Warszawie, ul. Marymoncka 32	Departament Orzecznictwa, Legislacji i Skarg	8.02.2008 r. decyzja DIS/DEC-119/3313/08
153.	5-6.12.2007 r. DIS-K-421/154/07	Accord Finance S.A. z siedzibą w Warszawie,	z urzędu	wykonano decyzję GI-DEC-DIS-274/06/737

		ul. Ogrodowa 58		
154.	5-6.12.2007 r. DIS-K-411/155/07	Accord Finance S.A. z siedzibą w Warszawie, ul. Ogrodowa 58	z urzędu	wykonano decyzję GI-DEC-DIS-272/06/735
155.	6.12.2007 r. GI-DIS-K- 421/156/07	Nordea Otwarty Fundusz Emerytalny z siedzibą w Warszawie, Al. Jana Pawła II 27	z urzędu	wykonano decyzję GI-DEC-DIS- 56/07/556
156.	6.12.2007 r. DIS-K-421/157/07	Nordea Powszechnie Towarzystwo Emerytalne S.A. z siedzibą w Warszawie, Al. Jana Pawła II 27	z urzędu	wykonano decyzję GI-DEC-DIS-57/07/557
157.	5-12.2007 r. DIS-K-421/158/07	Powiat Legionowski z siedzibą władz w Legionowie, ul. Sikorskiego 11	z urzędu	wykonano decyzję GI-DEC-DIS-62/07/574
158.	5-6.12.2007 r. DIS-K-421/159/07	Polski Związek Piłki Nożnej z siedzibą w Warszawie, ul. Miodowa 1	z urzędu	wykonano decyzję GI-DEC-DIS-359/06/989
159.	5.12.2007 r. DIS-K-421/160/07	Gmina Legionowo – Urząd Miasta Legionowo z siedzibą w Legionowie, ul. J. Piłsudskiego 3	z urzędu	wykonano decyzję GI-DEC-DIS-20/07/339
160.	10-12.12.2007 r. DIS-K-421/161/07	Archiwum Państwowe m. st. Warszawy - Oddział w Pułtusk z siedzibą w Pułtusk, ul. Zaulek 22	z urzędu	nie stwierdzono uchybień
161.	10-14.12.2007 r. DIS-K-421/162/07	Archiwum Akt Nowych z siedzibą w Warszawie, ul. Hankiewicza 1	z urzędu	13.03.2008 r. decyzja DIS/DEC-177/6682/08
162.	10-14.12.2007 r. DIS-K-421/163/07	Archiwum Państwowe m. st. Warszawy z siedzibą w Warszawie przy ul. Krzywe Koło 7 Miejsce kontroli – Oddział w Łowiczu, ul. 3 Maja 1	z urzędu	nie stwierdzono uchybień
163.	10-14.12.2007 r. DIS-K-421/164/07	Centrum Informatyki ZETO S. A. z siedzibą w Białymstoku, ul. Skorupska 9	z urzędu	nie stwierdzono uchybień
164.	10-14.12.2007 r. DIS-K-421/165/07	Cegedim Poland Sp. z o.o. z siedzibą w Warszawie, ul. Pileckiego 63	Prezes Naczelnej Rady Lekarskiej	nie stwierdzono uchybień
165.	11-12.12.2007 r. GI-DIS-K- 411/166/07	EMPiK Sp. z o.o. z siedzibą w Warszawie, ul. Marszałkowska 116/122	z urzędu	wykonano decyzje GI-DEC-DIS-16/07/292 i GI-DEC-DIS-52/07/532
166.	20.12.2007 r. DIS-K-421/167/07	Centrum Profilaktyki i Terapii Niepubliczny Zakład Opieki Zdrowotnej z siedzibą w Warszawie, ul. Grójecka 126	z urzędu	przywrócono stan zgodny z prawem
167.	17-18.12.2007 r. DIS-K-421/168/07	Centralny Organ Techniczny KSI (Komendant Główny Policji) z siedzibą w Warszawie, ul. Puławska 148/150	Komenda Główna Policji	19.12.2007 r. opinia w sprawie spełniania przez Krajowy System Informatyczny wymogów określonych w art. 36 – 39 ustawy o ochronie danych osobowych i 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
--	--	--	--	---

Załącznik nr 4 Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2007 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych.

l.p.	Data, sygnatura orzeczenia WSA lub NSA	Sygnatury decyzji Generalnego Inspektora Ochrony Danych Osobowych	Przedmiot sprawy	Rozstrzygnięcie WSA lub NSA
1.	3.01.2007 r. II SA/Wa 2110/06	GI-DEC-DIS-180/06/519, GI-DEC-DIS-349/06/953	Zbieranie danych osobowych pracowników w zakresie szerszym niż wynika to z przepisów Kodeksu pracy, niezgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych.	oddalenie wniosku o wstrzymanie wykonania decyzji
2.	11.01.2007 r. II SA/Wa 2265/06	GI-DEC-DS-378/06/1082	Wniosek o wstrzymanie wykonania decyzji	Wstrzymanie wykonania zaskarżonej decyzji
3.	11.01.2007 r. II SA/Wa 1525/06	GI-DEC-DS-216/06/593	Udostępnienie danych osobowych z UOKiK do NBP	Uchylenie zaskarżonej decyzji
4.	12.01.2007 r. I OSK 218/06	GI-DEC-DIS-257/04/547, GI-DEC-DIS-17/05/50	Niezgłoszenie rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych, niezawarcie w polityce bezpieczeństwa wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do poszczególnych pól informacyjnych i powiązania między nimi.	uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania Wojewódzkiemu Sądowi Administracyjnemu w Warszawie
5.	16.01.2007 r. II SA/Wa 1504/06	GI-DEC-DS-179/06/515,516 517	Przetwarzanie danych osobowych przez Gospodarczy Bank Wielkopolski S.A.	Umorzenie postępowania przed Wojewódzkim Sądem Administracyjnym w Warszawie
6.	18.01.2007 r. II SA/Wa 2328/06	GI-DEC-DS-385/06/1109, 1110	Wniosek o wstrzymanie wykonania decyzji	Odmowa wstrzymania wykonania decyzji
7.	23.01.2007 r. II SA/Wa 2240/06	GI-DEC-DS-117/05/330,331 332	Udostępnienie danych osobowych Związkowi Banków Polskich	Odrzucenie skargi
8.	23.01.2007 r. II SA/Wa 1337/06	GI-DEC-DS-152/06/457,458 459	Wniosek o nakazanie Prezydentowi Miasta Jastrzębie Zdrój udostępnienie danych osobowych	Umorzenie postępowania przed Wojewódzkim Sądem Administracyjnym w Warszawie
9.	23.01.2007 r. II SA/Wa 995/06	GI-DEC-DS-87/06/275,276, 277	Wniosek o nakazanie usunięcia danych osobowych ze Związku Banków Polskich	Uchylenie zaskarżonej decyzji
10.	25.01.2007 r. II SA/Wa	GI-DEC-DS-352/06/969,970	Udostępnienie przez Forum DZT S.A. danych osobowych skarżącej Centrum S.A.	Oddalenie skargi

	2136/06	971		
11.	25.01.2007 r. II SA/Wa 1526/06	GI-DEC-DS- 220/06/599,600	Przetwarzanie danych osobowych	Oddalenie skargi.
12.	29.01.2007 r. II SA/Wa 1423/06	GI-DEC-DS- 158/06/467	Udostępnienie danych osobowych przez Towarzystwo Ubezpieczeniowe podmiotowi nieuprawnionemu	Odmowa przywrócenia terminu do wniesienia skargi
13.	6.02.2007 r. II SA/Wa 1786/06	GI-DEC-DS- 263/06/699,700 701	Udostępnienie przez Spółdzielnię Mieszkaniową w Aleksandrowie Kujawskim danych osobowych POBUD Sp. z o.o.	Oddalenie skargi
14.	6.02.2007 r. II SA/Wa 1337/06	GI-DEC-DS- 152/06/457,458 459	Wniosek o nakazanie Prezydentowi Miasta Jastrzębie Zdrój udostępnienia danych osobowych	Odmowa uzupełnienia postanowienia
15.	8.02.2007 r. II SA/Wa 2111/06	GI-DEC-DS- 345/06/934,935 936,937,938, 939	Przetwarzanie danych osobowych	Odrzucenie skargi
16.	15.02.2007 r. II SA/2064/06	GI-DEC-DS- 317/06/861,862 863	Usunięcie danych osobowych z bazy danych BIK S.A.	Oddalenie skargi
17.	16.02.2007 r. I OSK 478/06	GI-DEC-DIS- 286/04/626, GI-DEC-DIS- 47/05/130	Zbieranie danych osobowych w zakresie szerszym niż jest to niezbędne dla realizacji celu przetwarzania danych.	oddalenie skargi kasacyjnej
18.	16.02.2007 r. I OSK 523/06	GI-DEC-DIS- 48/05/131, GI-DEC-DIS- 127/05/359	Zbieranie danych osobowych w zakresie szerszym niż jest to niezbędne dla realizacji celu przetwarzania danych, niedopełnianie obowiązku informacyjnego oraz rozstrzyganie indywidualnej sprawy wyłącznie w oparciu o operacje na danych osobowych dokonywane w systemie informatycznym.	umorzenie postępowania ze skargi kasacyjnej
19.	28.02.2007 r. II SA/Wa 1423/06	GI-DEC-DS- 158/06/467	Udostępnienie danych osobowych przez Towarzystwo Ubezpieczeniowe podmiotowi nieuprawnionemu	Odrzucenie skargi
20.	28.02.2007 r. II SA/Wa 156/06	GI-DEC-DS- 419/05/1219	Odmowa udostępnienia informacji publicznej	Zwrot skarżącemu połowy wpisu od skargi
21.	28.02.2007 r. II SA/Wa 2108/06	GI-DEC-DS.- 335/06/910,911 912,913	Odmowa udostępnienia danych osobowych	Oddalenie skargi
22.	7.03.2007 r. II SA/Wa 9/06	GI-DEC-DS- 380/05/1067, 1068,1069	Przetwarzanie danych osobowych skarżącego	Odrzucenie skargi kasacyjnej
23.	7.03.2007 r. II SA/Wa 2260/06	GI-DEC-DS- 372/06/1067, 1068	Przetwarzanie danych osobowych skarżącej przez PZU S.A.	Oddalenie skargi
24.	13.03.2007 r. II SA/Wa 2240/06	GI-DEC-DS- 117/05/330,331 332	Udostępnienie danych osobowych Związkowi Banków Polskich	Odrzucenie skargi kasacyjnej
25.	13.03.2007 r. II SA/Wa 2141/06	GI-DEC-DS- 351/06/962,963 964,965,966, 967,968	Przetwarzanie danych osobowych skarżącej przez Rzecznika Dyscyplinarnego dla Nauczycieli przy Wojewodzie Warmińsko-Mazurskim	Uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej

26.	16.03.2007 r. II SA/Wa 2110/06	GI-DEC-DIS- 180/06/519, GI-DEC-DIS- 349/06/953	Zbieranie danych osobowych pracowników w zakresie szerszym niż wynika to z przepisów Kodeksu pracy, niezgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych.	uchylenie zaskarżonej decyzji
27.	22.03.2007 r. II SA/Wa 1933/06	GI-DEC-DS- 303/06/826/827	Wniosek o stwierdzenie bezprawności przetwarzania danych osobowych przez Błaja News Sp. z o.o.	Oddalenie skargi
28.	23.03.2007 r. I OZ 185/07	GI-DEC-DS- 228/06/620	Udostępnienie danych osobowych przez PTC Sp. z o.o. Straży Miejskiej w Wałbrzychu	Uchylenie zaskarżonego postanowienia i przekazanie sprawy Wojewódzkiemu Sądowi Administracyjnemu w Warszawie do ponownego rozpoznania
29.	23.03.2007 r. II SA/Wa 2047/05	GI-DEC-DS- 297/05/845,846 847,848,849	Przetwarzanie danych osobowych skarżącego m.in. przez Prezydenta Miasta Ruda Śląska	Oddalenie skargi
30.	3.04.2007 r. I OZ 215/07	GI-DS- 430/279/05/ 5529,5530	Odmowa sporządzenia wykazu akt w sprawie prowadzonej przez GIODO	Oddalenie zażalenia na postanowienie WSA w Warszawie o odrzuceniu zażalenia na postanowienie
31.	13.04.2007 r. II SA/Wa 2079/06	GI-DEC-DS- 340/06/921,922 923,924	Wniosek o stwierdzenie nielegalności przetwarzania danych osobowych	Oddalenie skargi
32.	16.04.2007 r. II SAB/Wa 2/07	GI-DS- 430/838/05	Skarga na bezczynność	Zobowiązanie GIODO do rozpatrzenia wniosku w terminie 2 miesięcy od otrzymania prawomocnego wyroku
33.	17.04.2007 r. I OSK 391/07	GI-DEC-DS- 309/06/841,842 843	Przetwarzanie danych osobowych	Uchylenie zaskarżonego postanowienia WSA w Warszawie
34.	18.04.2007 r. II SA/Wa 2055/06	GI-DEC-DS- 313/06/849,850 851	Udostępnienie danych osobowych firmie windykacyjnej	Odrzucenie skargi
35.	20.04.2007 r. I OZ 272/07	GI-DEC-DS- 378/06/1080, 1081,1082	Wniosek o wstrzymanie decyzji w przedmiocie usunięcia danych osobowych z BIK S.A.	Uchylenie zaskarżonego postanowienia. Odmowa wstrzymania wykonania zaskarżonej decyzji
36.	26.04.2007 r. II SA/Wa 92/07	GI-DEC- DOLiS- 432/06/1257	Odmowa uwzględnienia wniosku złożonego w trybie ustawy o dostępie do informacji publicznej.	Odmowa przywrócenia terminu do wniesienia skargi
37.	8.05.2007 r. II SA/Wa 414/07	GI-DEC- DOLiS- 10/07/329,330	Przetwarzanie danych osobowych	Odrzucenie skargi
38.	9.05.2007 r. II SA/Wa 1552/06	GI-DEC-DS- 228/06/620	Udostępnienie danych osobowych przez operatora telefonii komórkowej	Odmowa wstrzymania wykonania zaskarżonej decyzji

39.	9.05.2007 r. II SA/Wa 1049/06	GI-DS- 430/213/03/ 1296,1297/06	Udostępnienie danych osobowych	Oddalenie odwołania na postanowienie GIODO
40.	17.05.2007 r. II SA/Wa 176/06	GI-DS- 430/279/05/ 5529,5530	Odmowa sporządzenia wykazu akt postępowania	Odrzucenie skargi
41.	22.05.2007 r. II SA/Wa 1049/06	GI-DS- 430/213/03/ 1296,1297/06	Przetwarzanie danych osobowych	Odrzucenie skargi kasacyjnej
42.	25.05.2007 r. I OSK 917/06	GI-DEC-DS- 297/05/845,846 847,848,849	Przetwarzanie danych osobowych	Oddalenie skargi kasacyjnej
43.	29.05.2007 r. II SA/Wa 893/07	GI-DEC-DS- 75/06/244	Udostępnienie danych osobowych przez towarzystwo ubezpieczeniowe	Odrzucenie skargi
44.	14.06.2007 r. II SA/Wa 92/07	GI-DEC- DOLiS- 432/06/1257	Wniosek w trybie ustawy o dostępie do informacji publicznej	Odrzucenie skargi
45.	14.06.2007 r. II S.A/Wa 92/07	GI-DEC- DOLiS- 432/06/1257	Wniosek o udostępnienie informacji publicznej	Odrzucenie skargi
46.	15.06.2007 r. I OZ 427/07	GI-DEC- DOLiS- 30/07/657,658	Przetwarzanie danych osobowych	Oddalenie zażalenia
47.	19.06.2007 r. II SA/Wa 852/07	GI-DS- 430/213/03/ 1296,1297/06	Przetwarzanie danych osobowych	Odrzucenie skargi
48.	26.06.2007 r. I OZ 459/07	GI-DEC-DS- 380/05/1067, 1068,1069	Przetwarzanie danych osobowych	Oddalenie zażalenia
49.	29.06.2007 r. II SA/Wa 1049/06	GI-DS- 430/213/03/ 1296,1297/06	Przetwarzanie danych osobowych	Odrzucenie zażalenia
50.	29.06.2007 r. I OSK 1098/06	GI-DEC-DS- 397/05/1153, 1154	Przetwarzanie danych osobowych przez NZOZ „Zdrowie Rodziny” Sp. z o.o. w Poznaniu	Oddalenie skargi kasacyjnej
51.	04.07.2007 r. II SA/Wa 2240/06	GI-DEC-DS- 117/05/330,331 332	Udostępnienie danych osobowych do Związku Banków Polskich	Odrzucenie skargi kasacyjnej
52.	5.07.2007r. II SA/Wa 261/07	GI-DEC-DIS- 257/04/07, GI-DEC-DIS- 17/05/50	Nie zgłoszenie rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych, nie zawarcie w polityce bezpieczeństwa wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do poszczególnych pól informacyjnych i powiązania między nimi.	Uchylenie zaskarżonej decyzji w zakresie pkt II
53.	17.07.2007 r. II SA/Wa 1141/07	GI-DS- 430/213/03/ 1296,1297/06	Odmowa zawieszenia postępowania administracyjnego	Odrzucenie skargi
54.	17.07.2007 r. I OZ 520/07	GI-DEC-DS- 151/06/455,456	Przetwarzanie danych osobowych	Odmowa zwolnienia z kosztów postępowania
55.	19.07.2007 r. II SA/Wa 93/07	GI-DEC- DOLiS 442/06	Wniosek o nakazanie udostępnienia danych osobowych	Oddalenie skargi
56.	08.08.2007 r. I OZ 584/07	GI-DEC-DS- 228/06/620	Nakaz udostępnienia danych osobowych	Uchylenie postanowienia WSA w Warszawie i przekazanie do ponownego rozpoznania

57.	14.08.2007 r. II SA/Wa 1252/07	GI-DEC- DOLiS- 109/07/2885	Udostępnianie danych osobowych abonentów operatora podmiotom trzecim	Odmowa wstrzymania wykonania zaskarżonej decyzji
58.	14.08.2007 r. II SA/Wa 1300/07	GI-DEC- DOLiS- 429/06/1247	Przetwarzanie danych osobowych	Odrzucenie skargi
59.	14.08.2007 r. II SA/Wa 2265/06	GI-DEC-DS- 378/06/1082	Nakazanie udostępnienia danych osobowych	Umorzenie postępowania przed WSA w Warszawie
60.	22.08.2007 r. II SA/Wa 793/07	GI-DEC- DOLiS- 56/07/1295, 1296	Wniosek o usunięcie danych osobowych	Oddalenie skargi
61.	23.08.2007 r. II SA/Wa 852/07	GI-DS- 430/212/03/ 1296,1297/06	Odmowa zawieszenia postępowania administracyjnego	Odmowa sprostowania postanowienia WSA w Warszawie. Odmowa wykładni postanowienia WSA w Warszawie.
62.	28.08.2007 r. II SA/Wa 71/7	GI-DEC-DS- 414/06/1199	Nakaz udostępnienia danych osobowych	Odmowa wstrzymania wykonania decyzji
63.	30.08.2007 r. II SA/Wa 2287/06	GI-DEC-DS- 357/06/986,987	Udostępnienie danych osobowych podmiotom nieuprawnionym	Postanowienie o oddaleniu odwołania od zarządzenia przewodniczącego
64.	14.09.2007 r. I OZ 655/07	GI-DS- 430/213/03/ 1296,1297/06	Odmowa zawieszenia postępowania administracyjnego	Oddalenie zażalenia
65.	17.09.2007 r. II SA/Wa 2287/06	GI-DEC-DS- 357/06/986,987	Udostępnienie danych osobowych podmiotom nieuprawnionym	Odrzucenie skargi kasacyjnej
66.	25.09.2007 r. I OZ 681/07	GI-DEC- DOLiS- 451/06/1307 1308	Przetwarzanie danych osobowych	Oddalenie zażalenia
67.	8.10.2007 r. II SA/Wa 889/07	GI-DEC- DOLiS- 64/07/1671,167 2	Przetwarzanie danych osobowych	Oddalenie skargi
68.	11.10.2007 r. II SA/Wa 1692/06	GI-DEC-DS- 225/06/613,614	Udostępnienie danych osobowych osobom nieupoważnionym	Odrzucenie zażalenia
69.	11.10.2007 r. II SA/Wa 700/07	GI-DOLiS- 430/426/06/ 1173,1174/07	Udostępnienie danych osobowych podmiotom nieuprawnionym	Oddalenie skargi
70.	16.10.2007 r. II SA/Wa 678/07	GI-DEC-DS- 309/06/841,842 843	Przetwarzanie danych osobowych	Odrzucenie skargi kasacyjnej
71.	16.10.2007 r. II SA/Wa 1427/06	GI-DS- 430/987/04/ 2245,2256, 2247	Udostępnienie danych osobowych Związkowi Banków Polskich	Odrzucenie skargi kasacyjnej
72.	16.10.2007 r. II SA/Wa 1427/06	GI-DS- 430/987/04/ 2245,2256, 2247	Udostępnienie danych osobowych Związkowi Banków Polskich	Odmowa sporządzenia uzasadnienia wyroku
73.	17.10.2007 r. II SA/Wa	GI-DEC-DS- 228/06/620	Wniosek o udostępnienie danych osobowych	Wstrzymanie wykonania

	1552/06			zaskarżonej decyzji
74.	22.10.2007 r. II SA/Wa 1384/07	GI-DS- 430/213/03/ 1296,1297/06	Przetwarzanie danych osobowych	Odrzucenie skargi
75.	26.10.2007 r. II SA/Wa 1994/06	GI-DEC-DS- 304/06/828	Przetwarzanie danych osobowych	Odmowa przywrócenia terminu do wniesienia odwołania od zarządzenia przewodniczącego
76.	7.11.2007 r. II SA/Wa 1740/07	GI-DEC- DOLiS- 114/07/2927, 2928,2929,293 0	Przetwarzanie danych osobowych	Odrzucenie skargi
77.	9.11.2007 r. I OZ 820/07	GI-DS- 430/213/03/ 1296,1297/06	Przetwarzanie danych osobowych	Oddalenie zażalenia
78.	13.11.2007 r. II SA/Wa 1692/06	GI-DEC-DS- 225/06/613,614	Udostępnienie danych osobowych osobom nieupoważnionym	Sprostowanie oczywistej omyłki
79.	15.11.2007 r. II SA/Wa 1994/06	GI-DEC-DS- 304/06/828	Przetwarzanie danych osobowych	Odrzucenie skargi kasacyjnej
80.	20.11.2007 r. II SA/Wa 1823/07	GI-DEC- DOLiS- 148/07/3926	Przetwarzanie danych osobowych	Przywrócenie terminu do wniesienia skargi
81.	28.11.2007 r. II SA/Wa 1164/07	GI-DEC- DOLiS- 89/07/2542,254 3,2544	Przetwarzanie danych osobowych	Odrzucenie skargi
82.	30.11.2007 r. II SA/Wa 1299/07	GI-DRZDO/ 401/DEC/ 003768/05- 197/07	Odmowa rejestracji zbioru danych osobowych	Uchylenie zaskarżonej decyzji
83.	6.12.2007 r. I OZ 912/07	GI-DEC-DS- 225/06/613,614	Udostępnienie danych osobowych osobom nieupoważnionym	Oddalenie zażalenia
84.	21.12.2007 r. I OZ 972/07	GI-DEC-DS- 228/06/620	Wniosek o udostępnienie danych osobowych	Oddalenie zażalenia

Załącznik nr 5 Informacje przekazane przez organy ścigania w sprawach skierowanych w 2007 r. przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa.

Informacja	Rok 2005	Rok 2006	Rok 2007
Umorzenie dochodzenia	13	2	17
Umorzenie dochodzenia w części	-	-	-
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	13	-	5
Umorzenie dochodzenia i odmowa podjęcia go na nowo	7	-	-
Wszczęcie dochodzenia	8	-	-
Odmowa wszczęcia dochodzenia	21	1	5
Wszczęcie śledztwa i jego umorzenie	15	-	2
Zawieszenie dochodzenia	1	-	2
Skierowanie sprawy do sądu	12	-	5
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	5	-	-
Brak informacji	13	-	-

Załącznik nr 6 Wykaz szkoleń przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych w roku 2007.

L.p.	Data i miejsce	Podmiot szkolony	Tematyka szkolenia
1.	25 stycznia 2007 r. Warszawa	studenci Wyższej Szkoły Przedsiębiorczości i Zarządzania im. L. Koźmińskiego	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych.
2.	31 stycznia 2007 r. Bruksela	polscy eurodeputowani	Prawne aspekty przetwarzania danych osobowych. Administrowanie zbiorami danych osobowych.
3.	23 lutego 2007 r. Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne oraz pracownicy centrali MSZ	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Interpretacja pojęć ustawy o ochronie danych osobowych.
4.	8 marca 2007 r. Warszawa	pracownicy Kancelarii Senatu	Podstawowe pojęcia ustawy o ochronie danych osobowych. Administrowanie danymi osobowymi.
5.	19 marca 2007 r. Warszawa	informatycy Ministerstwa Spraw Zagranicznych	Polityka bezpieczeństwa przetwarzania danych osobowych.
6.	20 marca 2007 r. Warszawa	kadra kierownicza Kancelarii Sejmu	Obowiązki administratora danych: podstawy przetwarzania danych osobowych, obowiązek informacyjny, rejestracja zbiorów danych osobowych, zabezpieczenie zbiorów danych.
7.	22 marca 2007 r. Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne oraz pracownicy centrali MSZ	Obowiązki administratora danych osobowych w zakresie zabezpieczenia danych. Odpowiedzialność karna i dyscyplinarna za naruszenia prawa do ochrony danych osobowych.
8.	26 marca 2007 r. Warszawa	pracownicy Izby Celnej	Obowiązki administratora danych osobowych w zakresie zabezpieczenia danych. Odpowiedzialność karna i dyscyplinarna za naruszenia prawa do ochrony danych osobowych. Rejestracja zbiorów danych osobowych.
9.	29 marca 2007 r. Warszawa	kadra kierownicza Kancelarii Prezesa Rady Ministrów	Praktyczne stosowanie ustawy o ochronie danych osobowych.
10.	29 marca 2007 r. Poznań	marszałkowie województw	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych.
11.	3 kwietnia 2007 r. Warszawa	przedsiębiorcy Polskiej Konfederacji Pracodawców Prywatnych „Lewiatan”	Rys historyczny prawa do prywatności i ochrony danych osobowych. Podstawowe pojęcia ustawy o ochronie danych osobowych. Instytucja powierzenia przetwarzania danych osobowych.
12.	16 kwietnia 2007 r. Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne oraz pracownicy centrali MSZ	Ustawowe wymogi dotyczące dokumentacji przetwarzania danych osobowych. Zasady organizacji ochrony danych osobowych.
13.	18 kwietnia 2007 r.	pracownicy Kancelarii	Informacja o sposobie korzystania z

	Warszawa	Prezesa Rady Ministrów	systemu e-GIODO. Praktyczne stosowanie ustawy o ochronie danych osobowych.
14.	19 kwietnia 2007 r. Szczecin	archiwiści zatrudnieni w jednostkach wymiaru sprawiedliwości	Obowiązki administratora danych osobowych. Polityka bezpieczeństwa przetwarzania danych osobowych.
15.	19 kwietnia 2007 r. Warszawa	pracownicy Kancelarii Senatu	Obowiązki administratora danych osobowych w zakresie zabezpieczenia danych. Odpowiedzialność karna i dyscyplinarna za naruszenie prawa do ochrony danych osobowych.
16.	20 kwietnia 2007 r. Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów	Instytucja powierzenia przetwarzania danych osobowych.
17.	25 kwietnia 2007 r. Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów	Realizacja uprawnień kontrolnych osób, których dane osobowe są przetwarzane w zbiorach danych.
18.	25 kwietnia 2007 r. Warszawa	pracownicy Izby Celnej	Prawne aspekty przetwarzania danych osobowych. Obowiązki administratora danych osobowych w zakresie zabezpieczenia danych.
19.	25 kwietnia 2007 r. Warszawa	studenci Uniwersytetu Kardynała Stefana Wyszyńskiego	Zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych. Pytania i odpowiedzi z praktyki stosowania ustawy o ochronie danych osobowych.
20.	27 kwietnia 2007 r. Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów	Praktyczne stosowanie ustawy o ochronie danych osobowych. Informacja o sposobie korzystania z systemu e-GIODO.
21.	9 maja 2007 r. Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów	Obowiązki administratora danych osobowych. Odpowiedzialność karna i dyscyplinarna za naruszenie prawa do ochrony danych osobowych.
22.	11 maja 2007 r. Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów	Obowiązki administratora danych osobowych. Odpowiedzialność karna i dyscyplinarna za naruszenie prawa do ochrony danych osobowych.
23.	15 maja 2007 r. Warszawa	pracownicy Kancelarii Sejmu	Obowiązki administratora danych osobowych. Odpowiedzialność karna i dyscyplinarna za naruszenie prawa do ochrony danych osobowych.
24.	16 maja 2007 r. Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne oraz pracownicy centrali MSZ	Podstawy prawne przetwarzania danych osobowych. Administrowanie zbiorami danych osobowych.
25.	16 maja 2007 r. Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów	Wymagania dotyczące dokumentacji przetwarzania danych osobowych.
26.	21 maja 2007 r. Gdańsk	sędziowie Sądu Apelacyjnego w Gdańsku	Prawo do prywatności i ochrony danych osobowych.
27.	21 maja 2007 r. Sopot	pracownicy Urzędu Miasta Sopotu	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych.
28.	22 maja 2007 r. Gdańsk	sędziowie Sądu Okręgowego w Gdańsku	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych.
29.	22 maja 2007 r. Gdańsk	pracownicy Urzędu Miasta Gdańska	Interpretacja pojęć ustawy o ochronie danych osobowych. Obowiązki administratora danych osobowych.

30.	22 maja 2007 r. Gdańsk	kadra kierownicza Pomorskiego Urzędu Wojewódzkiego w Gdańsku	Rys historyczny prawa do prywatności i ochrony danych osobowych. Podstawowe pojęcia ustawy o ochronie danych osobowych.
31.	22 maja 2007 r. Gdańsk	kadra kierownicza Urzędu Marszałkowskiego Województwa Pomorskiego	Rys historyczny prawa do prywatności i ochrony danych osobowych. Podstawowe pojęcia ustawy o ochronie danych osobowych.
32.	23 maja 2007 r. Sopot	studenci Wyższej Szkoły Finansów i Administracji w Gdańsku oraz przedstawiciele Spółdzielczej Kasy Oszczędnościowo- Rozliczeniowej	Rys historyczny prawa do prywatności i ochrony danych osobowych. Podstawowe pojęcia ustawy o ochronie danych osobowych.
33.	31 maja 2007 r. Kraków	prezesi i pracownicy Samorządowych Kolegiów Odwoławczych	Rys historyczny prawa do prywatności i ochrony danych osobowych. Zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych. Pytania i odpowiedzi z praktyki stosowania ustawy o ochronie danych osobowych.
34.	11 czerwca 2007 r. Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżających na placówki zagraniczne oraz pracownicy centrali MSZ	Obowiązki administratorów danych osobowych. Warunki, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych.
35.	13 czerwca 2007 r. Mikołajki	komornicy sądowi	Zasady udostępniania danych osobowych. Obowiązki administratorów danych osobowych.
36.	13 czerwca 2007 r. Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów	Podstawy przetwarzania danych osobowych. Pytania i odpowiedzi z praktyki stosowania ustawy o ochronie danych osobowych.
37.	15 czerwca 2007 r. Warszawa	kadra kierownicza Narodowego Banku Polskiego	Obowiązki administratora danych osobowych w zakresie zabezpieczenia danych. Odpowiedzialność karna i dyscyplinarna za naruszenia prawa do ochrony danych osobowych.
38.	18 czerwca 2007 r. Warszawa	pracownicy Kancelarii Senatu	Obowiązki administratora danych osobowych. Zabezpieczenie i rejestracja zbiorów danych osobowych.
39.	20 czerwca 2007 r. Janów Lubelski	pracownicy Lubelskiego Urzędu Wojewódzkiego	Zasady ochrony danych osobowych w świetle przepisów ustawy o ochronie danych osobowych.
40.	21 czerwca 2007 r. Olsztyn	pracownicy Służby Celnej, Administratorzy Bezpieczeństwa Informacji oraz ich zastępcy	Warunki, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych. Wymagania dotyczące dokumentacji przetwarzania danych osobowych. Informacje o sposobie korzystania z systemu e-GIODO.
41.	10 lipca 2007 r. Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne oraz pracownicy centrali MSZ	Podstawy przetwarzania danych osobowych. Pytania i odpowiedzi z praktyki stosowania ustawy o ochronie danych osobowych.
42.	07 września 2007 r. Kudowa Zdrój	pracownicy Spółdzielczej Kasy Oszczędnościowo- Kredytowej	Interpretacja podstawowych pojęć ustawy o ochronie danych osobowych.

43.	12 września 2007 r. Warszawa	Pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne	Minimalne wymagania techniczne i organizacyjne stawiane systemom informatycznym w zakresie ochrony danych osobowych.
44.	18 września 2007 r. Warszawa	kadra kierownicza Urzędu Komisji Nadzoru Finansowego	Podstawowe pojęcia ustawy o ochronie danych osobowych. Zasady zabezpieczania i przetwarzania danych osobowych.
45.	20 września 2007 r. Warszawa	kadra kierownicza Urzędu Marszałkowskiego Województwa Mazowieckiego	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Zakres przedmiotowy i podmiotowy ustawy o ochronie danych osobowych.
46.	27 września 2007 r. Warszawa	przedstawiciele samorządu terytorialnego województwa mazowieckiego	Minimalne wymagania techniczne i organizacyjne stawiane systemom informatycznym w zakresie ochrony danych osobowych.
47.	28 września 2007 r. Gołun na Kaszubach	sędziowie Wydziałów Karnych i Cywilnych Sądu Okręgowego w Gdańsku	Rys historyczny prawa do prywatności i ochrony danych osobowych.
48.	28 września 2007 r. Warszawa	sekretarze powiatów i miast	Podstawowe pojęcia ustawy o ochronie danych osobowych.
49.	9 października 2007 r. Warszawa	pracownicy centrali Ministerstwa Spraw Zagranicznych	Obowiązki administratora danych osobowych. Zabezpieczenie i rejestracja zbiorów danych osobowych.
50.	10 października 2007 r. Bruksela	polscy posłowie do Parlamentu Europejskiego	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych.
51.	6 listopada 2007 r. Lublin	pracownicy Lubelskiego Urzędu Wojewódzkiego	Prawne podstawy przetwarzania danych osobowych. Pytania i odpowiedzi z praktyki stosowania ustawy o ochronie danych osobowych.
52.	6 listopada 2007 r. Lublin	pracownicy centrali Ministerstwa Spraw Zagranicznych	Minimalne wymagania techniczne i organizacyjne stawiane systemom informatycznym w zakresie ochrony danych osobowych.
53.	7 listopada 2007 r. Wrocław	pracownicy Południowo-Zachodniej Spółdzielczej Kasy Oszczędnościowo-Rozliczeniowej	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Zakres przedmiotowy i podmiotowy ustawy o ochronie danych osobowych.
54.	7 listopada 2007 r. Wrocław	kadra kierownicza Marszałkowskiego Urzędu Województwa Dolnośląskiego	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Zakres przedmiotowy i podmiotowy ustawy o ochronie danych osobowych.
55.	21 listopada 2007 r. Karpacz	Pracownicy Państwowej Inspekcji Sanitarnej	Rys historyczny prawa do prywatności i ochrony danych osobowych. Zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych. Pytania i odpowiedzi z praktyki stosowania ustawy o ochronie danych osobowych.
56.	3-5 grudnia 2007 r. Wiśła	Administratorzy Bezpieczeństwa Informacji	Warunki, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych. Wymagania dotyczące dokumentacji przetwarzania danych osobowych. Informacje o sposobie korzystania z systemu e-GIODO.
57.	4 grudnia 2007 r.	Pracownicy centrali	Rys historyczny prawa do prywatności i

	Warszawa	Ministerstwa Spraw Zagranicznych	ochrony danych osobowych. Zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych. Pytania i odpowiedzi z praktyki stosowania ustawy o ochronie danych osobowych.
58.	7 grudnia 2007 r. Częstochowa	kuratorzy społeczni Sądu Rejonowego w Częstochowie	Podstawowe pojęcia ustawy o ochronie danych osobowych.
59.	12-14 grudnia 2007 r. Szklarska Poręba	pracownicy Sądu Okręgowego i Sądu Apelacyjnego we Wrocławiu	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Zakres przedmiotowy i podmiotowy ustawy o ochronie danych osobowych.
60.	18 grudnia 2007 r. Katowice	kuratorzy społeczni, zawodowi i aplikanci kuratorscy Sądu Rejonowego w Katowicach.	Pozycja prawna i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Zakres przedmiotowy i podmiotowy ustawy o ochronie danych osobowych.