



**Generalny Inspektor
Ochrony Danych Osobowych**

**SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH
W ROKU 2008**

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 2008 r. do 31 grudnia 2008 r.

SPIS TREŚCI

Część I.

Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych.....	5
1. Informacje ogólne	5
2. Biuro Generalnego Inspektora Ochrony Danych Osobowych	6
2.1. Struktura organizacyjna	6
2.2. Pracownicy Biura GIODO	6
2.3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2008 rok	7

Część II.

Stan wiedzy i przestrzegania przepisów o ochronie danych Osobowych.....	8
1. Informacje ogólne	8
2. Kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych	9
2.1. Czynności kontrolne	9
2.2. Kontrola przetwarzania danych osobowych w wybranych obszarach	10
2.2.1 Bezpieczeństwo publiczne	10
2.2.2 Marketing	11
2.2.3 Mieszkalnictwo	13
2.2.4 Oświata i szkolnictwo wyższe	14
2.2.5 Biura podróży	15
2.2.6 Inne	16
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych	17
3.1. Wydawanie decyzji	17
3.2. Decyzje w wybranych obszarach	19
3.2.1 Administracja publiczna	19
3.2.2 System Informacyjny Schengen	24
3.2.3 Sądy, prokuratura, Policja, komornicy	24
3.2.4 Banki i inne instytucje finansowe	27
3.2.5 Marketing	30
3.2.6 Sektor mieszkalnictwa	32
3.2.7 Ubezpieczenia społeczne, majątkowe i osobowe	35
3.2.8 Telekomunikacja	38
3.2.9 Sektor zatrudnienia	40
3.2.10 Inne.....	42
4. Prowadzenie rejestru zbiorów danych osobowych oraz udzielanie informacji o zarejestrowanych zbiorach	45
5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych	52
6. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych	62
6.1. Interpretacja przepisów	63
6.2. Działalność informacyjna	77
6.2.1. Współpraca ze środkami masowego przekazu	77
6.2.2. Publikacje	80
6.2.3. Szkolenia, staże, wymiana pracowników	81
6.2.4. Konkursy	83
6.2.5. Konferencje i seminaria	83

6.2.6. Internet	87
6.2.7. Inne informacje	90
7. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych	91
7.1. Międzynarodowe spotkania i konferencje	94
7.2. Wizyty robocze	96
7.3. Warsztaty Rozpatrywania Spraw	96
 Część III.	
Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2008 roku	97
 Część IV.	
Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych.....	110

Wykaz załączników

Załącznik nr 1	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2008 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego	113
Załącznik nr 2	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2008 do podmiotów prywatnych	117
Załącznik nr 3	Wykaz kontroli przeprowadzonych w 2008 roku	120
Załącznik nr 4	Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2008 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych	131
Załącznik nr 5	Informacje przekazane przez organy ścigania w sprawach skierowanych w 2008 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa	136
Załącznik nr 6	Wykaz szkoleń przeprowadzonych przez GODO w 2008 r.	137
Załącznik nr 7	Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych wydanych w 2008 roku w sprawach o wyrażenie zgody na przekazanie danych osobowych za granicę	140

Część I.

Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych

1. Informacje ogólne

Podstawę prawną działania Generalnego Inspektora Ochrony Danych Osobowych [GIODO] stanowi ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 z późn. 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 wraz załącznikiem zawierającym opis środków bezpieczeństwa na poziomie podstawowym, podwyższonym i wysokim (Dz. U. Nr 100, poz. 1024), wydane na podstawie art. 39a ustawy. Rozporządzenie 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,²
- 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,
- d) rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006 r. Nr 203, poz. 1494).

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.

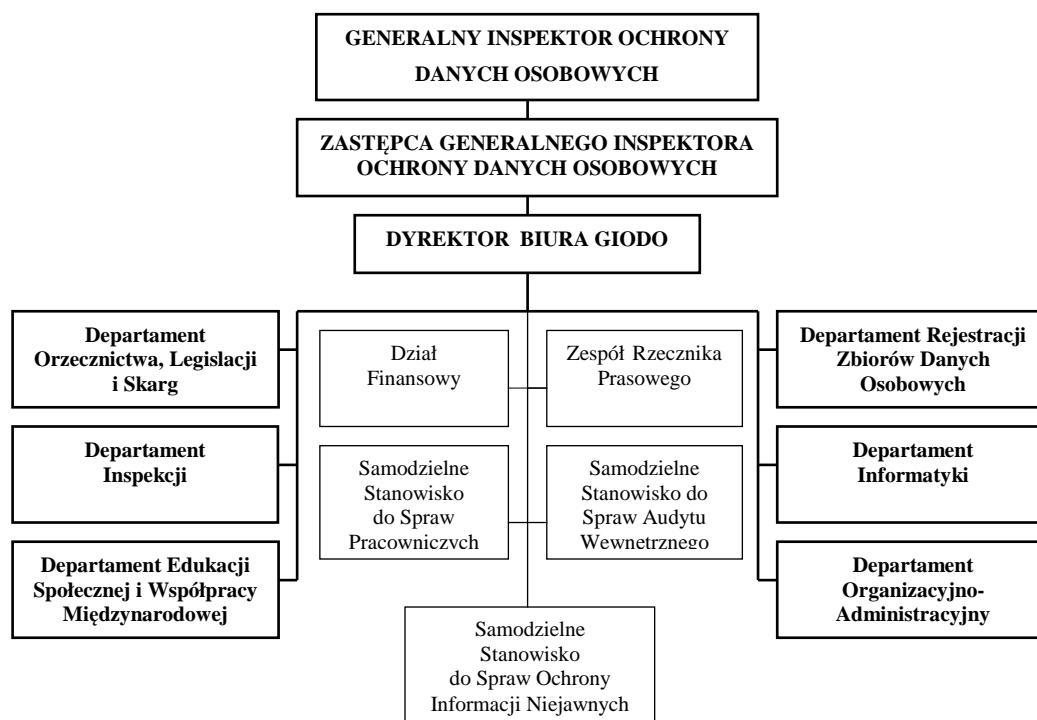
² W dniu 10 lutego 2009 r. weszło w życie nowe rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536).

2. Biuro Generalnego Inspektora Ochrony Danych Osobowych

2.1 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 Biuru 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 oraz innych osób wskazanych w Regulaminie Organizacyjnym.³

2.2. Pracownicy Biura GIODO

Stan zatrudnienia w Biurze GIODO na dzień 31 grudnia 2008 r. wyniósł 120 etatów (pełne etaty). Na stanowiskach merytorycznych zatrudnionych było 105 osób, a na stanowiskach pomocniczych 15 osób. Wyższe wykształcenie posiadało 106 pracowników, w tym 72 legitymowało się wykształceniem wyższym prawniczym.

Zatrudnienie w poszczególnych jednostkach organizacyjnych Biura GIODO w przeliczeniu na pełny etat na koniec 2008 r. przedstawia się następująco:

- GIODO – 1 osoba,
- Zastępca GIODO – 1 osoba,
- Asystent GIODO – 1 osoba,

- Dyrektor Biura – 1 osoba,
- Zespół Rzecznika Prasowego – 4 osoby,
- Departament Edukacji Społecznej i Współpracy Międzynarodowej [DESiWM] – 9 osób,
- Departament Informatyki [DIF] – 15 osób,
- Departament Inspekcji [DIS] – 21 osób,
- Departament Orzecznictwa, Legislacji i Skarg [DOLiS] – 27 osób,
- Departament Rejestracji Zbiorów Danych Osobowych [DRZDO] – 15 osób,
- Departament Organizacyjno-Administracyjny [DOA] – 15 osób,
- Dział Finansowy – 3 osoby,
- Samodzielne Stanowisko ds. Pracowniczych – 2 osoby.

2.3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2008 r

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2008 r. wynosił: **13 717** tys. zł, w tym:

wynagrodzenia	8 759 tys. zł
pochodne od wynagrodzeń	1 511 tys. zł
wydatki majątkowe	168 tys. zł
pozostałe wydatki	3 279 tys. zł

Środki finansowe otrzymane z Ministerstwa Finansów wynosiły: **13 395** tys. zł. Wydatki zrealizowane przez GIODO w 2008 roku wyniosły: **13 381** tys. zł, w tym:

wynagrodzenia	8 748 tys. zł
pochodne od wynagrodzeń	1 333 tys. zł
wydatki majątkowe	153 tys. zł
pozostałe wydatki	3 147 tys. zł

³ Zarządzenie nr 29/2007 Generalnego Inspektora Ochrony Danych Osobowych z dnia 14 września 2007 r. w sprawie wprowadzenia Regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych.

Część II.

Stan wiedzy i przestrzegania przepisów o ochronie danych osobowych

1. Informacje ogólne

Ustawa o ochronie danych osobowych wprowadza szczegółowe normy służące realizacji prawa do ochrony danych osobowych. Reguluje postępowanie przy przetwarzaniu danych osobowych, czyli operacjach, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zdefiniowanych jako wszelkie informacje dotyczące osoby fizycznej, pozwalające bez większego wysiłku na określenie tożsamości tej osoby. Danymi osobowymi nie będą jednak pojedyncze informacje o dużym stopniu ogólności. Staną się nimi dopiero z chwilą zestawienia ich z innymi, dodatkowymi informacjami, które w konsekwencji pozwolą na odniesienie ich do konkretnej osoby.

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.⁴ 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 przetwarzane dłużej, niż jest to niezbędne do osiągnięcia celu, dla którego zostały zebrane.

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 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.

⁴ 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.

Nad przestrzeganiem prawa obywateli do ochrony 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 [K.p.a.], o ile przepisy ustawy o ochronie danych osobowych nie stanowią inaczej (art. 22 ustawy).

Zgodnie z brzmieniem art. 12 wspomnianej 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 w szczególności 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 osób 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 dotyczący umożliwienia inspektorom dokonania tych czynności (art. 15 ust. 1 ustawy o ochronie danych osobowych).

Przeprowadzane w toku kontroli czynności (odbieranie wyjaśnień od kierownictwa i pracowników kontrolowanej jednostki, oględziny) są dokumentowane w formie protokołów przyjęcia ustnych wyjaśnień, protokołów przesłuchania świadka oraz protokołów oględzin miejsca, pomieszczeń, dokumentów, urządzeń, nośników, systemów informatycznych służących do przetwarzania danych osobowych. Na podstawie ustaleń zawartych w ww. protokołach, kserokopiach dokumentów przedłożonych w toku kontroli oraz wydruków z systemów informatycznych służących do przetwarzania danych osobowych, sporządzany jest protokół kontroli. Podpisany przez inspektorów, którzy kontrolę przeprowadzili, protokół kontroli 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,

tn. czy stwierdzone zostały nieprawidłowości w procesie przetwarzania danych osobowych, czy też nie, wszczynane jest postępowanie administracyjne lub kierowane jest do jednostki kontrolowanej 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 podejrzeniu popełnienia 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

W 2008 r. Generalny Inspektor ochrony Danych Osobowych przeprowadził łącznie 201 kontroli zgodności przetwarzania danych osobowych z przepisami ustawy.

2.2.1 Bezpieczeństwo publiczne

W okresie sprawozdawczym, w związku z wejściem Polski do strefy Schengen, Generalny Inspektor Ochrony Danych Osobowych przeprowadził kontrole podmiotów uprawnionych do bezpośredniego dostępu do Krajowego Systemu Informatycznego [KSI]⁵ w celu dokonywania wpisów danych Systemu Informacyjnego Schengen [SIS] oraz w celu wglądu do danych SIS, tj. jednostek Policji (8 kontroli⁶), jednostek Straży Granicznej (9 kontroli⁷), izb celnych (4 kontrole⁸) i konsulatów (2 kontrole⁹). Zakresem kontroli objęto dane osobowe przetwarzane przez te podmioty w związku z realizacją ich uprawnień wynikających z przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej.¹⁰

Na podstawie materiału dowodowego zebranego w toku kontroli przeprowadzonych w jednostkach Policji stwierdzono, że z nadanych upoważnień do dostępu do Krajowego Systemu Informatycznego oraz wykorzystania zasobów SIS dla policjantów i pracowników jednostek organizacyjnych Policji nie wynika rzeczywisty zakres uprawnień ww. osób do dostępu do zasobów SIS. Ponadto przeprowadzone kontrole wykazały, że w niektórych jednostkach **Policji** ewidencja osób upoważnionych do przetwarzania danych osobowych w związku z dostępem do danych SIS nie była w ogóle prowadzona albo była prowadzona w formie niespełniającej wymogów wynikających z art. 39 ust. 1 ustawy o ochronie danych osobowych¹¹ z uwagi na brak wszystkich elementów, tj. zakresu upoważnienia i identyfikatora użytkownika. W dokumencie stanowiącym politykę bezpieczeństwa zastrzeżenia wzbudził także brak wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe oraz niewskazanie w nim sposobu i formy, w jakich taki wykaz miałby zostać określony przez poszczególne jednostki Policji. W związku ze stwierdzonymi nieprawidłowościami w procesie przetwarzania danych osobowych Generalny Inspektor skierował do Komendanta Głównego Policji pismo w sprawie podjęcia działań mających na celu ich usunięcie.¹²

Kontrole przeprowadzone w jednostkach **Straży Granicznej** wykazały, że w niektórych z nich wystawione funkcjonariuszom tej formacji upoważnienia do dostępu do Krajowego Systemu Informatycznego oraz wykorzystania danych SIS nie spełniają wymogów wynikających z § 5 ust. 2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 grudnia 2007 r.

⁵ Centralnym Organem Technicznym KSI jest Komendant Główny Policji.

⁶ Np. DIS-K-421/46/08, DIS-K-421/61/08, DIS-K-421/72/08.

⁷ Np. DIS-K-421/116/08, DIS-K-421/121/08, DIS-K-421/126/08.

⁸ Np. DIS-K-421/147/08, DIS-K-421/154/08.

⁹ DIS-K-421/149/08 i DIS-K-421/193/08.

¹⁰ Dz. U. Nr 165, poz. 1170.

¹¹ 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.

¹² Pismo z dnia 29.07.2008 r. o sygn. DIS-K-421/46/08/19325.

w sprawie trybu dostępu do Krajowego Systemu Informatycznego¹³ w zakresie liczby wystawionych egzemplarzy upoważnień oraz włączania jednego egzemplarza upoważnienia do akt osobowych użytkownika końcowego. W jednej z poddanych kontroli jednostek Straży Granicznej stwierdzono również, że ewidencja osób upoważnionych do przetwarzania danych osobowych nie zawiera identyfikatora osoby upoważnionej do przetwarzania. Ponadto ustalono, że w aneksie nr 1 do „Wykazu zbiorów danych osobowych przetwarzanych w Straży Granicznej, których administratorem jest Komendant Główny Straży Granicznej” nie wymieniono aplikacji o nazwie „SISOne4All”, wykorzystywanej do dostępu do danych SIS. Stwierdzone uchybienia stanowiły podstawę do skierowania do Komendanta Głównego Straży Granicznej pisma o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości.¹⁴

W toku kontroli przeprowadzonych w **izbach celnych** ustalono, że dokumentacja stanowiąca politykę bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych nie zawiera informacji dotyczących dostępu do danych SIS za pomocą aplikacji „SISOne4All” oraz systemu informatycznego użytkowanego w kontrolowanych jednostkach. Stwierdzono również inne nieprawidłowości, jak nienadanie osobom posiadającym dostęp do danych SIS pisemnych upoważnień, brak ewidencji osób upoważnionych do dostępu do danych SIS lub nieokreślenie w niej zakresu upoważnienia do przetwarzania danych i identyfikatorów osób upoważnionych oraz nieprzeprowadzenie dla osób mających dostęp do Krajowego Systemu Informatycznego szkoleń z zakresu bezpieczeństwa i ochrony danych. W związku ze stwierdzonymi nieprawidłowościami w procesie przetwarzania danych osobowych, Generalny Inspektor skierował do Szefa Służby Celnej pismo o podjęcie działań mających na celu ich usunięcie.¹⁵

W październiku i grudniu 2008 r. przeprowadzono kontrole w **Konsulatach RP we Lwowie oraz Moskwie**. Dostęp do danych SIS w konsulatach realizowany jest za pośrednictwem systemu informatycznego o nazwie „Wiza – Konsul” oraz poprzez aplikację SISOne4All. System „Wiza – Konsul” jest zintegrowanym systemem służącym konsulom m.in. do wydawania wiz. Umożliwia on sprawdzenie, czy osoba ubiegająca się o wydanie wizej figuruje w SIS, w wykazie osób niepożądanych na terytorium RP oraz przeprowadzanie konsultacji wizowych krajowych i międzynarodowych. Sprawdzenia danych SIS wykonywane są jedynie przy użyciu stacjonarnych stacji roboczych. Serwery z systemem „Wiza – Konsul” znajdują się w Ministerstwie Spraw Zagranicznych oraz w Ambasadach RP. Transmisja danych pomiędzy ambasadami a MSZ jest szyfrowana przy wykorzystaniu sprzętowych szyfratorów.

Kontrole przeprowadzone w **konsulatach** wskazały na konieczność dokonania czynności kontrolnych w Ministerstwie Spraw Zagranicznych w celu uzupełnienia materiału dowodowego w zakresie przetwarzania danych osobowych w związku z dostępem do SIS. Kontrola taka zaplanowana została na 2009 r.

2.2.2 Marketing

W okresie sprawozdawczym skontrolowano 23 firmy marketingowe, w tym 20 kontroli przeprowadzono w ramach tzw. kontroli sektorowej.¹⁶ Zakresem kontroli objęto przetwarzanie danych osobowych klientów oraz pracowników firm marketingowych działających w Warszawie i Poznaniu.

Kontrolowane jednostki miały najwięcej problemów z prawidłowym wykonaniem obowiązków określonych w rozdziale 5 ustawy o ochronie danych osobowych. Nieprawidłowości dotyczyły w szczególności prowadzonej dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która nie spełniała wszystkich wymogów wynikających z § 4 i § 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne

¹³ § 5 ust. 2. Użytkownik instytucjonalny wystawia w dwóch egzemplarzach dla każdego użytkownika końcowego pisemne upoważnienie do dostępu do Krajowego Systemu Informatycznego oraz wykorzystania danych. Jeden egzemplarz pisemnego upoważnienia włącza się do akt osobowych użytkownika końcowego, drugi egzemplarz przekazuje się użytkownikowi końcowemu.

¹⁴ Pismo z dnia 14.01.2009 r. o sygn. DIS-K-421/116/08/1050/09.

¹⁵ Pismo z dnia 13.01.2009 r. o sygn. DIS-K-421/147/08/1010/09.

¹⁶ Np. kontrole: DIS-K-421/1/08, DIS-K-421/3/08, DIS-K-421/9/08 i DIS-K-421/18/08.

służące do przetwarzania danych osobowych.¹⁷ W kilku przypadkach inspektorzy GODO mieli zastrzeżenia do ewidencji osób upoważnionych do przetwarzania danych osobowych, np. z uwagi na brak zakresu upoważnienia do przetwarzania danych osobowych.

W toku kontroli firm marketingowych, do najczęściej stwierdzanych nieprawidłowości należały również uchybienia w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych. Nieprawidłowości te dotyczyły m.in. niezapewnienia przez systemy informatyczne służące do przetwarzania danych osobowych odnotowania daty pierwszego wprowadzenia danych do systemu.

Na podstawie wyników kontroli stwierdzono ponadto, że niektóre poddane kontroli firmy marketingowe nie dopełniały wobec osób, których dane dotyczą, w pełnym zakresie obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych¹⁸, jak również pozyskiwały od osób, których dane przetwarzały, jedno oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych w różnych celach. Efektem tej niedopuszczalnej praktyki było pozyskiwanie, a właściwie wymuszanie zgody na udostępnianie danych osobowych innym podmiotom.

Nieprawidłowości stwierdzono także w dokumentacji zawartej w aktach osobowych pracowników firm marketingowych. W toku kontroli ustalono, iż pracodawcy w związku ze stosowaniem nieaktualnych kwestionariuszy osobowych pozyskiwali w szerszym zakresie dane osobowe swoich pracowników (m.in. nazwisko rodowe matki), niż wynika to z przepisów art. 22¹ § 1, § 2 i § 4 Kodeksu pracy.¹⁹

W związku ze stwierdzonymi w toku kontroli uchybieniami wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości już usuniętych przez jednostki kontrolowane.²⁰ W wydanych decyzjach Generalny Inspektor nakazał m.in.: usunięcie danych po osiągnięciu celu, dla którego zostały pozyskane, zaprzestanie zbierania danych osobowych pracowników w zakresie szerszym, niż jest to określone w przepisach prawa (np. w zakresie nazwiska rodzowego matki); umieszczenie w treści kuponów konkursowych tak sformułowanej klauzuli zgody na przetwarzanie danych osobowych, aby zapewniała uczestnikom konkursów opcjonalność w kwestii wyrażenia zgody na przetwarzanie ich danych osobowych w celach marketingowych oraz by wyraźnie precyzowała, na rzecz jakiego podmiotu miałyby być prowadzone wspomniane działania marketingowe; dopełnienie obowiązku informacyjnego w zakresie poinformowania osób, których dane dotyczą, o adresie siedziby i pełnej nazwie administratora danych oraz celu zbierania danych laureatów loterii promocyjnej.

¹⁷ § 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.

¹⁸ 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 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.

¹⁹ 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.

²⁰ Np. decyzje o sygn. DIS/DEC-213/8452/08, DIS/DEC-435/18348/08, DIS/DEC-288/11881/08 i DIS/DEC-486/21461/08.

2.2.3 Mieszkalnictwo

W 2008 r. w podmiotach należących do omawianego sektora przeprowadzonych zostało 20 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, w tym 16 w spółdzielniach mieszkaniowych.²¹ W jednej ze spółdzielni dane osobowe przetwarzane były wyłącznie w formie papierowej, bez wykorzystania systemów informatycznych.

Skontrolowane spółdzielnie mieszkaniowe najwięcej problemów miały ze spełnieniem wymogów wynikających z przepisów rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Stwierdzone w tym zakresie uchybienia dotyczyły w szczególności niezastosowania mechanizmów kontroli dostępu do danych, niezapewniania przez systemy informatyczne służące do przetwarzania danych osobowych odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, zmieniania haseł dostępu rzadziej niż co 30 dni oraz niezabezpieczenia danych poprzez wykonywanie kopii zapasowych. Kontrole wykazywały także brak dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną lub niezawarcie w tej dokumentacji wszystkich wymaganych elementów, o których mowa w § 4 i § 5 wspomnianego rozporządzenia, nieopracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych lub niewpisanie do niej wszystkich informacji określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych oraz dopuszczenie do przetwarzania tych osób, którym nie zostały nadane przez administratora danych stosowne upoważnienia. W toku kilku kontroli ustalono ponadto, że nie został wyznaczony administrator bezpieczeństwa informacji.

Wyniki kontroli przeprowadzonych w spółdzielniach mieszkaniowych wskazują również, że podmioty te nie wykonywały podstawowych obowiązków wynikających z przepisów o ochronie danych osobowych. Do stwierdzonych w tym zakresie nieprawidłowości należało m.in. niedopełnianie obowiązku zgłoszenia prowadzonych zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (np. zbioru danych właścicieli lokali niebędących członkami spółdzielni, zbioru danych najemców miejsc parkingowych należących do zasobów spółdzielni), niezapewnienie, aby dane osobowe członków spółdzielni przetwarzane były zgodnie z prawem (przepisami prawa spółdzielczego) oraz niezastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych (np. przechowywanie dokumentacji zawierającej dane osobowe w szafach bez zamków w pomieszczeniach, w których przyjmowani są interesanci). Na 16 skontrolowanych spółdzielni tylko w 4 nie stwierdzono jakichkolwiek uchybień w procesie przetwarzania danych osobowych.

W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych przez jednostki kontrolowane, wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych w toku postępowania.²² Generalny Inspektor w decyzjach nakazywał w szczególności opracowanie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, nadanie upoważnień osobom dopuszczonym do przetwarzania danych osobowych, zgłoszenie do rejestracji Generalnemu Inspektorowi prowadzonego zbioru danych osobowych oraz zabezpieczenie dokumentacji zawierającej dane osobowe przed jej udostępnieniem osobom nieupoważnionym i zabranie przez osobę nieuprawnioną.

²¹ Np. kontrole: DIS-K-421/101/08, DIS-K-421/107/08, DIS-K-421/110/08.

²² Np. decyzje o sygn. DIS/DEC-748/31712/08, DIS/DEC-775/33105/08, DIS/DEC-844/35144/08.

2.2.4 Oświata i szkolnictwo wyższe

W okresie sprawozdawczym przeprowadzono w szkołach 25 kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w tym 24 kontrole to były tzw. kontrole sektorowe.²³ Objęto nimi przetwarzanie danych osobowych uczniów oraz pracowników ww. podmiotów.

Na podstawie ustaleń kontrolnych krytycznie należy ocenić poziom spełnienia przez ww. podmioty wymogów określonych w przepisach o ochronie danych osobowych, w szczególności w odniesieniu do przetwarzania danych przy użyciu systemów informatycznych. Uchybienia w tym zakresie dotyczyły m.in. niezmienniania co 30 dni hasel służących do uwierzytelnienia użytkowników, niezarejestrowania w systemie odrębnego identyfikatora dla każdego użytkownika systemu, niezabezpieczenia systemów informatycznych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, niewykonywania kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych oraz niezastosowania mechanizmów kontroli dostępu do danych osobowych.

Liczne zastrzeżenia dotyczyły także ewidencji osób upoważnionych do przetwarzania danych osobowych oraz dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, których kontrolowane jednostki albo w ogóle nie opracowały, albo nie zawierały w nich wszystkich wymaganych elementów, określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych oraz § 4 i § 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Poddane kontroli szkoły problemy miały również z zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, co skutkowało przechowywaniem dokumentacji zawierającej dane osobowe w sposób umożliwiający dostęp do niej osobom nieupoważnionym, tj. na otwartych regałach i w niezamykanych szafach w pomieszczeniach, w których przebywały również osoby postronne.

W toku przeprowadzonych kontroli zwrócono uwagę na kwestie przetwarzania przez szkoły danych Osobowych w systemach informatycznych o nazwach „Hermes” oraz „System Informacji Oświatowej” [SIO]. Stwierdzono, iż ww. systemy informatyczne nie spełniały wymogów określonych w § 7 ust. 1 pkt. 1 i 2, § 7 ust. 2 i § 7 ust. 3 wspomnianego rozporządzenia.²⁴

W systemie informatycznym o nazwie „System Informacji Oświatowej” dane osobowe są przetwarzane w celach określonych w ustawie z dnia 19 lutego 2004 r. o systemie informacji oświatowej.²⁵ Natomiast w systemie o nazwie „Hermes” dane te - w myśl postanowień rozporządzenia Ministra Edukacji Narodowej z dnia 30 kwietnia 2007 r. w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów i słuchaczy oraz przeprowadzania sprawdzianów i egzaminów w szkołach publicznych²⁶ - przetwarzane są w celu przesyłania do właściwej okręgowej komisji egzaminacyjnej informacji o tym, którzy uczniowie przystępują do sprawdzianu, egzaminu gimnazjalnego lub maturalnego. Stosowanie przez szkoły systemu informatycznego o nazwie „System Informacji Oświatowej”, wskazanego przez Ministra Edukacji Narodowej jest obowiązkiem określonym w ustawie o systemie informacji oświatowej. Natomiast system informatyczny o nazwie „Hermes” szkoły pobierają ze stron internetowych właściwych okręgowych komisji egzaminacyjnych, które wskazały ten system jako jedyny do stosowania. W związku z tym, że szkoły nie mają

²³ Np. kontrole: DIS-K-421/49/08, DIS-K-421/51/08 i DIS-K-421/53/08.

²⁴ § 7. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie: 1) daty pierwszego wprowadzenia danych do systemu; 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba; 3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; 4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych; 5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy. 2. Odnotowanie informacji, o których mowa w ust. 1 pkt. 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych. 3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

²⁵ Dz. U. Nr 49, poz. 463 z późn. zm.

²⁶ Dz. U. Nr 83, poz. 562 z późn. zm.

uprawnień do samodzielnego dostosowania ww. systemów informatycznych do wymogów określonych w przepisach o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Ministra Edukacji Narodowej o podjęcie działań mających na celu dostosowanie systemów informatycznych o nazwach „Hermes” oraz „System Informacji Oświatowej” do wymogów określonych w przepisach o ochronie danych osobowych.²⁷

W związku ze stwierdzonymi w toku kontroli uchybieniami wydane zostały decyzje nakazujące usunięcie uchybień w procesie przetwarzania danych osobowych oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych przez jednostki kontrolowane w toku postępowania.²⁸ W wydanych decyzjach Generalny Inspektor nakazał m.in. zapewnienie, aby dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym o nazwie „SIO” oraz w systemie informatycznym o nazwie „Hermes”, systemy te umożliwiały automatyczne odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego te dane, zapewnienie, aby w systemie informatycznym o nazwie „SIO” rejestrowany był dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia. Ponadto Generalny Inspektor Ochrony Danych Osobowych nakazał zabezpieczenie użytkowanych systemów informatycznych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2.2.5 Biura podróży

W okresie sprawozdawczym przeprowadzono 20 kontroli w wybranych losowo biurach turystycznych. Zakresem kontroli objęto w szczególności przetwarzanie danych osobowych obecnych, jak i potencjalnych klientów.²⁹

Na podstawie ustaleń kontrolnych należy krytycznie ocenić poziom spełnienia przez ww. podmioty wymogów określonych w przepisach o ochronie danych osobowych. Nieprawidłowości stwierdzono, m.in. w zakresie realizacji obowiązku informacyjnego wynikającego z art. 24 ust. 1 ustawy o ochronie danych osobowych. Przeprowadzone kontrole wykazały bowiem, że zarówno klienci, jak i potencjalni klienci, nie byli informowani o znanych lub przewidywanych odbiorcach lub kategoriach odbiorców danych, o prawie dostępu do treści swoich danych oraz ich poprawiania, a także o dobrowolności podania danych. Niektóre z biur podróży nie zgłosiły prowadzonych zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi (m.in. zbioru danych uczestników imprez turystycznych). Kontrolowane jednostki miały również wiele problemów z prawidłowym wykonaniem obowiązków dotyczących zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym i zabranieniem przez osobę nieuprawnioną (m.in. dokumentacja zawierająca dane osobowe przechowywana była w szafach niewyposażonych w zamki oraz na otwartych półkach i regałach).

Nieprawidłowości występowały także w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych i dotyczyły niezapewnienia przez systemy informatyczne służące do przetwarzania danych osobowych odnotowania m.in. daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Ponadto hasła uwierzytelnienia do systemów informatycznych były zmieniane rzadziej niż co 30 dni, a przesyłanie danych osobowych klientów przez sieć publiczną odbywało się w formie niezabezpieczonej (tj. bez szyfrowania danych).

Przeprowadzone kontrole wykazały, że biura podróży miały problemy z prawidłowym prowadzeniem dokumentacji opisującej sposób przetwarzania danych osobowych, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Uchybienia w tym zakresie polegały m.in. na niezawarcu w polityce bezpieczeństwa wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, a w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych na niezawarcu m.in. opisu procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

²⁷ Pismo z dnia 8 września 2008 r. o sygn. DIS-K-421/47/08/23320.

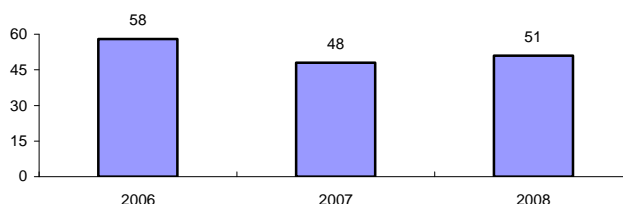
²⁸ Np. decyzje o sygn. DIS/DEC-657/27547/08, DIS/DEC-655/27563/08 i DIS/DEC-646/27140/08.

²⁹ Np. kontrole: DIS-K-421/155/08, DIS-K-421/157/08, DIS-K-421/159/08.

oraz sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych.

2.2.6 Inne

W okresie sprawozdawczym w podmiotach nienależących do sektorów omówionych w poprzednich rozdziałach przeprowadzono 51 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.³⁰ Grupa tych podmiotów jest bardzo zróżnicowana i obejmuje m.in. podmioty wykonujące działalność gospodarczą w zakresie transportu drogowego oraz podmioty zajmujące się produkcją i handlem.



Wykres 1.
Porównanie liczby przeprowadzonych kontroli w podmiotach należących do sektora „Inne” w latach 2006 – 2008.

Analizując wyniki kontroli należy stwierdzić, że jednostki kontrolowane miały problemy z prawidłowym wykonaniem podstawowych obowiązków wynikających z przepisów o ochronie danych osobowych. Uchybienia w tym zakresie dotyczyły w szczególności braku odrębnej klauzuli o wyrażeniu zgody na przetwarzanie danych w celu marketingu produktów i usług innych podmiotów, niedopełnienia w pełnym zakresie wobec osób, których dane dotyczą, obowiązku informacyjnego wynikającego z art. 24 ust. 1 ustawy o ochronie danych osobowych, oraz niezgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych prowadzonych zbiorów danych osobowych (np. zbioru danych osobowych klientów). 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 osobowych oraz § 4 i § 5 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

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 (m.in. niezapewnianie dla każdej osoby, której dane osobowe są przetwarzane w systemach informatycznych, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, zmiana haseł dostępu rzadziej niż co 30 dni).

W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych przez jednostki kontrolowane, wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych w toku postępowania.³¹ Generalny Inspektor w decyzjach nakazywał w szczególności dopełnianie wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, zmodyfikowanie systemu informatycznego służącego do przetwarzania danych osobowych tak, aby dla każdej osoby, której dane osobowe są w nim

³⁰ Np. DIS-K-421/15/08, DIS-K-421/27/08, DIS-K-421/31/08, DIS-K-421/120/08, DIS-K-421/172/08.

³¹ Np. decyzje o sygn. DIS/DEC-206/8000/08, DIS/DEC-540/24201/08 i DIS/DEC-659/27642/08.

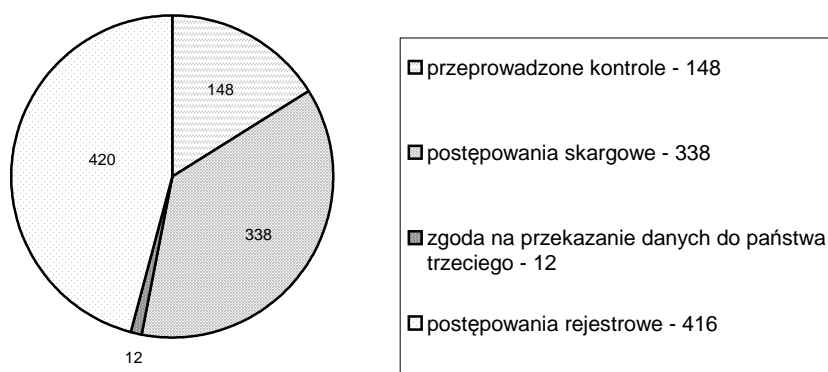
przetwarzane, system ten zapewniał odnotowanie daty pierwszego wprowadzenia danych do systemu oraz opracowanie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

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

3.1. Wydawanie decyzji

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 2008 r. Generalny Inspektor wydał **914 decyzji administracyjnych**, w tym 420 dotyczyło postępowań rejestrowych, 148 zostało wydanych w związku z przeprowadzonymi kontrolami, 338 wydano na skutek postępowania zainicjowanego skargą, zaś 12 dotyczyło zgody na przekazanie danych do państwa trzeciego.



Wykres 2.
Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2008 r.

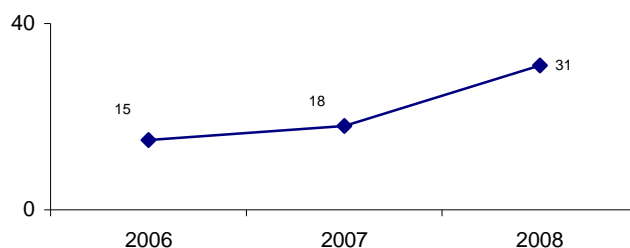
W analizowanym roku sprawozdawczym 2008 Generalny Inspektor Ochrony Danych Osobowych skierował do organu powołanego do ścigania przestępstw **31 zawiadomień o popełnieniu przestępstwa**. Jedno z nich dotyczyło stwierdzonego w trakcie przeprowadzanej kontroli przypadku udostępnienia danych osobom nieupoważnionym. Przedmiotem ww. zawiadomienia było naruszenie przez podmiot kontrolowany przepisu art. 36 ust. 1 i art. 31 ustawy o ochronie danych osobowych, które stanowiło wypełnienie znamion przestępstwa określonego w art. 51 ust. 1 wspomnianej ustawy. W zawiadomieniu wskazano między innymi, iż podmiot, któremu powierzono przetwarzanie danych osobowych na podstawie umowy wynikającej z art. 31 tejże ustawy, nie posiadał umocowania do udostępnienia danych klientów innym podmiotom i tym samym naruszył przepisy karne ustawy o ochronie danych osobowych.

Jak co roku, najwięcej zawiadomień o popełnieniu przestępstwa złożonych zostało w związku z postępowaniami prowadzonymi na skutek skarg wniesionych do Generalnego Inspektora. Spośród 30 sporządzonych zawiadomień najwięcej (21) dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego w art. 49 ust. 1 ustawy o ochronie

danych osobowych, przetwarzania danych przez podmioty nieuprawnione. Ponadto Generalny Inspektor Ochrony Danych Osobowych stwierdził 6 przypadków udostępnienia danych osobowych podmiotom nieuprawnionym. Te sprawy stały się podstawą do skierowania zawiadomień 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 działalność marketingową, polegającą na przysyłaniu do adresatów materiałów z ofertą sprzedaży. W postępowaniach prowadzonych przez organ, firmy marketingowe nie potrafiły w sposób wiarygodny wskazać źródła pozyskania danych osobowych adresata oraz podstawy prawnej udostępnienia (sprzedaży bazy danych osobowych) kolejnym podmiotom prowadzącym tego typu działalność. 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).

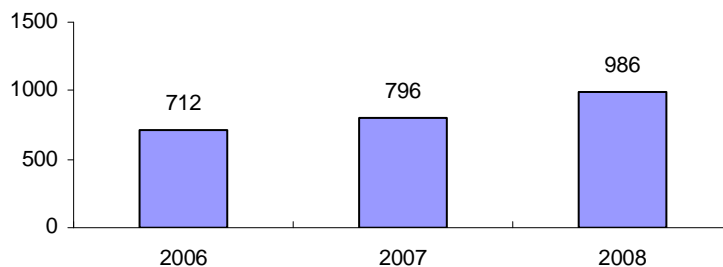
W podsumowaniu należy stwierdzić, że w porównaniu do poprzedniego okresu sprawozdawczego wzrosła liczba spraw, w których organ skierował zawiadomienia o podejrzeniu popełnienia przestępstwa. Wynika to niewątpliwie z pojawiania się coraz to nowych podmiotów trudniących się procederem bezprawnego gromadzenia danych. Sytuacja ta wymusza na Generalnym Inspektorze Ochrony Danych Osobowych intensyfikację działań w zakresie propagowania przestrzegania przepisów o ochronie danych osobowych oraz bardziej stanowcze i skrupulatne egzekwowanie od tych podmiotów przestrzegania przepisów ustawy.

Liczbę **zawiadomień o popełnieniu przestępstwa** składanych przez Generalnego Inspektora w latach 2006–2008 obrazuje Wykres 3.



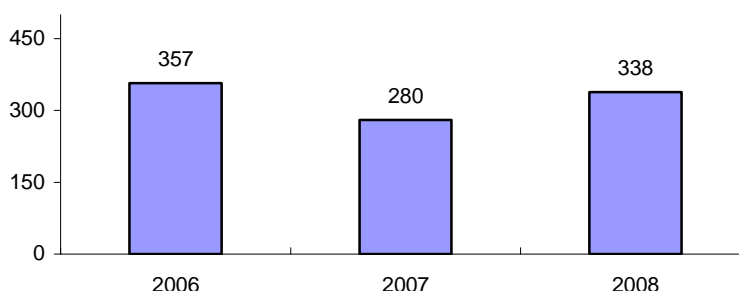
Wykres 3.
Porównanie liczby zawiadomień o popełnieniu przestępstwa kierowanych przez GIO w latach 2006–2008.

W 2008 r. do Departamentu Orzecznictwa, Legislacji i Skarg wpłynęło **986 skarg** dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2007, liczba ta uległa zwiększeniu, co przedstawia Wykres 4.



Wykres 4.
Liczbowe zestawienie skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006–2008.

W postępowaniach zainicjowanych tymi skargami wydanych zostało **338 decyzji administracyjnych**, z których 69 zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie [WSA] lub Naczelnego Sądu Administracyjnego (zał. 4).



Wykres 5.
Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008 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 2008 roku obejmował następujące obszary: 1) administracja publiczna, 2) System Informacyjny Schengen (SIS), 3) sądy, prokuratura, Policja, komornicy, 4) banki i inne instytucje finansowe, 5) marketing, 6) sektor mieszkalnictwa, 7) ubezpieczenia społeczne, majątkowe i osobowe, 8) telekomunikacja, 9) sektor zatrudnienia i 10) inne.

3.2. Decyzje w wybranych obszarach

3.2.1 Administracja publiczna

W 2008 r. do Biura Generalnego Inspektora wpłynęło 110 spraw z tego sektora. Podobnie jak w latach ubiegłych, wiele spraw dotyczyło przypadków udostępnienia danych osobowych na stronach internetowych urzędów gminy. W jednej z takich spraw,³² na stronie internetowej Biuletynu Informacji Publicznej [BIP] Gminy Lipowa, ujawniono oświadczenia majątkowe przewodniczącego Rady Gminy Lipowa oraz Wójta Gminy Lipowa. Ponadto znalazły się tam oświadczenia majątkowe kierowników jednostek organizacyjnych oraz radnych Gminy Lipowa w całości, a więc z częścią B tych oświadczeń, zawierającą dane osobowe w zakresie adresów zamieszkania oraz miejsca położenia nieruchomości wymienionych w punkcie II części A (adres). Generalny Inspektor Ochrony Danych Osobowych wystąpił do Wójta Gminy wskazując, że dane osobowe składającego oświadczenie zawarte w części B oświadczenia majątkowego są tajne i nie mogą być upubliczniane w BIP. Takie działanie nie ma umocowania w przepisach prawa i jest niezgodne z ustawą o ochronie danych osobowych.³³ Informacje zawarte w oświadczeniu majątkowym są jawne, z wyłączeniem informacji o adresie zamieszkania

³² DOLiS-440-32/08.

³³ Kwestie dotyczące składania oświadczeń majątkowych przez pracowników wydających decyzje w imieniu wójta (prezydenta miasta), w tym ich treść i warunki ujawniania, regulują przepisy ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.) oraz wydanego na jej

składającego oświadczenie oraz o miejscu położenia nieruchomości.³⁴ W toku postępowania Wójt Gminy Lipowa wskazał, iż powyższe upublicznienie oświadczeń majątkowych w całości było wynikiem błędu nowo zatrudnionego pracownika Urzędu, któremu udzielono upomnienia,³⁵ zaś kwestionowane dane w zakresie części B ww. oświadczeń majątkowych zostały usunięte z Biuletynu Informacji Publicznej Urzędu Gminy. W tej sprawie Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Wójta Gminy o podjęcie odpowiednich działań mających na celu wyeliminowanie tego typu zdarzeń w przyszłości, w szczególności poprzez przeszkolenie podległych Wójtowi Gminy pracowników z zakresu ustawy o ochronie danych osobowych oraz przepisów dotyczących zamieszczania informacji w Biuletynie Informacji Publicznej, a także wprowadzenie i stosowanie odpowiednich środków technicznych i organizacyjnych, w tym odpowiednich procedur, które zapobiegą bezpodstawnemu ujawnianiu danych osób składających oświadczenie.³⁶ W odpowiedzi na to wystąpienie Wójt Gminy poinformował GODO o przeszkoleniu pracowników we wskazanym przez organ zakresie.³⁷

W roku sprawozdawczym 2008 GODO stwierdził także inne przypadki ujawniania danych osobowych w Biuletynie Informacji Publicznej organów administracji publicznej, w szczególności ujawniania treści uchwał rady miasta zawierających dane osoby, której uchwała dotyczyła. W jednej z takich spraw³⁸ zarzucono bezprawne ujawnienie danych osobowych przez Burmistrza Pisz, w opublikowanej na stronie internetowej BIP uchwale Rady Miejskiej w Pisz. Uchwała ta została podjęta w związku z podejrzeniem popełnienia przestępstwa przy przydziale lokalu komunalnego osobom skarżącym i zobowiązywała Burmistrza Pisz do skierowania do prokuratury stosownego zawiadomienia.³⁹ Jako podstawę opublikowania uchwały zawierającej dane osobowe osób skarżących w BIP, Burmistrz Pisz wskazał przepisy ustawy o dostępie do informacji publicznej.⁴⁰ Generalny Inspektor Ochrony Danych Osobowych uznał, że udostępnienie na stronie internetowej BIP danych osobowych zawartych w ww. uchwale w zakresie imion i nazwisk osób skarżących, naruszało nie tylko zasadę adekwatności w procesie przetwarzania danych osobowych, ale także ich prawo do prywatności, które nie podlega wyłączeniu przy stosowaniu ustawy o dostępie do informacji publicznej. Zwłaszcza że osoby skarżące z tego prawa same nie zrezygnowały. Zdaniem organu ds. ochrony danych osobowych, przy upublicznieniu uchwały jedynie w celach informacyjnych zbędne było (nieadekwatne do celu) ujawnianie imion i nazwisk osób skarżących. Publikacja dokumentu zawierającego dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna nastąpić po odpowiednim przetworzeniu tych danych. W omawianej sprawie oznacza to, że uchwała Rady Miejskiej w Pisz powinna zostać upubliczniona po uprzednim usunięciu danych osób skarżących w zakresie ich imion i nazwisk. W ocenie Generalnego Inspektora, pozostawienie w treści uchwały jedynie adresu, którego ta uchwała dotyczy, nie naruszałoby obowiązku informacyjnego wynikającego z ustawy o dostępie do informacji publicznej i zarazem zapewniałoby ochronę prawa do prywatności z uwzględnieniem zasady adekwatności. W konsekwencji Generalny Inspektor Ochrony Danych Osobowych nakazał Burmistrzowi Pisz wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych osób skarżących poprzez usunięcie ze strony internetowej BIP ich danych osobowych w zakresie imion i nazwisk.⁴¹ Stanowisko organu zostało potwierdzone orzeczeniem Wojewódzkiego Sądu Administracyjnego w Warszawie, który oddalił skargę Burmistrza Pisz na decyzję organu ochrony danych osobowych.⁴²

W innej ze spraw⁴³ Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną,⁴⁴ na mocy której odmówił uwzględnienia wniosku o uznanie za nielegalne przekazanie przez Ministra Spraw Wewnętrznych i Administracji danych osobowych

podstawie rozporządzenia Prezesa Rady Ministrów z dnia 26 lutego 2003 r. w sprawie określenia wzorów formularzy oświadczeń majątkowych radnego gminy, wójta, zastępcy wójta, sekretarza gminy, skarbnika gminy, kierownika jednostki organizacyjnej gminy, osoby zarządzającej i członka organu zarządzającego gminą osobą prawną oraz osoby wydającej decyzje administracyjne w imieniu wójta (Dz. U. Nr 34, poz. 282 z późn. zm.). Na mocy art. 24 h ust. 1 ustawy o samorządzie gminnym, radny, wójt, zastępca wójta, sekretarz gminy, skarbnik gminy, kierownik jednostki organizacyjnej gminy, osoba zarządzająca i członek organu zarządzającego gminą osobą prawną oraz osoba wydająca decyzje administracyjne w imieniu wójta, są obowiązani do złożenia oświadczenia o swoim stanie majątkowym, które dotyczy ich majątku odrębnego oraz majątku objętego małżeńską wspólnością majątkową. Z przepisów art. 24 h ust. 3 pkt 3 i art. 24 h ust. 6 wynika, że pracownik wydający decyzje w imieniu wójta (prezydenta miasta) składa oświadczenie wójtowi (prezydentowi miasta), który dokonuje jego analizy, przekazuje jeden egzemplarz urzędowi skarbowemu i następnie przechowuje przez 6 lat. Jawne informacje zawarte w oświadczeniach majątkowych są udostępniane w Biuletynie Informacji Publicznej, o którym mowa w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. Nr 112, poz. 1198 z późn. zm.).

³⁴ Art. 24i ust. 1 ustawy o samorządzie gminnym.

³⁵ Pismo z dnia 6 lutego 2008 r. znak: 071/5/2008.

³⁶ Pismo z dnia 11 marca 2008 r. o sygn. DOLiS-440-32/08/6424.

³⁷ Pismo Wójta Gminy z dnia 25 marca 2008 r. znak 071/5/2008.

³⁸ Np. DOLiS-440-41/08.

³⁹ Uchwała Nr XVIII/186/07 Rady Miejskiej w Pisz z dnia 28 grudnia 2007 r.

⁴⁰ Art. 6 ust. 1 pkt 4 lit. a w związku z art. 7 ust. 1 pkt 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.).

⁴¹ Decyzja z dnia 17 kwietnia 2008 r. o sygn. DOLiS/DEC-246/08/9939,9942.

⁴² Wyrok WSA w Warszawie z dnia 18 listopada 2008 r. sygn. akt II SA/Wa 1177/08.

⁴³ DOLiS-440-8/07.

skarżących pochodzących z Centralnej Ewidencji Pojazdów i Kierowców podmiotowi zajmującemu się odzyskiwaniem wierzytelności. Udostępnienie znajdowało bowiem podstawę w przepisie art. 80c ust. 4 Prawa o ruchu drogowym⁴⁵ i uzasadnione było interesem prawnym spółki, gdyż dane udostępniono jej w celu podjęcia wobec dłużnika działań prawnych zmierzających do odzyskania wierzytelności.

W omawianym okresie Generalny Inspektor Ochrony Danych Osobowych prowadził również sprawę,⁴⁶ w której nakazał staroście powiatu usunięcie z dokumentacji dotyczącej skargi na powiatowego rzecznika konsumentów, danych osoby skarżącej (daty i miejsca urodzenia, imienia ojca, adresu zamieszkania na pobyt stały, numeru PESEL, serii i numeru dowodu osobistego), jako zebranych bez podstawy prawnej.⁴⁷ Wydając decyzję, GODO stwierdził, że zakres danych, jaki można zebrać w związku z przyjęciem skargi składanej ustnie, został mocą przepisu prawa⁴⁸ ograniczony do imienia, nazwiska i adresu osoby zgłaszającej skargę i nakazał usunięcie danych w zakresie wykraczającym poza katalog wynikający z tego przepisu. Zdaniem organu, zebranie danych w zakresie szerszym niż to przewidują obowiązujące przepisy było nieuprawnione.

Generalny Inspektor Ochrony Danych Osobowych prowadził również postępowanie w sprawie, w której Burmistrz Rogoźna opublikował na stronie internetowej urzędu miejskiego swoją korespondencję zawierającą dane osobowe skarżących.⁴⁹ Generalny Inspektor Ochrony Danych Osobowych w wystąpieniu⁵⁰ do Burmistrza wskazał, że publikacja listu, który zawiera dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna nastąpić po odpowiednim przetworzeniu danych osobowych w nim zawartych. List ten mógł zostać upubliczniony po uprzednim usunięciu z zakresu danych osobowych skarżących ich adresu zamieszkania. W konsekwencji działań podjętych przez GODO kwestionowane dane osobowe zostały usunięte przez Burmistrza ze strony internetowej. Podmiot ten w odpowiedzi na wystąpienie organu poinformował o pouczeniu Administratora Bezpieczeństwa Informacji o obowiązku zastosowania środków technicznych i organizacyjnych zapewniających odpowiednią ochronę przetwarzanych danych osobowych, jak również o skierowaniu tego pracownika na szkolenie z zakresu przygotowywania polityki bezpieczeństwa informacji.⁵¹ W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych umorzył postępowanie w tej sprawie.⁵² Skarżący jednak nie zgodzili się z tym rozstrzygnięciem – obecnie sprawa rozpatrywana jest przez Wojewódzki Sąd Administracyjny w Warszawie.

W innej sprawie⁵³ Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną⁵⁴ nakazującą dyrektorowi izby wytrzeźwień udostępnienie miejskiemu ośrodkowi pomocy społecznej danych osobowych osoby, wobec której prowadzone było postępowanie o przyznanie świadczeń z tytułu pomocy społecznej. Chodziło o informacje, czy i w jakim okresie osoba ta przebywała w izbie. GODO stanął w tej sprawie na stanowisku, iż informacji tych nie należy zaliczać do kategorii szczególnie chronionych, tj. danych o nałogu, czy orzeczeniu wydanym w postępowaniu sądowym lub administracyjnym. Udostępnienie ich było dopuszczalne na podstawie art. 23 ust. 1 pkt 2 ustawy, jako niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 11 ustawy o pomocy społecznej⁵⁵ – stanowiący podstawę weryfikacji i ew. odmowy

⁴⁴ Decyzja z dnia 8 lutego 2008 r. o sygn. DOLiS/DEC-113/08.

⁴⁵ Zgodnie z art. 80c ust. 4 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. z 2005 r. Nr 108, poz. 908 z późn. zm.), minister właściwy do spraw administracji publicznej może udostępnić dane lub informacje zgromadzone w ewidencji innym podmiotom niż wymienione w ust. 1-3, w tym osobom fizycznym, osobom prawnym lub jednostkom organizacyjnym nieposiadającym osobowości prawnej, jeżeli wykażą swój uzasadniony interes.

⁴⁶ DOLiS-441-3/07.

⁴⁷ Decyzja z dnia 13 marca 2008 r. o sygn. DOLiS/DEC-179/08.

⁴⁸ § 6 ust. 2 rozporządzenia Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków (Dz. U. Nr 5, poz. 46 z późn. zm.).

⁴⁹ DOLiS-440-495/08.

⁵⁰ Pismo z dnia 24 września 2008 r. o sygn. DOLiS-440-495/08/25095.

⁵¹ Pismo Burmistrza z dnia 27 października 2008 r. znak: Nr.OR.5242/1/2008.

⁵² Decyzja z dnia 19 grudnia 2008 r. o sygn. DOLiS/DEC-860/08.

⁵³ DOLiS-440-130/08.

⁵⁴ Decyzja z dnia 8 kwietnia 2008 r. o sygn. DOLiS/DEC-228/08.

⁵⁵ Art. 11 ustawy z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. 2008 r. Nr 115 poz. 728 z późn. zm.) stanowi, iż w przypadku stwierdzenia przez pracownika socjalnego marnotrawienia przyznanych świadczeń, ich celowego niszczenia lub korzystania w sposób niezgodny z przeznaczeniem bądź marnotrawienia własnych zasobów finansowych, może nastąpić ograniczenie świadczeń, odmowa ich przyznania albo przyznanie pomocy w formie świadczenia niepieniężnego (ust. 1). Brak współdziałania osoby lub rodziny z pracownikiem socjalnym w rozwiązywaniu trudnej sytuacji życiowej, odmowa zawarcia kontraktu socjalnego, niedotrzymywanie jego postanowień, nieuzasadniona odmowa podjęcia zatrudnienia, innej pracy zarobkowej przez osobę bezrobotną lub wykonywania prac społecznie użytecznych, o których mowa w przepisach o promocji zatrudnienia i instytucjach rynku pracy, lub nieuzasadniona odmowa podjęcia leczenia odwykowego w zakładzie leczenia odwykowego przez osobę uzależnioną mogą stanowić podstawę do odmowy przyznania świadczenia, uchylecia decyzji o przyznaniu świadczenia lub wstrzymania świadczeń pieniężnych z pomocy społecznej (ust. 2). W przypadku odmowy przyznania albo ograniczenia wysokości lub rozmiaru świadczeń z pomocy społecznej należy uwzględnić sytuację osób będących na utrzymaniu osoby ubiegającej się o świadczenie lub korzystającej ze świadczeń (ust. 3).

udzielenia świadczenia pomocy społecznej, jak i art. 105 tejże ustawy⁵⁶ – z którego wynika zasada mówiąca o możliwości udostępniania przez sądy, organy i jednostki organizacyjne odpowiednich informacji, jeśli mają znaczenie dla rozstrzygnięcia o przyznaniu lub wysokości świadczeń z pomocy społecznej).

Podobnie jak w latach ubiegłych, do GODO wpływały liczne skargi dotyczące nieprawidłowości w przetwarzaniu przez urzędy gmin danych zawartych w ewidencji działalności gospodarczej.⁵⁷ W każdej z takich spraw Generalny Inspektor Ochrony Danych Osobowych wskazywał na wynikającą z ustawy Prawo działalności gospodarczej⁵⁸ zasadę jawności ww. ewidencji oraz wyłączenia stosowania ustawy o ochronie danych osobowych wobec przedsiębiorców w rozumieniu ustawy o swobodzie działalności gospodarczej.⁵⁹

Prowadząc sprawy z tego sektora, Generalny Inspektor Ochrony Danych Osobowych stwierdził ponadto przesłanki do skierowania do prokuratury zawiadomienia o podejrzeniu popełnienia przestępstwa⁶⁰ z art. 49 ust. 1 ustawy. W jednej z takich spraw⁶¹ ustalił, iż dyrektor urzędu kontroli skarbowej wykorzystał dane osoby skarżącej i jej małżonka z systemu POLTAX dla potrzeb postępowania dyscyplinarnego prowadzonego wobec skarżącej. Uznano, że ww. dyrektor wykorzystał przedmiotowe dane niezgodnie z celem, dla którego zostały one pozyskane, tj. nie dla realizacji zadań wynikających z ustawy o kontroli skarbowej. Naruszył więc art. 23 ust. 1 pkt 2 w zw. z art. 26 ust. 1 pkt 2 ustawy.⁶² Prokuratura umorzyła śledztwo w przedmiotowej sprawie.⁶³

GODO skierował do prokuratury zawiadomienie o podejrzeniu popełnienia przez osoby odpowiedzialne za przetwarzanie danych osobowych nauczycieli, przestępstwa określonego w art. 52 ustawy,⁶⁴ polegającego na naruszeniu obowiązku zabezpieczenia danych.⁶⁵ Skarga dotyczyła zagubienia przez wójta gminy danych osobowych nauczycieli zawartych we wnioskach o wydanie legitymacji służbowej nauczyciela. Prokuratura odmówiła wszczęcia dochodzenia w tej sprawie.⁶⁶ Na skutek zaskarżenia tego stanowiska przez Generalnego Inspektora Ochrony Danych Osobowych, organy ścigania wszczęły ponownie dochodzenie, które następnie zostało umorzone.⁶⁷

W 2008 r. Generalny Inspektor Ochrony Danych Osobowych prowadził także sprawę, w toku której wystąpił do Dyrektora Wojewódzkiej Izby Celnej⁶⁸ o zmianę praktyki niezgodnego z prawem pozyskiwania danych o karalności oraz o stanie zdrowia, podczas spisywania protokołu osoby podejrzanej o popełnienie wykroczenia. Organ zwrócił w swoim wystąpieniu uwagę na to, że pozyskiwanie takich danych nie znajduje podstaw prawnych oraz powoduje naruszenie zasady merytorycznej poprawności i adekwatności danych do celu, dla którego są pozyskiwane, tj. art. 26 ust. 1 pkt 3 ustawy. W odpowiedzi na to wystąpienie Dyrektor Wojewódzkiej Izby Celnej poinformował, iż zobowiązał podległych mu funkcjonariuszy do zaniechania kwestionowanej praktyki oraz nakazał przeprowadzenie w przedmiotowym zakresie szkoleń wewnętrznych.⁶⁹

Generalny Inspektor Ochrony Danych Osobowych wystąpił również do dyrektora jednego z miejskich ośrodków pomocy społecznej [MOPS] o każdorazowe rozważanie potrzeby udostępniania danych osobowych osób korzystających z pomocy społecznej innym podmiotom, realizującym na ich rzecz świadczenia finansowe ze środków pomocy społecznej. Każde bowiem nieuzasadnione udostępnienie danych może narażać MOPS na zarzut naruszenia zarówno ustawy o ochronie danych osobowych,

⁵⁶ Zgodnie z art. 105 ww. ustawy, sądy, organy i jednostki organizacyjne są obowiązane niezwłocznie, nie później jednak niż w terminie 7 dni, udostępnić lub udzielić na wniosek pracownika socjalnego odpowiednich informacji, które mają znaczenie dla rozstrzygnięcia o przyznaniu lub wysokości świadczeń z pomocy społecznej.

⁵⁷ Np. DOLiS-440-322/08.

⁵⁸ Zgodnie z art. 7 ust. 2 ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej (Dz. U. z 1999 r. Nr 101, poz. 1178 z późn. zm.), ewidencja działalności gospodarczej jest jawna i dane osobowe w niej zawarte nie podlegają przepisom ustawy o ochronie danych osobowych.

⁵⁹ Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095 z późn. zm.).

⁶⁰ Zawiadomienie z dnia 26 lutego 2008 r. o sygn. DOLiS/ZAW-2/08.

⁶¹ DOLiS-430/380/07.

⁶² Zgodnie z art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Zgodnie z art. 26 ust. 1 pkt 2 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 zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2.

⁶³ Postanowienie prokuratury z dnia 31 grudnia 2008 r. o sygn. 4Ds.305/08.

⁶⁴ Zgodnie z art. 52 ustawy o ochronie danych osobowych, 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 do roku.

⁶⁵ Zawiadomienie z dnia 17 lipca 2008 r. o sygn. DOLiS/ZAW-15/08.

⁶⁶ Postanowienie Prokuratury z dnia 28 sierpnia 2008 r. o sygn. 2Ds1057/08.

⁶⁷ Postanowienie Prokuratury z dnia 14 maja 2009 r. o sygn. 2Ds 669/09/D.

⁶⁸ Sygnalizacja z dnia 29 kwietnia 2008 r. o sygn. DOLiS-440-245/08.

jak i ustawy o pomocy społecznej.⁷⁰ W odpowiedzi na to wystąpienie Dyrektor MOPS poinformował o uwzględnieniu uwag GIODO poprzez wprowadzenie procedur umożliwiających realizację zadań ośrodka w postaci przyznawania pomocy społecznej bez przekazywania danych osobowych klientów innym podmiotom.⁷¹

W roku sprawozdawczym 2008 organ ds. ochrony danych osobowych interweniował także w sprawie pozyskiwania przez Burmistrza Miasta Wielunia danych osobowych w formularzu *wniosku o ustalenie warunków zabudowy lub lokalizacji inwestycji celu publicznego*, w zakresie imion, nazwisk i adresów zamieszkania właścicieli działek sąsiednich w stosunku do działek wnioskodawcy (inwestora). Jako podstawę prawną żądania ww. danych Burmistrz wskazał art. 28 K.p.a., przerzucając w ten sposób na wnioskodawcę obowiązek podania danych właścicieli działek sąsiadujących z działką inwestora. Generalny Inspektor Ochrony Danych Osobowych stanął na stanowisku, że art. 28 K.p.a. powinien być stosowany łącznie z art. 52 ustawy o planowaniu i zagospodarowaniu przestrzennym.⁷² Tymczasem przepis ten nie przewiduje, aby wniosek miał zawierać dane osobowe właścicieli działek sąsiadujących z działką przeznaczoną do inwestycji. Zgodnie z ust. 1 i 2 powołanego przepisu, ustalenie lokalizacji inwestycji celu publicznego następuje na wniosek inwestora, a wniosek ten powinien zawierać: 1) określenie granic terenu objętego wnioskiem, przedstawionych na kopii mapy zasadniczej lub, w przypadku jej braku, na kopii mapy katastralnej, przyjętych do państwowego zasobu geodezyjnego i kartograficznego, obejmujących teren, którego wniosek dotyczy, i obszaru, na który ta inwestycja będzie oddziaływać, w skali 1:500 lub 1:1000, a w stosunku do inwestycji liniowych również w skali 1:2000; 2) charakterystykę inwestycji, obejmującą: a) określenie zapotrzebowania na wodę, energię oraz sposobu odprowadzania lub oczyszczania ścieków, a także innych potrzeb w zakresie infrastruktury technicznej, a w razie potrzeby również sposobu unieszkodliwiania odpadów, b) określenie planowanego sposobu zagospodarowania terenu oraz charakterystyki zabudowy i zagospodarowania terenu, w tym przeznaczenia i gabarytów projektowanych obiektów budowlanych, przedstawione w formie opisowej i graficznej, c) określenie charakterystycznych parametrów technicznych inwestycji oraz dane charakteryzujące jej wpływ na środowisko. W odpowiedzi na wystąpienie Generalnego Inspektora Ochrony Danych Osobowych,⁷³ Burmistrz Wielunia poinformował, iż uwzględnił uwagi organu i usunął ze wspomnianego formularza część dotyczącą danych osobowych właścicieli działek sąsiadujących z działką wnioskodawcy.

Analiza dotycząca działalności organu ochrony danych osobowych w sektorze „administracja publiczna” wykazuje, że najczęściej pojawiającym się problemem było zbyt liberalne podejście administratorów danych osobowych (organów administracji publicznej) do kwestii dostępu do informacji publicznych zawierających dane osobowe przetwarzane przez konkretny organ administracji, w związku z podejmowanymi działaniami. Realizując obowiązek ujawniania informacji o sprawach publicznych, administratorzy danych pomijają fakt istnienia prawa wynikającego z ustawy o ochronie danych osobowych. Poza tym do GIODO nadal wpływały skargi, których przyczyną było błędne przekonanie 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 osobowych.⁷⁴

Dodać również trzeba, że na podstawie analizy treści skarg rozpatrywanych w latach 2007 – 2008 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 zanik przypadków nieuzasadnionego wykorzystywania tych uregulowań jako przeszkody w bezzwłocznym załatwieniu konkretnej sprawy administracyjnej.

⁶⁹ Pismo z dnia 29 maja 2008 r. znak: 330000-WOP-0561-16/2007/2008.

⁷⁰ Wystąpienie z dnia 11 września 2008 r. o sygn. GI-DS-430/634/05.

⁷¹ Pismo Dyrektora MOPS z dnia 25 listopada 2008 r. znak: MOPS/S/K/3/2008.

⁷² Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. Nr 80. poz. 717 z późn. zm.)

⁷³ Pismo z dnia 2 października 2008 r. o sygn. DOLIS-440-502/08/26006.

⁷⁴ 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).

3.2.2 System Informacyjny Schengen (SIS)

Wraz z przystąpieniem Polski w dniu 21 grudnia 2007 r. do strefy Schengen, pojawiła się kwestia kontroli prawidłowości przetwarzania danych osobowych w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej. Z art. 8 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej⁷⁵ wynika, iż Generalny Inspektor Ochrony Danych Osobowych sprawuje kontrolę nad tym, czy wykorzystanie danych nie narusza praw osób, których dane dotyczą. Wspomniana kontrola, odbywa się na zasadach uregulowanych w ustawie o ochronie danych osobowych.

W 2008 roku, Generalny Inspektor Ochrony Danych Osobowych rozpatrzył **7 spraw** z tego sektora. Dotyczyły one sytuacji, w której służby graniczne jednego z państw Strefy odmówiły cudzoziemcowi figurującemu w Systemie Informacyjnym Schengen jako „osoba niepożądana”, wjazdu na teren Unii Europejskiej.⁷⁶ W jednej ze spraw Generalny Inspektor Ochrony Danych Osobowych ustalił, iż dane zostały wprowadzone do SIS przez Urząd do Spraw Cudzoziemców na podstawie art. 125 ust. 3 w związku z art. 128 i art. 134a pkt 2 ustawy o cudzoziemcach.⁷⁷ Tym samym organ stwierdził w tej sprawie zastosowanie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych i nie nakazał usunięcia z SIS danych osobowych osoby skarżącej.

Natomiast w dwóch innych sprawach z tego sektora dane osobowe obywatela polskiego zostały wprowadzone do SIS przez organy innych państw. W jednej z nich, wskutek wszczęcia postępowania wyjaśniającego i zwrócenia się o wyjaśnienia do organu ochrony danych osobowych obcego państwa, dane te zostały usunięte, ponieważ upłynął terminu, na który zostały tam wprowadzone.⁷⁸ W drugiej z rozpatrywanych tego typu spraw, wskutek wszczęcia przez organ ochrony danych osobowych postępowania wyjaśniającego, strona (obce państwo) odpowiedzialna za wpis usunęła dane osobowe z SIS.

3.2.3 Sądy, prokuratura, Policja, komornicy

W 2008 r. wpłynęły **24 skargi** dotyczące tego sektora. Wśród nich pojawiła się kwestia⁷⁹ pozyskiwania przez komornika sądowego informacji dotyczących osoby skarżącej oraz członków jej rodziny i żądania w trybie art. 761 § 1 K.p.c.⁸⁰ od uczestników postępowania egzekucyjnego oraz organów administracji publicznej informacji odnośnie nieruchomości stanowiących własność osoby skarżącej oraz jej rodziców.

Przy analizowaniu tego problemu Generalny Inspektor Ochrony Danych Osobowych wziął pod uwagę stanowisko Sądu Najwyższego, zgodnie z którym użyte w art. 761 § 1 K.p.c. sformułowanie *informacji niezbędnej do prowadzenia egzekucji*, należy rozumieć jako prawo żądania przez komornika udzielenia informacji potrzebnej do prawidłowego przeprowadzenia egzekucji. Nie ulega zaś wątpliwości, że do zakresu takich informacji należy ustalenie, czy to dłużnik jest właścicielem zajętej rzeczy, czy też osoba trzecia, a także, czy osobie tej przysługuje w stosunku do zajętej rzeczy inne uprawnienie, pozwalające na zgłoszenie żądania zwolnienia zajętego przedmiotu z egzekucji. Można wręcz powiedzieć, że tego typu informacje i ustalenia należą do fundamentalnych, gdyż w przeciwnym razie mogłoby dojść do zlicytowania przedmiotu należącego do osoby trzeciej, a nie do dłużnika”.⁸¹

⁷⁵ Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz. U. Nr 165, poz. 1170 z późn. zm.).

⁷⁶ Np. DOLiS-440-732/08, DOLiS-440-685/08.

⁷⁷ Zgodnie z art. 125 ust. 3 ustawy o cudzoziemcach, wskazany w art. 124 pkt 4 tej ustawy wykaz cudzoziemców, których pobyt na terytorium Rzeczypospolitej Polskiej jest niepożądany, prowadzi Szefer Urzędu do Spraw Cudzoziemców.

⁷⁸ DOLiS-440-164/08.

⁷⁹ DOLiS-440-6/08.

⁸⁰ Zgodnie z art. 761 § 1 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.), organ egzekucyjny może żądać od uczestników postępowania złożenia wyjaśnień oraz zasięgać od organów administracji publicznej, organów wykonujących zadania z zakresu administracji publicznej, organów podatkowych, organów rentowych, banków, spółdzielczych kas oszczędnościowo-kredytowych, przedsiębiorstw maklerskich, organów spółdzielni mieszkaniowych, zarządów wspólnot mieszkaniowych oraz innych podmiotów zarządzających mieszkaniem i lokalami użytkowymi, jak również innych instytucji i osób nieuczestniczących w postępowaniu, informacji niezbędnych do prowadzenia egzekucji.

⁸¹ Tak w wyroku Sądu Najwyższego – Izba Cywilna z dnia 6 kwietnia 2006 r. sygn. akt IV CSK 6/2006.

Na gruncie tej sprawy pojawił się również problem tajemnicy komorniczej unormowanej w art. 20 ust. 1 ustawy o komornikach sądowych i egzekucji⁸² i zastosowania tych przepisów w związku z art. 5 ustawy o ochronie danych osobowych.⁸³ Generalny Inspektor Ochrony Danych Osobowych uznał, że ustawa o komornikach sądowych i egzekucji nie przewiduje bardziej rygorystycznych wymogów udostępniania danych osobowych, nie zapewnia większej ochrony prywatności osób fizycznych, niż ustawa o ochronie danych osobowych. Tajemnica komornicza nie spełnia tym samym wymogów określonych w art. 5 ustawy o ochronie danych osobowych, tj. nie zapewnia dalej idącej ochrony. W związku z tym Generalny Inspektor Ochrony Danych Osobowych odmówił uwzględnienia wniosku osoby skarżącej.⁸⁴

W 2008 roku Generalny Inspektor Ochrony Danych Osobowych wszczął ponadto postępowanie w dotyczące wpisywania przez prokuraturę rejonową na stronie adresowej kopert sygnatury akt oraz informacji o przedmiocie pisma (postanowienia, zawiadomienia).⁸⁵ W ten sposób uwiadczane były informacje o przedmiocie postępowania, jak „postanowienie o zatrzymaniu prawa jazdy”, „zawiadomienie o skierowaniu aktu oskarżenia do sądu”, „odpis postanowienia o zabezpieczeniu majątkowym”. Taki sposób umieszczania informacji na kopercie prowadził do ujawnienia osobom trzecim treści przesyłki, a tym samym do naruszenia istotnej sfery prywatności jej adresata. W ocenie Generalnego Inspektora Ochrony Danych Osobowych działanie takie naruszało przepisy dwóch ustaw, a mianowicie Kodeksu postępowania karnego i ustawy o ochronie danych osobowych.

Mając na uwadze, że kwestionowana praktyka dotyczyć mogła nie tylko jednej, ale wielu prokuratur w kraju, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Ministra Sprawiedliwości o podjęcie działań mających na celu zaniechanie umieszczania na kopertach informacji o treści pisma.⁸⁶ Organ ds. ochrony danych osobowych zauważył, że art. 23 ust. 1 ustawy o ochronie danych osobowych określa warunki przetwarzania danych, stwierdzając w szczególności, że przetwarzanie danych jest dopuszczalne wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Tymczasem, zgodnie z art. 7 Konstytucji RP, organy władzy publicznej działają na podstawie i w granicach prawa, natomiast sposób doręczania pism w postępowaniu karnym określa art. 128 § 2 Kodeksu postępowania karnego, stanowiący, że wszelkie pisma przeznaczone dla uczestników postępowania doręcza się w taki sposób, by treść ich nie była udostępniona osobom niepowołanym.

W odpowiedzi na ww. wystąpienie Zastępcy Prokuratora Generalnego poinformował, iż przypadki oznaczania na kopercie rodzaju pisma wysyłanego do stron procesowych lub innych uczestników postępowania zostaną wyeliminowane „jako niezasadne”.⁸⁷

W omawianym okresie rozpatrywana była także skarga na odmowę udostępnienia adresów zamieszkania sędziów sądu rejonowego.⁸⁸ W tej sprawie wnioskodawca nie uzasadnił w sposób wiarygodny potrzeby posiadania danych. Osoba skarżąca nie wykazała w swoim wniosku do administratora danych – Prezesa Sądu Rejonowego dla m. st. Warszawy – celu, w jakim dane te miałyby być wykorzystane. W uzasadnieniu stwierdzono jedynie, że „udostępnienie adresów zamieszkania na podstawie przywołanych przepisów (art. 29 ust. 2 i 3 ustawy o ochronie danych osobowych⁸⁹) jest dozwolone, w przypadku wskazania, iż są one niezbędne do wystąpienia przeciwko ww. osobom na drogę sądową.” Cytowane uzasadnienie nie dawało podstaw do wydania przez organ nakazu udostępnienia danych osobowych, dlatego organ odmówił uwzględnienia wniosku.⁹⁰

W innej ze spraw z tego sektora, ocenie organu poddana została kwestia legalności przetwarzania danych osobowych osoby skarżącej zawartej w wyroku sądowym.⁹¹ Impulsem do takiej oceny była skarga na nieuprawnione przetwarzanie przez

⁸² Zgodnie z art. 20 ust. 1 ustawy o komornikach sądowych i egzekucji, komornik jest obowiązany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na wykonywane czynności. Obowiązek, o którym mowa w ust. 1, trwa także po odwołaniu komornika (ust. 2). Obowiązek zachowania tajemnicy ustaje, gdy komornik składa zeznanie jako świadek lub strona przed sądem lub prokuratorem, chyba że ujawnienie tajemnicy zagraża dobru państwa. W tym przypadku od obowiązku zachowania tajemnicy może zwolnić komornika Minister Sprawiedliwości (ust. 3).

⁸³ Zgodnie z art. 5 ustawy o ochronie danych osobowych, jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

⁸⁴ Decyzja z dnia 24 października 2008 r. o sygn. DOLiS/DEC-691/08.

⁸⁵ DOLiS-440-208/08.

⁸⁶ Pismo z dnia 5 czerwca 2008 r. o sygn. DOLiS-440-208/08.

⁸⁷ Pismo z dnia 8 września 2008 r. znak: PR I 073-31/08.

⁸⁸ DOLiS-440-296/08.

⁸⁹ Zgodnie z art. 29 ust. 2 ustawy o ochronie danych osobowych, dane osobowe, z wyłączeniem danych, o których mowa w art. 27 ust. 1, mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w ust. 1, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Art. 29 ust. 3: dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

⁹⁰ Decyzja z dnia 1 sierpnia 2008 r. o sygn. DOLiS/DEC-462/08.

⁹¹ DOLiS-440-189/07.

komendanta wojewódzkiego policji danych osobowych skarżącego, zawartych we wcześniej wydanym wyroku sądu rejonowego, w związku z postępowaniem w sprawie cofnięcia skarżącemu pozwolenia na broń palną myśliwską. Skarżący zakwestionował legalność udostępnienia przez komendanta wspomnianego wyroku sądowego podmiotom nieuprawnionym - placówkom medycznym, które sporządziły opinie: lekarską i psychologiczną na potrzeby ww. postępowania - wskazując, że skazanie na podstawie ww. wyroku sądowego uległo zatarciu.

Po przeprowadzeniu postępowania administracyjnego organ wydał rozstrzygnięcie,⁹² w którym nie podzielił stanowiska osoby skarżącej. Znaczenie miał tu fakt, iż kwestionowane działania komendanta podejmowane było w ramach postępowania administracyjnego prowadzonego na podstawie Kodeksu postępowania administracyjnego i ustawy o broni i amunicji.⁹³ Tymczasem przepisy K.p.a. nie tylko uprawniają komendanta, lecz nakładają na niego obowiązek zebrania wyczerpującego materiału dowodowego w postępowaniu dotyczącym cofnięcia pozwolenia na broń. Natomiast kwestionowane wykorzystanie danych osobowych skarżącego utrwalonych w ww. wyroku sądowym miało na celu spełnienie powyższego obowiązku. Dlatego Generalny Inspektor Ochrony Danych Osobowych uznał działania komendanta za uprawnione w świetle przepisów ustawy.⁹⁴ Informacje zawarte w wyroku wykorzystane zostały jako dowód na to, iż osoba skarżąca dopuściła się w przeszłości określonych zachowań (tj. groził członkom rodziny użyciem broni palnej) nie zaś, że za czyny te została skazana. Informacja ta była istotna dla rozstrzygnięcia sprawy, zaś jej pominięcie mogłoby spowodować zarzut naruszenia art. 77 § 1 K.p.a.⁹⁵

Generalny Inspektor Ochrony Danych Osobowych badał również sprawę pozyskiwania przez prokuraturę danych osobowych w zakresie numeru PESEL, na potrzeby identyfikacji świadka przed rozpoczęciem składania przez niego zeznań.⁹⁶ W toku postępowania w tej sprawie organ ustalił, że pozyskując dane osobowe osoby skarżącej wraz z numerem PESEL, prokuratura opierała się na regulacjach zawartych m.in. w ustawie o prokuraturze,⁹⁷ ustawie o ewidencji ludności i dowodach osobistych⁹⁸ oraz rozporządzeniu Ministra Sprawiedliwości z dnia 27 sierpnia 2007 r. Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury. Z art. 3 ust. 1 pkt 5a ustawy o prokuraturze wynika, iż nałożone na Prokuratora Generalnego oraz podległych mu prokuratorów ustawowe zadania wykonywane są m.in. przez gromadzenie, przetwarzanie i analizowanie w systemach informatycznych danych, w tym danych osobowych, pochodzących z prowadzonych lub nadzorowanych na podstawie ustawy postępowań oraz z udziału w postępowaniu sądowym, administracyjnym, w sprawach o wykroczenia lub innych postępowaniach. Prawo do przetwarzania danych osobowych przez prokuraturę przewiduje również art. 44h ust. 1 pkt 1 wspomnianej wyżej ustawy o ewidencji ludności i dowodach osobistych. Zgodnie z tą regulacją, dane ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, organom administracji publicznej, sądom, prokuraturze. Podsumowując powyższe należy stwierdzić, że polski ustawodawca dopuszcza przetwarzanie przez prokuraturę danych osobowych, w tym numeru PESEL, o ile związane jest to z wykonywaniem przez tę instytucję zadań określonych w ustawie. Ponadto zgodnie z art. 191 § 1 K.p.k., przesłuchanie rozpoczyna się od zapytania świadka o imię, nazwisko, wiek, zajęcie, miejsce zamieszkania, karalność za fałszywe zeznanie lub oskarżenie oraz stosunek do stron. Z treści tego przepisu nie wynika, aby określał on zamknięty katalog danych, których można żądać od świadka rozpoczynając jego przesłuchanie. Generalny Inspektor Ochrony Danych Osobowych wziął również pod uwagę fakt, iż niewątpliwie pierwszorzędne znaczenie ma dla organu przesłuchującego ustalenie tożsamości osoby przesłuchiwanej ponad wszelką wątpliwość, a z art. 31a ust. 1 ustawy o ewidencji ludności i dowodach osobistych wynika, że funkcję taką spełnia numer PESEL, bowiem, jak stanowi ten przepis, jednoznacznie określa osobę fizyczną.

⁹² Decyzja z dnia 17 czerwca 2008 r. o sygn. DOLiS/DEC-365/08.

⁹³ Zgodnie z art. 9 ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. 2004 r. Nr 52, poz. 525 z późn. zm.), broń palną i amunicję do tej broni, z wyłączeniem przypadków, o których mowa w art. 11, można posiadać na podstawie pozwolenia na broń wydanego przez właściwego ze względu na miejsce stałego pobytu zainteresowanej osoby lub siedzibę zainteresowanego podmiotu komendanta wojewódzkiego Policji. W dalszych przepisach ustawy, określenie „właściwe organy Policji” odnosi się do organów upoważnionych do wydawania pozwoleń na broń lub karty rejestracyjnej broni, o których mowa w ust. 1-4 (art. 9 ust. 5 ustawy o broni i amunicji). Art. 18 ustawy o broni i amunicji wskazuje na przesłanki uzasadniające cofnięcie przez właściwy organ Policji pozwolenia na broń, natomiast art. 20 powołanego aktu prawnego stanowi wprost, że cofnięcie pozwolenia na broń dokonywane jest w formie decyzji administracyjnej. Art. 15 ust. 5 ustawy o broni i amunicji upoważnia organy Policji do żądania od osoby posiadającej pozwolenie na broń niezwłocznego poddania się badaniom lekarskim i psychologicznym i przedstawienia wydanych orzeczeń. Szczegółowy tryb i warunki wydawania ww. orzeczeń, i ich kwestionowania regulują przepisy stosownego rozporządzenia (art. 7 ustawy o broni i amunicji).

⁹⁴ Art. 27 ust. 2 pkt 2 ustawy.

⁹⁵ Zgodnie art. 77 § 1 K.p.a., organ administracji publicznej jest obowiązany w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy.

⁹⁶ DOLiS-440-603/08.

⁹⁷ Ustawa z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2008 r., Nr 7 poz. 39 z późn. zm.).

W celu pełnego wyjaśnienia sprawy Generalny Inspektor Ochrony Danych Osobowych przeanalizował również kwestię zastosowania Regulaminu wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury jako podstawy przetwarzania w toku postępowania przygotowawczego numeru PESEL osoby przesłuchiwanej w charakterze świadka. Zgodnie ze wspomnianym Regulaminem, przed przesłuchaniem (podczas postępowania dowodowego), sprawdza się dane osobowe przesłuchiwanego na podstawie dowodu osobistego lub innego dokumentu stwierdzającego tożsamość, czyniąc o tym stosowną wzmiankę w protokole przesłuchania (§ 120 ust. 1 rozporządzenia). W świetle powyższego Generalny Inspektor Ochrony Danych Osobowych uznał, iż pozyskanie przez Prokuraturę numeru PESEL osoby przesłuchiwanej w charakterze świadka i ujawnienie go w protokole takiego przesłuchania nie może być uznane za naruszające zasady przetwarzania danych określonych w ustawie o ochronie danych osobowych. Wniosku tego nie może zmienić fakt, iż wprost nie przewidują tego przepisy Kodeksu postępowania karnego regulujące zasady prowadzenia postępowania przygotowawczego. Takie uprawnienie bowiem, jak wynika z analizy cytowanych przepisów, dają inne, wskazane wyżej powszechnie obowiązujące akty prawne.

Podsumowując, odnośnie do tego sektora zauważalny jest spadek liczby skarg zasadnych. Bez wątpienia jest to wynikiem systematycznej, ściślej współpracy Generalnego Inspektora Ochrony Danych Osobowych z Komendą Główną Policji oraz coraz powszechniejszej znajomości i właściwego stosowania przez pracowników szeroko rozumianego wymiaru sprawiedliwości przepisów ustawy o ochronie danych osobowych.

3.2.4 Banki i inne instytucje finansowe

Najwięcej skarg wpływających w 2008 r. do Generalnego Inspektora Ochrony Danych Osobowych dotyczyło analizowanego sektora (**179 skarg**). Podobnie jak w latach ubiegłych przedmiotem skarg czyniono najczęściej udostępnienie danych osobowych przez banki firmom windykacyjnym, przysyłanie niechcianej oferty kredytowej (marketingowej), pozyskiwanie danych osobowych w zbyt szerokim zakresie, gdyż dotyczącym np. statusu mieszkaniowego, posiadanego majątku i zobowiązań oraz udostępniania danych osobowych przez banki innym podmiotom,⁹⁹ w tym najczęściej na rzecz Biura Informacji Kredytowej [BIK] i do bankowego rejestru prowadzonego przez Związek Banków Polskich [ZBP].

W omawianym roku sprawozdawczym – podobnie jak w latach ubiegłych – nadal pojawiały się wnioski o nakazanie usunięcia danych z Biura Informacji Kredytowej S.A. i Związku Banków Polskich¹⁰⁰ oraz dotyczące nieprawidłowości przy spełnianiu obowiązku informacyjnego z ustawy o ochronie danych osobowych przez banki i ww. podmioty.¹⁰¹ W jednej ze spraw dotyczących spełnienia obowiązku informacyjnego organ nakazał nie tylko bankowi, ale i Biuru Informacji Kredytowej S.A. oraz Związkowi Banków Polskich wypełnienie wobec osoby skarżącej obowiązku informacyjnego z art. 25, przyjmując, że również na tych instytucjach (BIK S.A. i ZBP), jako na odrębnych administratorach danych, spoczywa ten obowiązek. W innej ze spraw prowadzonych w 2008 r. organ wydał decyzję administracyjną¹⁰² nakazującą bankowi usunięcie danych skarżącego ze zbioru prowadzonego przez Biuro Informacji Kredytowej S.A., jako że bank nie spełnił jednej z przesłanek z art. 105a ust. 3 Prawa bankowego, tj. nie poinformował skarżącego o zamiarze przetwarzania jego danych przez BIK po wygaśnięciu zobowiązania skarżącego bez jego zgody. GIODO uznał, iż w sytuacji, gdy bank nie dysponuje zgodą osoby na przetwarzanie jej danych w zbiorach BIK, to powinien niezwłocznie spowodować usunięcie jej danych z tego zbioru bądź zadbać o spełnienie przesłanek z art. 105a ust. 3 Prawa bankowego, warunkujących przetwarzanie danych mimo braku zgody. W praktyce oznacza to niezwłoczne dopełnienie obowiązku informacyjnego, o którym mowa w tym przepisie. W związku z zakwestionowaniem tego stanowiska przez BIK, sprawa ta jest obecnie rozpatrywana przez Wojewódzki Sąd Administracyjny w Warszawie.

W roku sprawozdawczym 2008 analizowana była również sprawa o naruszenie przepisów ustawy o ochronie danych osobowych w związku z przesłaniem przez bank do osoby skarżącej listem zwykłym korespondencji zawierającej jej dane osobowe.¹⁰³ Generalny

⁹⁸ Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 Nr 139, poz. 993 z późn. zm.).

⁹⁹ Np. DOLiS-440-7/08, DOLiS-440-19/08, DOLiS-440-45/08, DOLiS-440-48/08, DOLiS-440-60/08, DOLiS-440-77/08.

¹⁰⁰ Np. DOLiS-440-90/08, DOLiS-440-108/08, DOLiS-440-198/08.

¹⁰¹ GI-DOLiS-430-20/06.

¹⁰² Decyzja z dnia 4 kwietnia 2008 r. o sygn. DOLiS/DEC-220/08.

¹⁰³ DOLiS-440-380/08.

Inspektor Ochrony Danych Osobowych przyjął w tej sprawie stanowisko, iż przepisy prawa¹⁰⁴ nie zobowiązują administratora danych do stosowania szczególnej formy doręczania korespondencji, w tym przesyłania korespondencji zawierającej dane osobowe listem poleconym. GODO przywołał wyrok WSA w Warszawie,¹⁰⁵ w którym stwierdzono, iż nie ma obowiązku przesyłania listami poleconymi korespondencji zawierającej dane osobowe, a Generalny Inspektor Ochrony Danych Osobowych, a tym bardziej sąd, nie mogą nakazać stosowania tego typu środków, które zabezpieczałyby dane.

Do Generalnego Inspektora Ochrony Danych Osobowych wpływały również skargi na przekazanie danych osobowych przez bank firmom windykacyjnym.¹⁰⁶ W tego typu sprawach najczęściej osoby skarżące kwestionowały działanie banku (udostępnienie danych), twierdząc, że nie posiadały zadłużenia wobec banku (administratora danych). Wówczas organ wskazywał takim osobom, że nie ma kompetencji do badania podstaw prawnych przekazania wierzytelności (i w konsekwencji danych osobowych) do windykacji. W tego typu sprawach Generalny Inspektor Ochrony Danych Osobowych wyjaśniał, iż może zająć stanowisko dopiero po przedstawieniu przez osobę skarżącą orzeczenia sądowego, z którego wynikałoby, że nie istnieje zobowiązanie na które powołuje się bank.

Najliczniejszą grupę skarg na podmioty z tego sektora stanowiły wnioski o usunięcie danych osobowych ze zbioru Biura Informacji Kredytowej S.A. przekazanych tam przez banki. W jednej z takich spraw organ ds. ochrony danych osobowych wydał decyzję nakazującą bankowi spowodowanie usunięcia ze zbioru prowadzonego przez BIK konkretnych danych osobowych.¹⁰⁷ W sprawie tej nie budziła wątpliwości legalność udostępnienia danych osobowych,¹⁰⁸ tylko fakt, że choć bank złożył dyspozycję usunięcia danych osobowych ze zbiorów danych posiadanych przez BIK, to jednak podmiot ten pozostawił wnioskowane dane w zbiorze i przetwarzał je w celu stosowania przez banki metod statystycznych, o których mowa w art. 128 ust. 3 Prawa bankowego, mimo że bank nie zwracał się o to. Generalny Inspektor uznał, że na tle obowiązujących przepisów w pełni zasadny jest wniosek, iż BIK S.A. nie jest upoważnione do samodzielnego decydowania o celu przetwarzania przekazanych mu przez bank informacji stanowiących tajemnicę bankową. Działanie BIK, które otrzymało od banku informacje o danym kliencie (osobie fizycznej) w celu przetwarzania ich dla potrzeb oceny zdolności kredytowej i analizy ryzyka kredytowego, a obecnie przetwarza je w celu stosowania metod statystycznych, o których mowa w art. 128 ust. 3, jest – w ocenie GODO – pozbawione podstaw prawnych. Biuro Informacji Kredytowej - jako podmiot, który nie podlega wymogom kapitałowym ustanowionym w art. 128 ust. 3 Prawa bankowego - nie jest bowiem uprawnione do stosowania metod statystycznych. Zgodnie z brzmieniem wspomnianego artykułu wyłącznie banki mogą stosować metody statystyczne do obliczania wymogów kapitałowych i w rezultacie decydować o potrzebie przetwarzania danych osobowych ich klientów (byłych klientów) dla celów stosowania metod statystycznych z art. 128 ust. 3 Prawa bankowego. W tej sprawie dane osoby skarżące niewątpliwie przekazane zostały przez Bank na rzecz BIK S.A. w ściśle określonym celu – oceny zdolności kredytowej i analizy ryzyka kredytowego. Tymczasem – jak ustalono w toku postępowania - BIK przetwarza dane osobowe osoby skarżącej dla realizacji celu, który nie jest w istocie sprecyzowany.

Podobnie organ ds. ochrony danych osobowych rozstrzygnął w sprawie, w której nakazał bankowi spowodowanie usunięcia danych osobowych skarżącej ze zbiorów BIK S.A. i ZBP, gdyż bank nie spełnił przesłanek z art. 105a ust. 3 Prawa bankowego, pozwalających na przetwarzanie danych w zbiorach ww. instytucji po wygaśnięciu zobowiązania, tj. nie poinformowano skarżącej o zamiarze przetwarzania informacji stanowiących tajemnicę bankową bez jej zgody.¹⁰⁹

GODO zajmował się również kwestią stosowania przez jeden z banków wewnętrznych regulacji (regulaminu) przy wykorzystaniu elektronicznych kanałów obsługi klientów indywidualnych. W sprawie tej okazało się, że bank może rozwiązać umowę rachunku bez wypowiedzenia w przypadku zgłoszenia przez klienta sprzeciwu wobec wykorzystania jego danych osobowych do celów marketingowych banku i otrzymywania, za pośrednictwem elektronicznych kanałów dostępu, informacji o produktach firm współpracujących z bankiem. Ze względu na to, iż działanie takie mogło naruszać nie tylko przepisy ustawy o ochronie danych osobowych, ale również regulacje Prawa bankowego oraz godzić w prawa konsumenckie, GODO powiadomił o sprawie Urząd Ochrony Konkurencji i Konsumentów [UOKiK] oraz Komisji Nadzoru Finansowego [KNF]. W efekcie KNF poinformowała Generalnego Inspektora Ochrony Danych Osobowych, że zaleciła

¹⁰⁴ Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji technicznej oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

¹⁰⁵ Wyrok wydany w sprawie o sygn. akt II SA/Wa 735/2004.

¹⁰⁶ Np. DOLIS-440-413/08.

¹⁰⁷ Decyzja z dnia 26 czerwca 2008 r. o sygn. DOLIS/DEC-390/08.

¹⁰⁸ Było to działanie zgodne z art. 23 ust. 1 pkt 2 ustawy w zw. z art. 105 ust. 4 Prawa bankowego.

¹⁰⁹ Decyzja administracyjna z dnia 2 lipca 2008 r. o sygn. DOLIS/DEC-406/08.

bankowi dostosowanie prowadzonej działalności do przepisów ustawy o ochronie danych osobowych, natomiast bank dostosował swoją działalność do wydanego przez KNF zalecenia. Prezes UOKiK uznał natomiast, że stosowane przez bank wzorce umowne były sprzeczne z przepisami o elektronicznych instrumentach płatniczych i wezwał bank do odpowiednich zmian wzorca umownego.

Generalny Inspektor Ochrony Danych Osobowych interweniował również w sprawach, w których banki nie odpowiadały na wnioski osób skarżących w zakresie przekazania im stosownych informacji w trybie wskazanym w art. 33 ustawy o ochronie danych osobowych. Ustaliwszy, że takowe wnioski wpływały do administratorów danych, a banki swoich obowiązków jednak nie wypełniały bądź wypełniały błędnie (tzn. w niepełnym zakresie), Generalny Inspektor Ochrony Danych Osobowych nakazywał wypełnienie wobec tych osób obowiązku informacyjnego w zakresie wskazanym w art. 33 ustawy.¹¹⁰

Omawiając zagadnienie spełnienia obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych, nie sposób pominąć orzeczenia Wojewódzkiego Sądu Administracyjnego w Warszawie¹¹¹ rozstrzygającego co do uzależnienia realizacji tego uprawnienia kontrolnego od uiszczenia stosowanej opłaty na pokrycie kosztów związanych z dostępem do danych osobowych – kosztów przesyłki. Sąd oddalając skargę na decyzję Generalnego Inspektora Ochrony Danych Osobowych stwierdził, iż administrator danych nie ma prawa do pobierania takiej opłaty, chyba że osoba uprawniona zwraca się z wnioskiem o udzielenie informacji częściej niż co 6 miesięcy.

W 2008 roku do Generalnego Inspektora Ochrony Danych Osobowych docierały również sygnały o tym, że w jednym z banków mogło dochodzić do „kradzieży tożsamości” i wykorzystywania skradzionych danych do zawierania umów kredytowych z tym bankiem. W związku z powyższym organ interweniował u Przewodniczącego Komisji Nadzoru Finansowego, do którego zwrócił się z wnioskiem o rozważenie zbadania prawidłowości wykonywania czynności bankowych w tym podmiocie.¹¹² W odpowiedzi na to wystąpienie Przewodniczący Komisji Nadzoru Finansowego stwierdził, iż w związku z przeprowadzoną kompleksową inspekcją w tym banku brak jest uwag co do przestrzegania przez bank standardów bezpieczeństwa przy wykonywaniu czynności bankowych.¹¹³

Warto w tym miejscu zauważyć, iż w omawianym sektorze pojawiły się również uchybienia skutkujące koniecznością wystąpienia przez organ z zawiadomieniami o podejrzeniu popełnienia przestępstwa. W jednej z takich spraw GODO poinformował prokuraturę o możliwości popełnienia przez jeden z banków przestępstwa z art. 51 ustawy, uznając za nielegalne przesłanie karty bankomatowej przyklejonej do druku firmowego tego banku w niezapakowanej kopercie. Wskutek powyższego do danych osobowych adresata takiej przesyłki mogły mieć dostęp osoby nieuprawnione. Skierowano również zawiadomienie o podejrzeniu popełnienia przestępstwa¹¹⁴ z art. 51 ust. 1 ustawy, polegającego na zamieszczeniu bez podstawy prawnej na stronie internetowej, tzw. bazy danych oszustów zbożowych, obejmującej dane w zakresie: imion, nazwisk, adresów, numerów NIP oraz numerów telefonów. Według informacji zamieszczonej na wspomnianej stronie internetowej, dane te zostały umieszczone przez maklera. W świetle zgromadzonego materiału dowodowego nie można było wykluczyć, iż nastąpiło bezprawne upublicznienie danych osobowych.

Zawiadomieniem o podejrzeniu popełnienia przestępstwa z art. 51 ust. 1 ustawy¹¹⁵ zakończyła się również sprawa, w której organ ustalił, iż dane osobowe osoby skarżącej, zawarte w dokumentach złożonych do podmiotu oferującego pożyczki, zostały udostępnione pracownikowi banku bez jej wiedzy i zgody, a także mimo braku jakiegokolwiek umowy współpracy między tym podmiotem a bankiem. W konsekwencji osoby odpowiedzialne w tym podmiocie za przetwarzanie danych podjęły czynności skutkujące udostępnieniem danych osobowych osobom nieupoważnionym.

Zauważyć należy, że w porównaniu z latami ubiegłymi znacznie wzrosła liczba skarg dotyczących tego sektora. Przyczyną tego zjawiska, jak wynika z przedmiotu skarg, było pojawienie się większej liczby przypadków niewłaściwego zabezpieczenia danych osobowych przez banki oraz ciągle spornej kwestii legalności udostępniania danych osobowych do zbiorów danych prowadzonych przez Biuro Informacji Kredytowej S.A. i Związek Banków Polskich.

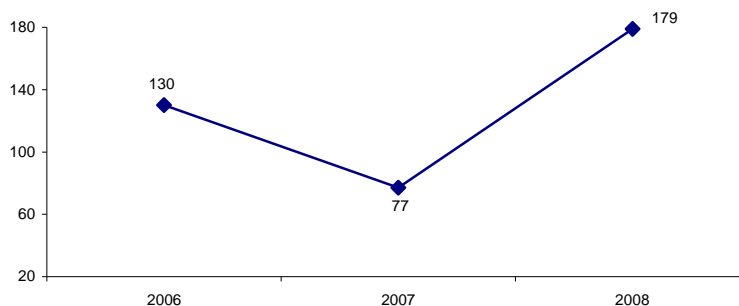
¹¹⁰ Decyzja z dnia 5 maja 2008 r. o sygn. DOLiS/DEC-264/08.

¹¹¹ Wyrok WSA w Warszawie z dnia 13 maja 2008 r. sygn. akt II SA/Wa 336/08 – nieprawomocny.

¹¹² Pismo z dnia 1 grudnia 2008 r. o sygn. DOLiS-440-760/08/33143.

¹¹³ Pismo Przewodniczącego Komisji Nadzoru Finansowego z dnia 3 lutego 2009 r. znak: DPP/023/1889/6/08/09/MG.

¹¹⁴ Zawiadomienie z dnia 10 kwietnia 2008 r. o sygn. DOLiS/ZAW-8/08.



Wykres 6.
Zestawienie porównawcze liczby skarg dotyczących sektora bankowości, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

3.2.5 Marketing

W roku 2008 organ ds. ochrony danych osobowych był adresatem **13 skarg** kwalifikujących się do tego sektora. Najczęściej pojawiającym się zarzutem było przetwarzanie danych osobowych w celach marketingowych bez zgody osoby, której dane te dotyczyły.¹¹⁶ W sprawach z tego sektora główną formą reagowania na przetwarzanie danych osobowych w celach marketingowych były adresowane do administratorów danych sygnałizacje Generalnego Inspektora Ochrony Danych Osobowych. W sprawach, w których naruszenie ustawy o ochronie danych osobowych następowało na masową skalę, a administratorzy danych nie wyrażali woli współpracy z organem w celu zlikwidowania uchybień, Generalny Inspektor Ochrony Danych Osobowych kierował do odpowiednich organów zawiadomienia o podejrzeniu popełnienia przestępstwa.

Warte odnotowania jest prawomocne zakończenie sprawy wszczętej przez organ z urzędu, w której Generalny Inspektor Ochrony Danych Osobowych nakazał Telekomunikacji Polskiej S.A. nieudostępnianie podmiotom trzecim danych osobowych jej abonentów - konsumentów w rozumieniu art. 22¹ Kodeksu cywilnego¹¹⁷ - w celu innym, niż wynikający z realizacji powszechnie świadczonej usługi „ogólnokrajowego spisu abonentów,” w sytuacji braku odrębnej zgody abonentów zezwalającej Telekomunikacji Polskiej S.A. na powyższe działanie.¹¹⁸ Generalny Inspektor Ochrony Danych Osobowych ustalił, iż Spółka wprowadziła usługę sprzedaży baz danych zawierających numery osób prywatnych, tj. abonentów indywidualnych TP S.A. W ramach tej praktyki proponowała usługę „udostępniania numerów telefonów abonentów prywatnych tp” w postaci bazy numerów telefonów zgodną ze złożonym zamówieniem i przekazywanych klientowi na nośniku CD. Jako podstawy powyższego przekazania numerów telefonów abonentów Spółka wskazała art. 66 i 67 ustawy Prawo telekomunikacyjne,¹¹⁹ oraz zgodę osoby, której dane dotyczą, na publikację danych w powszechnie dostępnych spisach abonentów, bądź brak sprzeciwu abonenta na takie udostępnienie. Przedmiotową zgodę Spółka pozyskiwała na podstawie formularza, którego treść brzmi: „(...) wyrażam/nie wyrażam zgody na zamieszczenie identyfikujących mnie danych osobowych w spisach Abonentów Telekomunikacji Polskiej S.A. i innych przedsiębiorców telekomunikacyjnych oraz wykorzystanie identyfikujących mnie danych dla potrzeb świadczenia przez Telekomunikację Polską S.A. usługi informacji o numerach telefonicznych (...)”. W sprawie tej Generalny Inspektor Ochrony Danych Osobowych stwierdził, że zgoda, jakiej w przedmiotowej sprawie udzielają abonenci na umieszczenie ich danych w „ogólnokrajowym spisie abonentów,” nie może być utożsamiana ze zgodą na udostępnienie ich danych osobowych w ramach świadczenia usługi „sprzedaży baz danych”. Są to dwie różne usługi świadczone w dwóch różnych celach. Pierwsza usługa niewątpliwie znajduje swoje podstawy w przepisach Prawa telekomunikacyjnego. Natomiast usługa „sprzedaży baz danych” świadczona jest przez TP S.A. wyłącznie w celach komercyjnych i ma za zadanie ułatwić nabywcom baz danych skuteczne i precyzyjne dotarcie do klientów,

¹¹⁵ Pismo z dnia 31 lipca 2008 r. o sygn. DOLiS/ZAW-16/08/19731, dot. DOLiS-440/227/08.

¹¹⁶ Np. DOLiS-440-51/08.

¹¹⁷ Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.).

¹¹⁸ Decyzja z dnia 14 maja 2007 r. o sygn. GI-DEC-DOLiS-109/07/2885.

obniżenie kosztów pozyskania nowych klientów, szybkie przeprowadzenie badań marketingowych oraz efektywne wykorzystanie budżetu na promocję i reklamę. Z tego wynika, że cele ww. usług TP S.A. w sposób zasadniczy są od siebie różne. W związku z tym Generalny Inspektor Ochrony Danych Osobowych uznał, iż udostępnianie przez Telekomunikację Polską S.A. danych osobowych swoich abonentów (konsumentów) podmiotom trzecim w analizowanej formie, bez wyraźnej zgody osób, których te dane dotyczą oraz wobec faktu, iż nie znajduje to uzasadnienia w przepisach Prawa telekomunikacyjnego, jest sprzeczne z postanowieniami ustawy o ochronie danych osobowych.

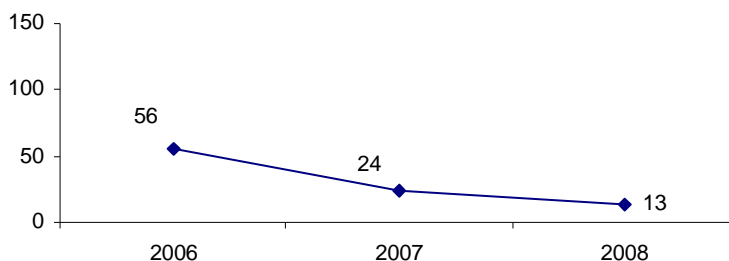
Powyższe stanowisko organu zostało potwierdzone przez Naczelny Sąd Administracyjny¹²⁰ i Wojewódzki Sąd Administracyjny w Warszawie, który oddalił skargę TP S.A.¹²¹

Liczna grupa skarg z tego sektora dotyczyła treści klauzuli zgody, której zapis dawał podmiotom świadczącym usługi marketingowe prawo do przetwarzania danych osobowych w celu promocji produktów i usług podmiotów trzecich (innych niż administrator danych). W jednej z tego typu spraw Generalny Inspektor Ochrony Danych Osobowych uznał za konieczne wystąpienie¹²² do firmy marketingowej o zmianę klauzuli zgody zamieszczanej na kuponach konkursowych firmy, tj. o zastosowanie odrębnej i całkowicie niezależnej od innych oświadczeń woli, klauzuli zgody na przetwarzanie danych osobowych innym podmiotom oraz odrębną klauzulę zgody na przekazywanie informacji handlowej za pomocą środków komunikacji elektronicznej.

W kolejnej sprawie Generalny Inspektor Ochrony Danych Osobowych zawiadomił właściwy organ ścigania o podejrzeniu popełnienia przestępstwa z art. 49 ust. 1 ustawy,¹²³ w związku z przetwarzaniem danych w celu marketingowym przez operatora telewizyjnego, mimo wniesienia przez osobę skarżącą sprzeciwu wobec przetwarzania danych w tym celu i złożenia reklamacji w tym zakresie. Podobną decyzję GODO podjął w sprawie spółki marketingowej,¹²⁴ która przetwarzała dane osobowe skarżącego bez podstawy prawnej,¹²⁵ tj. mimo wniesienia sprzeciwu przez osobę skarżącą i niedopełnienia przez administratora danych obowiązku informacyjnego, o którym stanowi art. 33 ustawy o ochronie danych osobowych (art. 49 i 54 ustawy).

Warto podkreślić w tym miejscu, iż często spotykanym zjawiskiem przy przetwarzaniu danych osobowych w celach marketingowych było lekceważenie (ignorowanie) przez administratorów danych zasadnych sprzeciwów osób, których dane były w tych celach wykorzystywane. Jeśli w takich sprawach organ ds. ochrony danych osobowych stwierdził naruszenie zasad ochrony danych, kierował do organów powołanych do ścigania przestępstw, stosowne zawiadomienia. Niestety, podobnie jak w poprzednich latach, przypadki naruszeń ustawy o ochronie danych osobowych najczęściej kończyły się odmową wszczęcia dochodzenia bądź szybkim umorzeniem postępowań, albo uznaniem, że brak jest znamion czynu karalnego lub odrzuceniem wniosku o ściganie z uwagi na niską społeczną szkodliwość czynu.

W podsumowaniu należy wskazać, iż w sektorze marketingu utrzymuje się odnotowany już w latach ubiegłych systematyczny spadek liczby skarg, co obrazuje Wykres 7.



Wykres 7.
Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych w celach marketingowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

¹¹⁹ Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

¹²⁰ Wyrok z dnia 26 stycznia 2009 r. sygn. akt I OSK 174/08.

¹²¹ Wyrok z dnia 12 listopada 2007 r. sygn. akt II SA/Wa 1252/07.

¹²² Wystąpienie z dnia 29 lutego 2008 r. o sygn. DOLiS-440-126/07.

¹²³ Zawiadomienie z dnia 14 kwietnia 2008 r. o sygn. DOLiS/ZAW-10/08.

¹²⁴ DOLiS-440-303/08.

Niewątpliwie w znacznym stopniu jest to efekt konsekwentnej działalności informacyjnej GIODO, rygorystycznego stosowania przepisów ustawy o ochronie danych osobowych 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, a także szeroko zakrojonej działalności edukacyjnej organu, ukierunkowanej na podniesienie świadomości obywateli w zakresie ochrony dotyczących ich danych osobowych.

3.2.6 Sektor mieszkalnictwa

Skargi wpływające na podmioty z tego sektora dotyczyły głównie zagadnień przetwarzania danych osobowych przez spółdzielnie mieszkaniowe, wspólnoty mieszkaniowe oraz zarządców nieruchomości.

Najczęściej zarzucano im upublicznianie danych osobowych poprzez wywieszenie na klatkach schodowych bądź na drzwiach wejściowych do budynków pism lub ogłoszeń, zawierających dane osobowe osób skarżących. W tego typu sprawach upublicznianie danych co do zasady naruszało ustawę o ochronie danych osobowych. Dlatego Generalny Inspektor Ochrony Danych Osobowych kierował wystąpienia z wezwaniem do zaprzestania tego typu praktyk, co spotykało się z pozytywną najczęściej reakcją administratorów danych. W jednej z takich spraw¹²⁶ organ ds. ochrony danych osobowych skierował sygnalizację do przewodniczącego zarządu wspólnoty mieszkaniowej, celem zaprzestania praktyki upubliczniania danych osobowych dotyczących postępowania sądowego wytoczonego wspólnocie, w treściach informacji umieszczanych na tablicach ogłoszeń.¹²⁷ Zarząd wspólnoty mieszkaniowej zastosował się do zaleceń organu.¹²⁸

Generalny Inspektor Ochrony Danych Osobowych spotkał się z polemiką ze strony zarządu jednej ze wspólnot mieszkaniowych w sprawie, w której wystąpił z sygnalizacją¹²⁹ w związku z upublicznieniem przez ten zarząd danych osobowych osoby skarżącej w treści ogłoszeń o zebraniu właścicieli nieruchomości umieszczonych na klatce schodowej budynku. Generalny Inspektor Ochrony Danych Osobowych, podobnie jak w innych tego typu sprawach, zwrócił się o zmianę ww. praktyki, argumentując, że prowadzi ona do naruszenia przepisów ustawy o ochronie danych osobowych. W odpowiedzi zarząd wspólnoty stwierdził, że klatka schodowa, na której wisiały owe ogłoszenia „jest pomieszczeniem dostępnym jedynie dla mieszkańców budynku, a dostęp do niej jest możliwy tylko przy pomocy domofonu zainstalowanego przy drzwiach wejściowych.” Generalny Inspektor Ochrony Danych Osobowych uznał, że taki pogląd jest sprzeczny z zasadami prawidłowego przetwarzania danych osobowych i nie przyjął argumentów zarządu wspólnoty. Wskazał ponadto, że ewentualne ujawnienie danych w treści takich ogłoszeń mogłoby być uznane za zgodne z ustawą, jeżeli odbyłoby się to za zgodą osoby, której dane dotyczą oraz, że osiągnięcie celu, jakim jest zawiadomienie członków wspólnoty o czasie, miejscu i przedmiocie zebrania możliwe jest poprzez upublicznienie tej informacji w miejscu ogólnodostępnym, ale bez pełnej identyfikacji osoby, której sprawa miała być omawiana na tym zebraniu. Zarząd wspólnoty ostatecznie zgodził się z tą argumentacją i zapewnił, że nie powtórzy praktyki zakwestionowanej przez organ, i że zebrania będą zwoływane zgodnie z art. 32 pkt 4 ustawy o własności lokali.¹³⁰

W 2008 r. Generalny Inspektor Ochrony Danych Osobowych prowadził również sprawę,¹³¹ w której za niedopuszczalne uznał¹³² przetwarzanie przez wspólnotę mieszkaniową danych osobowych jej członka w zakresie, w jakim są one ujawnione w posiadanej przez wspólnotę kopii aktu notarialnego. Dokonywane jest bowiem w zakresie szerszym, niż uzasadnia to cel ich przetwarzania, wynikający w szczególności z przepisów ustawy o własności lokali.¹³³ Generalny Inspektor Ochrony Danych Osobowych nakazał zatem wspólnocie

¹²⁵ Zawiadomienie z dnia 7 sierpnia 2008 r. o sygn. DOLiS/ZAW-18/08/20383.

¹²⁶ DOLiS-440-236/07.

¹²⁷ Sygnalizacja z dnia 1 kwietnia 2008 r. o sygn. DOLiS-440-236/07.

¹²⁸ Pismo z dnia 29 kwietnia 2008 r. znak: L.dz. 36/08.

¹²⁹ Pismo z dnia 6 czerwca 2008 r. o sygn. DOLiS-440-218/08.

¹³⁰ Pismo z dnia 25 czerwca 2008 r.

¹³¹ GI-DOLiS-430/17/07.

¹³² DOLiS/DEC-3/318,319/08.

¹³³ Ustawa z dnia 24 czerwca 1994 r. o własności lokali (Dz. U. z 2000 r. Nr 80, poz. 903 z późn. zm.).

usunięcie z kopii aktów notarialnych takich danych osobowych osoby skarżącej, jak seria i numer dowodu tożsamości, numer PESEL, NIP, informacja o pochodzeniu funduszy na zakup lokalu, informacja o cenie lokalu i sposobie płatności, informacja o zaciągnięciu kredytu na zakup lokalu, informacja o poddaniu się egzekucji na podstawie aktu notarialnego w trybie art. 777 § 1 pkt 4 K.p.c. oraz informacja o kosztach zawarcia umowy kupna-sprzedaży lokalu i sposobie ich pokrycia. Dane te są bowiem nieadekwatne do nałożonych na wspólnotę obowiązków ustawowych. Zdaniem organu ds. ochrony danych osobowych, wspólnota może natomiast dysponować takimi danymi z aktu notarialnego, jak powierzchnia lokalu, udział procentowy we wspólnych częściach budynku i we własności gruntu, jako niezbędnymi do obliczenia kosztów zarządu nieruchomością wspólną, jak i do ewentualnego dochodzenia należności w postępowaniu upominawczym, o którym mowa w art. 15 ust. 2 ustawy o własności lokali.¹³⁴ Informacje te są też niezbędne do naliczania i rozliczania zaliczek na pokrycie kosztów utrzymania nieruchomości wspólnej, głosowania nad uchwałami Wspólnoty i windykacji należności. Dane te są zatem danymi adekwatnymi w stosunku do celu ich przetwarzania przez Wspólnotę, a sposób utwardzenia tych danych poprzez skopiowanie aktu notarialnego nie przesądza o legalności lub nielegalności ich przetwarzania. Warto w tym miejscu wskazać na stanowisko NSA, który w wyroku z dnia 7 listopada 2003 r.¹³⁵ podkreślił, iż „ustawa o ochronie danych osobowych nie zajmuje się określeniem techniki gromadzenia danych osobowych, lecz zakresem ich przetwarzania (...)”.

W sprawach z tego sektora Generalny Inspektor Ochrony Danych Osobowych kierował również zawiadomienia o podejrzeniu popełnienia przestępstwa. W jednej ze spraw organ złożył zawiadomienie o podejrzeniu popełnienia przestępstwa określonego w art. 51 ust. 1 ustawy, polegającego na udostępnieniu przez osoby odpowiedzialne za przetwarzanie danych w spółdzielni budowlano-mieszkaniowej, w liście kierowanym przez zarząd spółdzielni do członków spółdzielni, danych zwykłych i szczególnie chronionych osobom nieupoważnionym.¹³⁶ GIODO uznał, że spółdzielnia miała prawo udostępnić jedynie te dane, które znajdują się w rejestrze, o którym mowa w art. 30 Prawa spółdzielczego (tj. imiona, nazwiska oraz miejsce zamieszkania, wysokość zadeklarowanych i wniesionych udziałów, wysokość wniesionych wkładów, ich rodzaj, jeżeli są to wkłady niepieniężne, zmiany tych danych, datę przyjęcia w poczet członków, datę wypowiedzenia członkostwa i jego ustania, a także inne dane przewidziane w statucie). W zakresie udostępnienia danych szczególnie chronionych nie została spełniona natomiast żadna z przesłanek wynikających z art. 27 ust. 2 pkt. 1-10 ustawy. Udostępnienie miało zakres szerszy niż dopuszczają to przepisy prawa. Administrator danych nie dołożył w tej sprawie należytej staranności w celu zabezpieczenia danych, do czego jest zobowiązany mocą art. 26 ust. 1 ustawy.

W omawianym okresie sprawozdawczym pojawił się również problem zabezpieczenia danych osobowych w przesyłkach kierowanych przez spółdzielnie do swoich członków. W jednej z takich spraw¹³⁷ Generalny Inspektor Ochrony Danych Osobowych wydał nakaz usunięcia uchybień w procesie przetwarzania danych osobowych osoby skarżącej, poprzez zaprzestanie doręczania korespondencji w formie otwartych przesyłek.¹³⁸ W tej sprawie ustalono bowiem, że spółdzielnia mieszkaniowa dostarczała korespondencję swoim członkom w otwartych kopertach, bądź bez kopert, co stanowiło naruszenie art. 36 ust. 1 ustawy o ochronie danych osobowych.

W innej sprawie z tego sektora Generalny Inspektor Ochrony Danych Osobowych uznał, iż zachodzą przesłanki podejrzenia popełnienia przestępstwa, tj. naruszenia przepisu art. 51 ust. 1 ustawy o ochronie danych osobowych, wskutek udostępnienia przez osoby odpowiedzialne za przetwarzanie danych w spółdzielni mieszkaniowej, imienia i nazwiska osoby skarżącej zawartych w kopii pisma dotyczącego zaskarżenia uchwały spółdzielni. Dane w zakresie imienia i nazwiska udostępniono szerokiemu kręgowi osób poprzez wywieszenie kopii ww. pism w miejscach ogólnodostępnych. Celem takiego działania było zawiadomienie osób uprawnionych do przekształceń prawa do lokali w budynku, w którym usytuowane jest mieszkanie osoby skarżącej, o pozyskaniu z sądu zawiadomienia o zaskarżeniu uchwały i przesłaniu do spółdzielni odpisu pozwu.¹³⁹ Po skierowaniu przez prokuraturę aktu oskarżenia do sądu termin rozprawy wyznaczony został na III kwartał 2009 r.

¹³⁴ Zgodnie z art. 15 ust. 2 ustawy o własności lokali, należności z tytułu kosztów zarządu mogą być dochodzone w postępowaniu upominawczym, bez względu na ich wysokość.

¹³⁵ Sygn. akt II SA 1432/02.

¹³⁶ Zawiadomienie z dnia 25 marca 2008 r. o sygn. akt DOLiS/ZAW-6/08.

¹³⁷ GI-DOLiS-430/308/07.

¹³⁸ Decyzja z dnia 6 października 2008 r. o sygn. DOLiS/DEC-620/08/26334,26338.

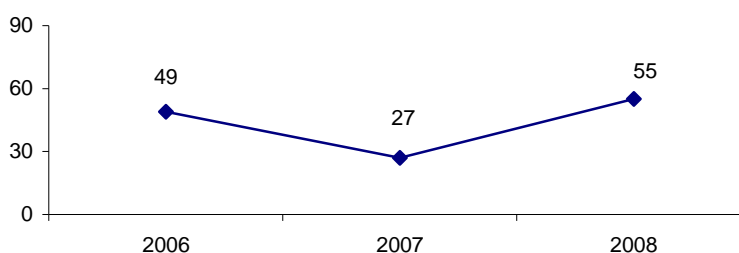
¹³⁹ Zawiadomienie z dnia 14 maja 2008 r. o sygn. DOLiS/ZAW-11/08.

Kolejnym problemem analizowanym przez organ w 2008 r. była kwestia wideonadзору. Generalny Inspektor Ochrony Danych Osobowych wystąpił do prezesa jednej ze spółdzielni mieszkaniowych w sprawie stosowania przez nią wideonadзору,¹⁴⁰ w celu rejestracji przypadków niszczenia roślinności posadzonej na obszarze objętym monitoringiem oraz zachowania się osób będących pod wpływem alkoholu. Organ wskazał, że w świetle przepisów Konstytucji RP (art. 47), orzecznictwa Trybunału Konstytucyjnego oraz europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r. takie działanie jest bezprawne.

Generalny Inspektor Ochrony Danych Osobowych był również adresatem skarg dotyczących odmowy udostępnienia przez spółdzielnie danych osobowych swoich członków wierzycielom osoby, której wnioskowane dane dotyczyły. W takich sprawach organ rozstrzygał na korzyść wnioskodawców (wierzycieli), m.in. nakazując spółdzielni mieszkaniowej udostępnienie danych osobowych dotyczących jej członka pełnomocnikowi wierzyciela w celu wykorzystania informacji o członkostwie i posiadaniu przez tę osobę własnościowego spółdzielczego prawa do lokalu mieszkalnego w toczącym się wobec niej postępowaniu egzekucyjnym. W jednej z takich spraw Generalny Inspektor Ochrony Danych Osobowych uznał, że znajduje tu zastosowanie przesłanka z art. 23 ust. 1 pkt. 2 i 5 ustawy o ochronie danych osobowych. Według wnioskodawcy, w sprawie zachodziło bowiem uzasadnione podejrzenie, iż osoba, której wnioskowane dane dotyczyły, mogła wyzbyć się majątku (własnościowego spółdzielczego prawa do lokalu mieszkalnego w spółdzielni) na rzecz swojej siostry, w celu uniknięcia egzekucji z tego lokalu w związku z posiadaniem przez nią zadłużeniem.¹⁴¹

Podsumowując ten rozdział należy wskazać, iż podobnie jak w latach ubiegłych przeważającą liczbę skarg stanowiły te dotyczące upubliczniania danych osobowych. Znamienne jednak jest to, że po każdej z interwencji Generalnego Inspektora Ochrony Danych Osobowych, administratorzy danych zmieniali swoją praktykę kładąc większy nacisk na zasady przetwarzania danych osobowych wynikające z ustawy o ochronie danych osobowych.

W analizowanym roku 2008, w porównaniu z latami ubiegłymi, odnotowano wzrost liczby skarg na przetwarzanie danych przez ww. podmioty.¹⁴²



Wykres 8.
Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych osobowych z zakresu mieszkalnictwa, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

¹⁴⁰ Pismo z dnia 24 października 2008 r. o sygn. DOLiS-035-1368/08/28697.

¹⁴¹ Decyzja z dnia 19 grudnia 2008 r. o sygn. DOLiS/DEC-856/08/35326,35329.

¹⁴² 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.

3.2.7 Ubezpieczenia społeczne, majątkowe i osobowe

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

W odniesieniu do skarg dotyczących ubezpieczeń społecznych warte odnotowania były dosyć często pojawiające się przypadki odmowy wydania osobie skarżącej dokumentacji zawierającej jej dane osobowe. W jednej z takich spraw lekarz oraz ZUS odmówili wydania osobie skarżącej wyników badań, na które osoba ta została skierowana przez ZUS.¹⁴³ GODO w tym przypadku nie kwestionował prawa osoby skarżącej do zaznajomienia się z tą dokumentacją. Wskazał jednak na brak swojej właściwości w kwestii formułowania nakazu wydania dokumentacji zawierającej dane osobowe. Przedmiotem nakazu może być bowiem udostępnienie informacji o danych osobowych, czego nie można utożsamiać z wydaniem nośników (dokumentów) zawierających te dane.

W innej sprawie, Wojskowa Agencja Mieszkaniowa [WAM] zakwestionowała odmowę ZUS udzielenia jej informacji dotyczących niepełnosprawności osoby, wobec której Agencja prowadzi postępowanie o eksmisję z lokalu mieszkalnego.¹⁴⁴ WAM, jako organ egzekucyjny, po wszczęciu postępowania egzekucyjnego przeciwko osobie fizycznej, rozważał wystąpienie do sądu z pozwem o nakazanie opróżnienia lokalu mieszkalnego zajmowanego przez ww. osobę oraz o orzeczenie o uprawnieniu do otrzymania lokalu socjalnego. W związku z powyższym zwrócił się do ZUS z wnioskiem o udostępnienie danych osobowych w zakresie informacji, czy osoba ta jest emerytem lub rencistą spełniającym kryteria do otrzymania świadczenia z pomocy społecznej lub osobą niepełnosprawną w rozumieniu przepisów ustawy o pomocy społecznej, wskazując jako podstawę prawną tego żądania art. 27 ust. 2 pkt. 5 i 10¹⁴⁵ ustawy w związku z art. 38 i 45 ustawy o zakwaterowaniu Sił Zbrojnych Rzeczypospolitej Polskiej,¹⁴⁶ w związku z art. 19 § 7 ustawy o postępowaniu egzekucyjnym w administracji.¹⁴⁷ WAM wskazała również, iż uzyskane dane zostaną wykorzystane w celu ustalenia, czy osobie tej przysługuje prawo do otrzymania lokalu socjalnego. ZUS odmówił WAM udostępnienia danych osobowych. Generalny Inspektor Ochrony Danych Osobowych uznał, iż ZUS zasadnie odmówił uwzględnienia żądanych danych osobowych.¹⁴⁸ GODO przyjął takie stanowisko, powołując się na art. 27 ust. 2 ustawy o ochronie danych osobowych, który stanowi, iż przetwarzanie danych osobowych jest dopuszczalne między innymi wówczas, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której one dotyczą i stwarza pełne gwarancje ich ochrony. GODO przyjął, że jeżeli istnieją inne przepisy prawa, które odmiennie regulują przetwarzanie – w tym udostępnianie danych osobowych - to przepisy te stanowią samodzielną przesłankę przetwarzania danych, o której mowa w art. 27 ust. 2 pkt 2 ustawy. W przedmiotowej sprawie takimi regulacjami były przepisy ustawy o systemie ubezpieczeń społecznych,¹⁴⁹ które regulują kwestię przetwarzania tzw. danych wrażliwych (m.in. informacji o stanie zdrowia, w tym także o stopniu niepełnosprawności osoby objętej ubezpieczeniem

¹⁴³ DOLIS-440-12/08.

¹⁴⁴ DOLIS-440-22/08.

¹⁴⁵ Zgodnie z art. 27 ust. 2 pkt 5, przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli dotyczy danych, które są niezbędne do dochodzenia praw przed sądem; przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym (pkt 10).

¹⁴⁶ Zgodnie z art. 38 ust. 1 wspomnianej ustawy, w przypadku żołnierzy służby stałej, którzy nie uiszczają pełnych opłat za używanie lokalu lub pełnych opłat pośrednich z tytułu zajmowania lokalu mieszkalnego przez łączny okres dłuższy niż trzy miesiące, dyrektor oddziału regionalnego Agencji wydaje decyzję o prawie zamieszkiwania w kwaterze zastępczej, o której mowa w art. 50 ust. 1 pkt 2, a w przypadku odmowy jej przyjęcia dyrektor oddziału regionalnego Agencji zarządza, w trybie art. 45, przymusowe przekwaterowanie do tej kwatery zastępczej, wraz ze wszystkimi wspólnie zamieszkującymi osobami. Ust. 2: W stosunku do osób niebędących żołnierzami służby stałej, które nie uiszczają pełnych opłat za używanie lokalu lub pełnych opłat pośrednich z tytułu zajmowanego lokalu mieszkalnego przez łączny okres dłuższy niż trzy miesiące, dyrektor oddziału regionalnego Agencji zarządza przymusowe wykwaterowanie w trybie art. 45 (Dz. U. 2005 r. Nr 41 poz. 398 z późn. zm.).

¹⁴⁷ Zgodnie z art. 19 § 7 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.), Dyrektor oddziału regionalnego Wojskowej Agencji Mieszkaniowej jest organem egzekucyjnym uprawnionym do stosowania egzekucji z wynagrodzenia za pracę oraz ze świadczeń z zaopatrzenia emerytalnego albo z ubezpieczenia społecznego, w egzekucji administracyjnej należności pieniężnych z tytułu opłat za używanie lokalu i opłat pośrednich związanych z zajmowaniem lokali mieszkalnych będących w dyspozycji Wojskowej Agencji Mieszkaniowej.

¹⁴⁸ Decyzja z dnia 13 maja 2008 r. o sygn. DOLIS/DEC-292/08 - nieprawomocna; wyrok WSA w Warszawie z dnia 10 lutego 2009 r. o sygn. akt II SA/Wa 1554/08 – nieprawomocny.

¹⁴⁹ Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2007 r. Nr 11, poz. 74 z późn. zm.).

społecznym). W świetle art. 34 ust. 3 tej ustawy, do informacji zawartych na kontach ubezpieczonych i kontach płatników składek oraz danych źródłowych będących podstawą zapisów na tych kontach, stosuje się przepisy o ochronie danych osobowych. Art. 34 ust. 4 ustawy o systemie ubezpieczeń społecznych przewiduje również, że wykorzystywanie danych osobowych i innych informacji zgromadzonych na kontach ubezpieczonych dopuszczalne jest jedynie w przypadkach określonych w ustawie. Jednocześnie, w myśl art. 50 ust. 3 omawianego aktu prawnego, dane zgromadzone na koncie ubezpieczonego, o których mowa w art. 40, i na koncie płatnika składek, o których mowa w art. 45, mogą być udostępniane sądom, prokuratorom, organom kontroli skarbowej, organom podatkowym, komornikom sądowym, ośrodkom pomocy społecznej, powiatowym centrom pomocy rodzinie oraz Komisji Nadzoru Ubezpieczeń i Funduszy Emerytalnych, z uwzględnieniem przepisów dotyczących ochrony danych osobowych. Z brzmienia art. 50 ust. 3 ustawy o systemie ubezpieczeń społecznych wynika zatem, że dopuszczalność udostępniania przez ZUS danych zgromadzonych na koncie ubezpieczonych została ograniczona wyłącznie do wskazanych w omawianym przepisie podmiotów. Nie zachodziły zatem w tej sprawie podstawy prawne dla udostępnienia przez ZUS danych osobowych podmiotom niewymienionym w ww. katalogu (w tym przypadku WAM). Organ ds. ochrony danych osobowych stwierdził jednocześnie, że w świetle powyższego powoływanie się przez WAM na przepisy art. 27 ust. 2 pkt 5 i pkt 10 ustawy nie mogło zostać uwzględnione. Udostępnienie danych osobowych osoby ubezpieczonej w oparciu o wskazane przepisy prowadziłoby bowiem do „obejścia” przepisu art. 50 ust. 3 ustawy o systemie ubezpieczeń społecznych, co z pewnością nie było intencją ustawodawcy, który wyraźnie określił katalog podmiotów, którym ZUS może udostępniać dane zgromadzone na kontach ubezpieczonych. Ponadto należy w tym miejscu zauważyć, że odmowa nakazania ZUS udostępnienia danych osobowych nie uniemożliwiała WAM prowadzenia postępowania egzekucyjnego ani też wystąpienia do sądu z pozwem, o którym mowa w art. 45 ust. 3 ustawy o zakwaterowaniu Sił Zbrojnych Rzeczypospolitej Polskiej. Zgodnie bowiem z art. 143 § 2 ustawy o postępowaniu egzekucyjnym w administracji, zobowiązanemu przysługuje prawo zgłoszenia zarzutu, o którym to uprawnieniu powinien zostać pouczone przez organ egzekucyjny w treści tytułu wykonawczego.¹⁵⁰ Podstawą zarzutu w sprawie prowadzenia egzekucji administracyjnej, stosownie do art. 33 pkt 6 ustawy o postępowaniu egzekucyjnym w administracji, może być niedopuszczalność egzekucji administracyjnej lub zastosowanego środka egzekucyjnego.

W odniesieniu do spraw z sektora ubezpieczeń majątkowych na uwagę zasługuje prawomocnie zakończone postępowanie¹⁵¹ ze skargi na udostępnienie (bez zgody osoby skarżącej) danych osobowych przez Powszechny Zakład Ubezpieczeń S.A. [PZU S.A.], na rzecz Towarzystwa Ubezpieczeń i Reasekuracji Warta S.A. [TUiR Warta]. W sprawie tej osoba skarżąca zawarła umowę ubezpieczenia z PZU S.A. w zakresie AC, OC, NW i Assistance. W związku z kolizją drogową, w której osoba skarżąca była stroną poszkodowaną, złożyła w PZU S.A. zawiadomienie o szkodzie w jej pojeździe, wnosząc zarazem o „wyplacenie odszkodowania w warunkach odpowiedzialności sprawcy szkody” i „pokrycie kosztów naprawy samochodu zaliczkowo z mojego ubezpieczenia auto casco”. Następnie osoba skarżąca zgłosiła szkodę w TUIR WARTA S.A. będącym ubezpieczycielem sprawcy kolizji. W tym celu skarżąca wypełniła formularz „Zgłoszenie szkody komunikacyjnej” i powiadomiła o tym PZU S.A., które następnie przekazało akta szkody do TUIR WARTA S.A. w celu dalszej likwidacji. Generalny Inspektor Ochrony Danych Osobowych ustalił, że od chwili zgłoszenia przez PZU S.A. szkody z auto casco do chwili ustalenia sprawcy tej szkody, PZU S.A. wykonał wstępne czynności ubezpieczeniowe związane z jej likwidacją, a wobec późniejszego ustalenia, iż sprawca szkody był ubezpieczony w TUIR WARTA S.A., czynności te zostały wykonane przez PZU S.A. na rzecz TUIR WARTA S.A. Natomiast dokumentacja dotycząca szkody została przesłana przez PZU S.A. do TUIR WARTA S.A. jednocześnie z żądaniem zapłaty należnego PZU S.A. wynagrodzenia. Ustalono również, że pomiędzy PZU S.A. i TUIR WARTA S.A. obowiązywało porozumienie co do zasad wzajemnej współpracy w zakresie obsługi likwidacji szkód z obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych za szkody powstałe w związku z ruchem tych pojazdów.

Generalny Inspektor Ochrony Danych Osobowych nie potwierdził w tej sprawie zarzutów co do bezprawnego udostępnienia danych osobowych pomiędzy ww. ubezpieczycielami. Uznał bowiem, że zastosowanie miał art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. PZU S.A. mógł udostępnić dane osobowe TUIR WARTA S.A. bez zgody osoby, której dane dotyczyły.

¹⁵⁰ Art. 27 § 1 pkt 9 ustawy o postępowaniu egzekucyjnym w administracji.

Zgoda osoby, której dane dotyczą na ich przetwarzanie, nie jest jedyną i wyłączną okolicznością czyniącą proces przetwarzania legalnym. Ustawa nie daje również żadnych innych podstaw, aby traktować ją w sposób uprzywilejowany, jako przesłankę główną, podstawową.¹⁵² W sprawie tej istotne znaczenie miały natomiast przepisy ustawy o działalności ubezpieczeniowej.¹⁵³ W wyniku zgłoszenia przez osobę szkody powstałej na skutek kolizji drogowej, PZU S.A. dokonał wstępnych czynności ubezpieczeniowych określonych w art. 3 ust. 5 pkt. 1 i 2 ustawy o działalności ubezpieczeniowej, którymi są ustalenie przyczyn i okoliczności zdarzeń losowych i ustalenie wysokości szkód oraz rozmiaru odszkodowań. Do powyższych czynności PZU S.A. uprawniony był na podstawie art. 3 ust. 7 przywołanej ustawy w związku z porozumieniem zawartym przez PZU S.A. i TUIR WARTA S.A. Warto zauważyć ponadto, że w toku niniejszego postępowania Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Komisji Nadzoru Finansowego – jako organu sprawującego nadzór nad zakładami ubezpieczeń, wykonującymi działalność ubezpieczeniową na terytorium Rzeczypospolitej Polskiej - o wykładnię powyższego przepisu. W wyjaśnieniach otrzymanych od KNF wskazano, iż „(...) istotą regulacji zawartej w art. 3 ust. 7 ustawy ubezpieczeniowej jest dopuszczenie możliwości zlecenia przez zakład ubezpieczeń wykonania niektórych czynności ubezpieczeniowych innemu zakładowi ubezpieczeń, niebędącemu stroną umowy ubezpieczenia, w związku z wykonywaniem której czynność ubezpieczeniowa jest dokonywana. Przepis przesądza nadto, że w takim przypadku dana czynność nie traci charakteru ubezpieczeniowej (...). Nie powinno budzić wątpliwości, że kwestie zlecenia wykonania czynności ubezpieczeniowych pozostają w domenie prawa cywilnego. Z tego względu należy uznać, iż dopuszczalna jest każda prawem przewidziana forma współpracy pomiędzy zakładami ubezpieczeń, w tym stosunek prawny o charakterze ciągłym. Wyras „wniosek” powinien być rozumiany w przedmiotowym przypadku potocznie, jako inicjatywa jednego zakładu ubezpieczeń skierowana do drugiego w przedmiocie zlecenia wykonania czynności ubezpieczeniowej. Inicjatywy takie Inter Partes mogą być uregulowane w dowolny dopuszczony przez prawo sposób. Stwierdzić zatem należy, że w świetle wykładni językowej oraz systemowej nie ma podstaw do uznania, iż przedmiotem regulacji art. 3 ust. 7 ustawy o działalności ubezpieczeniowej jest procedura zlecenia wykonania czynności ubezpieczeniowej, przewidująca konieczność złożenia wniosku o określonych walorach formalnych.” W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych w swoim rozstrzygnięciu nie podzielił zarzutów osoby skarżącej.¹⁵⁴ WSA w Warszawie¹⁵⁵ przychylił się do stanowiska Generalnego Inspektora Ochrony Danych Osobowych uznając, że działanie ubezpieczyciela - polegające na przesłaniu zakładowi ubezpieczeniowemu sprawcy kolizji drogowej wypłacającemu odszkodowanie, materiału ze wstępnych czynności ubezpieczeniowych dokonanych po zgłoszeniu szkody – odbyło się w zgodzie z zasadami przetwarzania danych osobowych, tj. na podstawie art. 23 ust. 1 pkt 2 ustawy w związku z art. 3 ustawy o działalności ubezpieczeniowej (w szczególności jej ust. 1, ust. 4 pkt. 2 i 5, ust. 5 pkt. 1 i 2 oraz ust. 7).

W innej sprawie Generalny Inspektor Ochrony Danych Osobowych zawiadomił¹⁵⁶ o podejrzeniu popełnienia przestępstwa przez osoby odpowiedzialne w towarzystwie ubezpieczeń za przetwarzanie danych osobowych klientów (określonego w art. 51 ust. 1 ustawy), które bezprawnie udostępniły dane osobie nieupoważnionej, oraz przestępstwa określonego w art. 52 tej ustawy, polegającego na umożliwieniu zabrania danych osobowych przez osobę nieuprawnioną. Z załączonych do skargi wydruków dokumentów pozyskanych przez osobę skarżącą od zakładu ubezpieczeń wynikało, że zawierają one dane osobowe, które nie dotyczą osoby skarżącej, lecz innych klientów ubezpieczyciela, zaś dokumenty te nie pozostają w związku z likwidacją spowodowanej przez osobę skarżącą szkody. Organ ustalił, że w procesie przetwarzania danych nie została spełniona żadna

¹⁵¹ GI-DS-430-510/06.

¹⁵² Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wydanie III, Zakamycze 2004 r., str. 472.

¹⁵³ Zgodnie z art. 3 ust. 1 ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. Nr 124, poz. 1151 z późn. zm.), przez działalność ubezpieczeniową rozumie się wykonywanie czynności ubezpieczeniowych związanych z oferowaniem i udzielaniem ochrony na wypadek ryzyka wystąpienia skutków zdarzeń losowych. Stosownie do art. 3 ust. 4 pkt 2 w zw. z ust. 3 pkt 1 omawianego aktu prawnego, czynnością ubezpieczeniową jest również wypłacanie odszkodowań i innych świadczeń należnych z tytułu umów ubezpieczenia. Z kolei w myśl art. 3 ust. 7 ustawy ubezpieczeniowej czynności, o których mowa w ust. 4 pkt 2 (j.w.) i pkt 5 (prowadzenie postępowań regresowych oraz postępowań windykacyjnych związanych z wykonywaniem umów ubezpieczenia, reasekuracji oraz gwarancji ubezpieczeniowych) oraz ust. 5 pkt 1 (ustalenie przyczyn i okoliczności zdarzeń losowych) i pkt 2 (ustalenie wysokości szkód oraz rozmiaru odszkodowań oraz innych świadczeń należnych), uważa się za czynności ubezpieczeniowe także wtedy, gdy ich wykonywania podejmuje się zakład ubezpieczeń na wniosek innego zakładu ubezpieczeń, Ubezpieczeniowego Funduszu Gwarancyjnego, Polskiego Biura Ubezpieczycieli Komunikacyjnych lub uprawnionego z tytułu umów, o których mowa w art. 3 pkt 1, także gdy umowy te zawarte są z innym zakładem ubezpieczeń.

¹⁵⁴ Decyzja z dnia 21 sierpnia 2007 r. o sygn. GI-DEC-DOLiS-180/07.

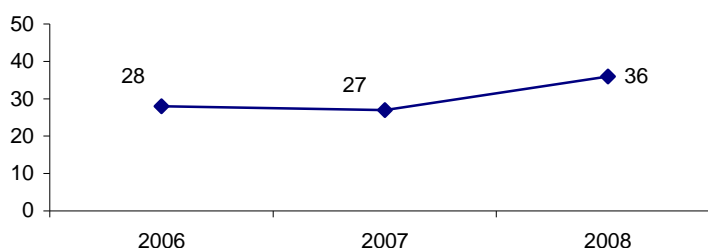
¹⁵⁵ Wyrok z dnia 6 maja 2008 r. sygn. akt II SA/Wa 60/08.

¹⁵⁶ Zawiadomienie z dnia 7 marca 2008 r. o sygn. DOLiS/ZAW-3/08.

przesłanka dopuszczalności przetwarzania danych. Natomiast doszło do udostępnienia danych osobowych klientów ubezpieczyciela osobie nieupoważnionej, jak również naruszono prawa i wolności tych osób, w szczególności ich konstytucyjne prawo do ochrony prawnej życia prywatnego. Działania ubezpieczyciela doprowadziły także do naruszenia art. 26 ust. 1 i art. 36-39 ustawy, tj. obowiązku dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą w zakresie zapewnienia bezpieczeństwa danych w procesie ich przetwarzania. Sprawa została umorzona.

Podkreślenia wymaga, iż w 2008 r. odnotowano spadek liczby zasadnych skarg na niewłaściwe zabezpieczenie danych osobowych przez administratorów danych z tego sektora. Coraz więcej skarg dotyczy natomiast odmowy udostępnienia danych ze swoich zbiorów przez ubezpieczycieli. Najczęściej jednak skargi te nie były zasadne. Administratorzy słusznie odmawiali udostępnienia danych powołując się na brak podstawy prawnej do skutecznego ich żądania. Przyczyn takiego zjawiska upatrywać należy w konsekwentnej polityce Generalnego Inspektora Ochrony Danych Osobowych polegającej na skrupulatnym egzekwowaniu w latach poprzednich przepisów regulujących zasady prawidłowego zabezpieczania danych osobowych przez podmioty z tego sektora.

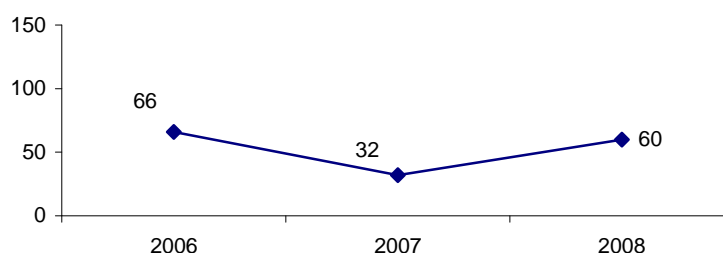
Podsumowując należy zauważyć, że w porównaniu do lat ubiegłych wzrosła liczba skarg dotyczących przetwarzania danych osobowych w sektorze ubezpieczeń (zob. Wykres 9).



Wykres 9.
Zestawienie porównawcze liczby skarg dotyczących sektora ubezpieczeń,
które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

3.2.8 Telekomunikacja

W 2008 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **60 skarg** z tego sektora, co w stosunku do roku poprzedniego stanowi prawie dwukrotny ich wzrost.



Wykres 10.
Zestawienie porównawcze liczby skarg dotyczących sektora telekomunikacji, które wpłynęły
do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

Część z nich dotyczyła kwestii legalności udostępnienia przez operatorów telekomunikacyjnych danych osobowych firmom windykacyjnym¹⁵⁷. W badanych sprawach organ nie dopatrzył się jednak naruszenia ustawy o ochronie danych osobowych. Udostępnienie tym podmiotom danych osobowych odbywało się najczęściej w związku ze zleceniem przeprowadzenia czynności windykacyjnych

¹⁵⁷ Np. DOLiS-440-17/08, DOLiS-440-18/08, DOLiS-440-43/08, DOLiS-440-194/08.

i dokonywane było na podstawie art. 31 ustawy o ochronie danych osobowych,¹⁵⁸ ewentualnie wskutek sprzedaży wierzytelności przysługującej osobie skarżącej. Wtedy zastosowanie znajdowała przesłanka legalnego przetwarzania danych osobowych z art. 23 ust. 1 pkt 5 w zw. z art. 23 ust. 4 tej ustawy.¹⁵⁹ Organ uznał, iż sprzedaż wierzytelności i udostępnienie w związku z tym danych dłużnika jest działaniem w usprawiedliwionym celu administratora danych.

Pojawiły się również sprawy, w których skarżący podnosili niespełnienie przez operatorów telekomunikacyjnych obowiązków informacyjnych z ustawy o ochronie danych osobowych. W jednej z takich spraw¹⁶⁰ organ ds. ochrony danych osobowych wydał decyzję,¹⁶¹ mocą której nakazał operatorowi telefonii komórkowej wypełnienie wobec osoby skarżącej obowiązku informacyjnego z art. 32 ust. 1 pkt. 2, 3 i 4, w zw. z art. 33 ustawy, tj. dotyczącego zakresu, treści oraz czasu pozyskania danych osobowych skarżącego. Mocą tej samej decyzji GODO nakazał zaprzestania udostępniania danych osobowych skarżącego innym operatorom, na potrzeby ustalenia jego zdolności do regulowania płatności z tytułu świadczonych przez te podmioty usług telekomunikacyjnych bez zgody tej osoby. Poza tym operator nie wykazał się żadną przesłanką, w tym przesłanką zgody, dającą podstawę prawną do zakwestionowanego udostępniania danych.

Pojawiły się również skargi w sprawie ujawniania przez operatorów telekomunikacyjnych zastrzeżonych numerów telefonicznych, m.in. poprzez umieszczenie w internetowej książce telefonicznej zastrzeżonych danych osoby skarżącej.¹⁶² Generalny Inspektor Ochrony Danych Osobowych ustalił, że serwis internetowy, na którym ujawniono dane osobowe (imię, nazwisko i numer telefonu) nie należy do operatora telekomunikacyjnego, który świadczy usługi osobie skarżącej, ale został utworzony przez podmiot zagraniczny posługujący się w sposób nieuprawniony bazą danych abonentów operatora. Wskazany serwis został zamieszczony nielegalnie i zawiera dane abonentów pochodzące z książki telefonicznej opublikowanej przez tego operatora i wydanej na płycie CD w 2004 roku. Baza danych abonentów została zamieszczona w internetowej książce telefonicznej na skutek złamania przez podmiot użytkujący ten portal, istniejących zabezpieczeń zastosowanych przez operatora i obecnie administruje zbiorem danych osobowych abonentów w sposób nieuprawniony. Dane osobowe skarżącej zamieszczone w Internecie pochodzą właśnie z książki telefonicznej aktualnej na koniec 2003 r., w której figurowały jako niezastrzeżone. W sprawie tej operator telekomunikacyjny złożył zawiadomienie o podejrzeniu popełnienia przestępstwa. Osoba skarżąca została poinformowana, że w tej sytuacji złożenie analogicznego zawiadomienia przez Generalnego Inspektora byłoby bezprzedmiotowe.

W 2008 r. do GODO wpłynął także wniosek komendanta miejskiego Policji o wyrażenie zgody na uzyskanie przez Policję od operatora telekomunikacyjnego danych osobowych abonenta korzystającego ze zidentyfikowanego numeru telefonu w związku z prowadzeniem sprawy o wykroczenie.¹⁶³ Z treści tego wniosku wynikało, że komendant miejski nie zwracał się wcześniej do tego operatora o udostępnienie danych. Sprawę zakończono zatem informując komendanta, że do zadań Generalnego Inspektora Ochrony Danych Osobowych nie należy wydawanie zgody na udostępnienie danych, lecz wydawanie decyzji administracyjnej ewentualnie nakazującej udostępnienie. Wskazano również, że uprawnienie Policji do pozyskania od operatora telekomunikacyjnego danych osobowych abonenta podejrzanego o popełnienie wykroczenia znajduje uzasadnienie w art. 23 ust. 1 pkt. 2 i 4 ustawy o ochronie danych osobowych, w związku z art. 161 Prawa telekomunikacyjnego, art. 20 ust. 1 ustawy o Policji

¹⁵⁸ 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 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).

¹⁵⁹ Zgodnie z art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy 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. Zgodnie zaś z art. 23 ust. 4 pkt 2 za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 5, uważa się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

¹⁶⁰ GI-DOLiS-430/491/07.

¹⁶¹ Decyzja z dnia 6 marca 2008 r. o sygn. DOLiS/DEC-169/08 – nieprawomocna; wyrok WSA w Warszawie z dnia 26 lutego 2009 r. sygn. akt II SA/Wa 1685/08 – nieprawomocny.

¹⁶² Np. DOLiS-440-168/08, DOLiS-441-15/08, DOLiS-440-898/08.

¹⁶³ DOLiS-440-391/08.

oraz art. 54 § 1 i art. 57 § 2 pkt 1 ustawy Kodeks postępowania w sprawach o wykroczenia. Stanowisko GODO w tej sprawie znalazło potwierdzenie w orzeczeniu Naczelnego Sądu Administracyjnego.¹⁶⁴

Podobnie jak w latach ubiegłych, również w tym roku sprawozdawczym pojawiały się sprawy wykorzystywania przez operatorów telekomunikacyjnych danych osobowych swoich klientów w celach marketingowych bez podstawy prawnej. W większości przypadków okazywało się, że takie działanie miało umocowanie w przepisach ustawy o ochronie danych osobowych, tj. w art. 23 ust. 1 pkt 5 w zw. z art. 23 ust. 4 pkt 2. Pojawiały się jednak również sprawy, w których przetwarzano dane bez oparcia w przepisach ustawy o ochronie danych osobowych. Dla przykładu, GODO wystąpił do dyrektora generalnego jednego z operatorów telekomunikacyjnych o przestrzeganie przepisów ustawy o ochronie danych osobowych podczas wykorzystywania danych osobowych abonentów operatora w celu marketingu produktów lub usług innego podmiotu.¹⁶⁵ Podstawą wystąpienia było ustalenie przez organ, że operator przetwarzał dane osobowe w ww. celu bez uzyskania uprzedniej zgody osoby, której dane te dotyczyły. Operator błędnie przyjął w tym przypadku, że oferta zawarcia umowy kredytowej z innym podmiotem (bankiem) wówczas, gdy za zawarcie takiej umowy klient otrzyma dodatkowy pakiet darmowych minut, nie jest marketingiem produktów lub usług operatora. Tymczasem znajduje tu zastosowanie art. 23 ust. 1 pkt 5 w zw. z art. 23 ust. 4 ustawy o ochronie danych osobowych.

Omawiając sprawy z tego sektora nie można pominąć orzeczenia Wojewódzkiego Sądu Administracyjnego w Warszawie,¹⁶⁶ który po rozpatrzeniu sprawy udostępniania przez operatora telekomunikacyjnego numerów telefonów abonentów prywatnych dobieranych pod kątem potrzeb nabywcy, np. według kryterium geograficznego, stwierdził, że taki zestaw informacji stanowi dane osobowe w rozumieniu ustawy. Sąd wskazał, że zgoda na umieszczenie danych w powszechnie dostępnych spisach abonentów nie może być utożsamiana ze zgodą na udostępnienie danych w celach marketingowych innym podmiotom. Stanowisko to zostało podzielone przez Naczelnego Sąd Administracyjny.¹⁶⁷

Wskazać ponadto należy, iż w przeciwieństwie do lat poprzednich, w 2008 r. Generalny Inspektor Ochrony Danych Osobowych nie stwierdził skarg dotyczących bezprawnego przetwarzania danych osobowych (i udostępnienia ich podmiotom trzecim) w związku z niezasadnym – w ocenie osób skarżących – dochodzeniem należności.

3.2.9 Sektor zatrudnienia

W 2008 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęły **24** skargi na działalność podmiotów z tego sektora. Wśród nich na uwagę zasługuje prawomocnie zakończona sprawa, w której rozważana była kwestia odpowiedzialności za prawidłowe przetwarzanie danych osobowych przez pracownika, któremu pracodawca powierzył dokumentację zawierającą swoje dane osobowe oraz kwestia zachowania zasad bezpieczeństwa danych przez pracodawcę. Sprawa dotyczyła działań byłego pracodawcy, który – w czasie trwania zatrudnienia – powierzył osobie skarżącej pewną ilość egzemplarzy dokumentu wyznaczającego zakres jego obowiązków na określonym stanowisku. Jeden z egzemplarzy ww. dokumentu przeznaczony był dla skarżącego, natomiast pozostałe miały być – po zapoznaniu się z nimi i podpisaniu – zwrócone pracodawcy. Dokument ten w czasie, gdy pozostawał w dyspozycji skarżącego, był przez niego przechowywany w miejscu pracy. Ponieważ w tym czasie doszło do przerobienia treści ww. dokumentu, skarżący zarzucił swojemu pracodawcy, że ten – jako administrator danych zatrudnionych u niego pracowników – nie zapewnił należytych warunków technicznych i organizacyjnych przechowywania ww. dokumentu zawierającego w swej treści dane osobowe, a tym samym naruszył art. 36 ustawy. Decyzje wydane w przedmiotowej sprawie przez GODO (odmowa uwzględnienia wniosku utrzymana w mocy po rozpoznaniu wniosku skarżącego o ponowne rozpatrzenie sprawy) spotkały się z pełną aprobatą zarówno WSA w Warszawie,¹⁶⁸ jak i NSA.¹⁶⁹ Jak podkreśliły ww. sądy: „(...) nie ulega najmniejszej wątpliwości, że osoba, której dane dotyczą, nie jest w niczym ograniczona w dysponowaniu

¹⁶⁴ Wyrok z dnia 5 lutego 2008 r. sygn. akt I OSK 37/07.

¹⁶⁵ Pismo z dnia 15 grudnia 2008 r. o sygn. DOLiS-440-499/08/34679.

¹⁶⁶ Wyrok WSA w Warszawie z dnia 12 listopada 2007 r. sygn. akt II SA/Wa 1252/07.

¹⁶⁷ Wyrok NSA z dnia 26 stycznia 2009 r. sygn. akt I OSK 174/08.

¹⁶⁸ Wyrok z dnia 26 stycznia 2007 r. sygn. akt II SA/Wa 1256/06.

swoimi danymi (...) od chwili przekazania trzech egzemplarzy dokumentu do dyspozycji skarżącego, który to pokwitował, to właśnie na nim spoczywał obowiązek właściwego zabezpieczenia tego dokumentu (...)" . Tym samym ww. sądy przychyliły się do stanowiska GODO, iż w opisanej sprawie administratora danych osobowych nie można czynić odpowiedzialnym (na podstawie art. 36 ustawy) za nienależyte zabezpieczenie danych osobowych.

Na przywołanie zasługuje również sprawa, w której Generalny Inspektor Ochrony Danych Osobowych nakazał jednemu z banków (pracodawcy) zaprzestanie praktyki polegającej na pozyskiwaniu od związku zawodowego funkcjonującego przy tym banku informacji o osobach korzystających z ochrony ww. związku w formie imiennej listy pracowników.¹⁷⁰ Postępowanie w tej sprawie zainicjowało pismo przewodniczącego oraz zastępcy komisji zakładowej związku zawodowego funkcjonującego przy banku, w którym ww. osoby wniosły do Generalnego Inspektora Ochrony Danych Osobowych o wydanie decyzji w sprawie przetwarzania danych osobowych członków związku przez bank.¹⁷¹ Organ ustalił w sprawie, że zastępca dyrektora departamentu kadr banku wystąpił m.in. do przewodniczącego komisji zakładowej związku przy banku o udzielenie informacji w formie wykazu o osobach korzystających z ochrony związku zawodowego. W ocenie komisji zakładowej związku, kierując takie żądanie wykraczono poza zakres upoważnienia zawartego w przepisach prawa.¹⁷² W swojej decyzji Generalny Inspektor Ochrony Danych Osobowych przyjął, że dane osobowe ujawniające przynależność związkową należą do kategorii danych tzw. szczególnie chronionych,¹⁷³ a legitymowanie się przez administratora danych podstawą do gromadzenia danych osobowych w określonym zakresie, nie upoważnia go do zbierania danych w zakresie szerszym, niż jest to niezbędne do realizacji celu, dla którego dane są zbierane.¹⁷⁴ Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swoimi danymi, a interesem administratora danych, który nie może stawiać swego interesu ponad dobro osoby, której dane przetwarza. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane.¹⁷⁵ W sprawie tej powołano również zasady wynikające z przepisów Konstytucji RP,¹⁷⁶ ustawy o związkach zawodowych¹⁷⁷ w związku z przepisami Kodeksu pracy¹⁷⁸ oraz orzecznictwo Trybunału Konstytucyjnego.¹⁷⁹ Organ ds. ochrony danych osobowych przyjął, że przepisy art. 30 ust. 2¹ ustawy o związkach zawodowych oraz art. 23² ustawy Kodeksu pracy, nie upoważniają banku do pozyskiwania od związku zawodowego imiennej listy pracowników korzystających z ochrony ww. związku zawodowego. Pozyskiwanie tego rodzaju danych narusza bowiem jedną z podstawowych zasad przetwarzania danych osobowych, jaką jest zasada adekwatności. Również gromadzenie danych „na zapas” jest niedopuszczalne w świetle przepisów ustawy o ochronie danych osobowych. Organ nie zakwestionował jednak prawa banku do pozyskiwania informacji o pracownikach

¹⁶⁹ Wyrok z dnia 7 maja 2008 r. sygn. akt I OSK 998/07.

¹⁷⁰ Decyzja z dnia 30 czerwca 2008 r. o sygn. DOLIS/DEC-397/08.

¹⁷¹ Powołując się na 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.).

¹⁷² W tym z art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz art. 22¹ ustawy z dnia 26 czerwca 1974 r. Kodeksu pracy (Dz. U. 1998 r. Nr 21 poz. 94 z późn. zm.).

¹⁷³ Wymienionych w art. 27 ust. 1 ustawy.

¹⁷⁴ Art. 26 ust. 1 pkt 3 ustawy.

¹⁷⁵ Jak wskazuje się w literaturze przedmiotu, z przepisu art. 26 ust. 1 pkt 3 ustawy wynika w szczególności zakaz zbierania wszelkich danych dla celu zebrania danych nieistotnych, niemających znaczenia, jak i danych o większym, niż uzasadniony tym celem, stopniu szczególności. Relewantność danych powinna być oceniana najpóźniej w momencie ich zbierania. Zob. J. Barta R. Markiewicz „Ochrona danych osobowych. Komentarz”, Zakamycze 2001, s. 416.

¹⁷⁶ Źródło ochrony danych osobowych to art. 47 i 51 Konstytucji RP.

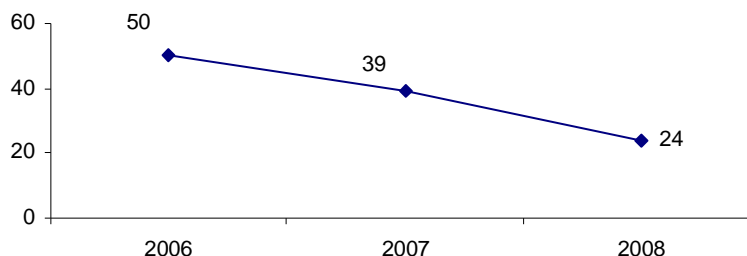
¹⁷⁷ Zgodnie z art. 30 ust. 2¹ ustawy o związkach zawodowych, w indywidualnych sprawach ze stosunku pracy, w których przepisy prawa pracy zobowiązują pracodawcę do współdziałania z zakładową organizacją związkową, pracodawca jest obowiązany zwrócić się do tej organizacji o informację o pracownikach korzystających z jej ochrony, 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.

¹⁷⁸ W art. 23² ustawy Kodeksu pracy, w świetle której, jeżeli przepisy prawa pracy przewidują współdziałanie pracodawcy z zakładową organizacją związkową w indywidualnych sprawach ze stosunku pracy (przepisem takim jest np. art. 38 Kodeksu pracy), pracodawca ma obowiązek współdziałać w takich sprawach z zakładową organizacją związkową reprezentującą pracownika z tytułu jego członkostwa w związku zawodowym albo wyrażenia zgody na obronę praw pracownika niezrzeszonego w związku - zgodnie z ustawą o związkach zawodowych.

¹⁷⁹ Konstytucja RP z 2 kwietnia 1997 r., w przeciwieństwie do poprzednio obowiązujących przepisów konstytucyjnych, wprost normuje prawo do prywatności stanowiąc w art. 47, iż „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”. Konstytucja wprowadza też w art. 51 nową kategorię prawa jednostki do ochrony danych osobowych, w zakres którego wchodzi m.in. warunek ustawowej podstawy ujawnienia przez jednostkę informacji dotyczących jej osoby (...). Przytoczone powyżej przepisy Konstytucji pozostają w określonej relacji wzajemnej: prawo do prywatności, statutowane w art. 47, zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51” (Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r. sygn. akt U. 5/97, opubl. OTK ZU 1998/4 poz. 46 Prokuratura i Prawo - dodatek 1998/9 poz. 51, podobnie Postanowienie Trybunału Konstytucyjnego z dnia 24 czerwca 1998 r. sygn. akt U. 4/97, opubl. OTK ZU 1998/4 poz. 54). Natomiast w wyroku z dnia 24 czerwca 1997 r. Trybunał Konstytucyjny wskazując rangę prawa do prywatności uznał m.in., iż nie ma ono charakteru absolutnego i może podlegać ograniczeniom. Konieczne jest przy tym jednak, by ograniczenia tego prawa formułowane były w sposób czyniący zadość wymaganiom konstytucyjnym. Zdaniem Trybunału Konstytucyjnego oznacza to, że ograniczenie prawa bądź wolności może nastąpić tylko wtedy, jeżeli przemawia za tym inna norma, zasada lub wartość konstytucyjna, a stopień tego ograniczenia musi pozostać w odpowiedniej proporcji do rangi interesu, któremu ograniczenie to ma służyć (Orzeczenie Trybunału Konstytucyjnego z dnia 24 czerwca 1997 r. sygn. akt K. 21/96, opubl. OTK ZU 1997/2 poz. 23, zob. Prokuratura i Prawo - dodatek 1997/10 poz. 60). Z powyższego jednoznacznie wynika, iż przepisy ustawy o ochronie danych osobowych odzwierciedlają konstytucyjne prawo każdej jednostki do ochrony prywatności, tj. prawa do ochrony danych osobowych.

korzystających z ochrony związkowej, tylko sposób jego realizacji. GIODO wskazał przy tym, że bank mając na uwadze unormowania wynikające przede wszystkim z przepisów ustawy o ochronie danych osobowych, powinien realizować prawo z art. 30 ust. 2¹ ustawy o związkach zawodowych poprzez indywidualne wystąpienie odnoszące się do poszczególnego pracownika.¹⁸⁰

W roku sprawozdawczym 2008 odnotowano spadek liczby skarg dotyczących sektora zatrudnienia, co obrazuje Wykres 11.



Wykres 11.
Zestawienie porównawcze liczby skarg dotyczących sektora zatrudnienia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

W porównaniu z latami ubiegłymi skargi dotyczące tego sektora często obejmowały zarzut naruszenia dóbr osobistych osób skarżących bądź nieprawidłowego prowadzenia akt pracowniczych. W każdym z takich przypadków organ ds. 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.

3.2.10 Inne

Wśród skarg, które Generalny Inspektor Ochrony Danych Osobowych badał w 2008 r. wyodrębnić należy te, które z racji swojego przedmiotu nie mogły być zakwalifikowane do wcześniej przedstawionych kategorii spraw.

Najciekawsze z nich to te zainicjowane wnioskami o nakazanie wydawcom gazet udostępnienia danych osobowych dziennikarzy, w celu wystąpienia przez wnioskodawcę z powództwem cywilnym w związku z naruszeniem dóbr osobistych publikacją prasową.¹⁸¹ W większości tego typu wniosków Generalny Inspektor Ochrony Danych Osobowych nakazywał udostępnienie danych, pod warunkiem że wniosek o udostępnienie wypełniał dyspozycję art. 29 ust. 2 ustawy o ochronie danych osobowych,¹⁸² tj. że żądane dane osobowe są niezbędne do wytoczenia powództwa cywilnego przeciwko osobom, których dane te dotyczą. Organ brał w takich sprawach pod uwagę, że dla skuteczności wytoczenia powództwa niezbędne jest wniesienie pozwu, który spełniać powinien warunki określone w art. 187 § 1 Kodeksu postępowania cywilnego. Natomiast w myśl art. 126 § 1 pkt 1 tej ustawy, każde pismo procesowe powinno zawierać, m.in. oznaczenie sądu, do którego jest skierowane, imię i nazwisko lub nazwę stron, ich przedstawicieli ustawowych i pełnomocników. Z regulacji tych wynika, iż niezbędnym elementem pozwu o naruszenie dóbr osobistych jest oznaczenie w nim osoby w zakresie jej adresu zamieszkania, przeciwko której żądanie określone w pozwie jest skierowane. W sprawach kończących się wydaniem nakazu udostępnienia danych, organ wskazywał ponadto na brak możliwości powołania się w sprawie na przeszkodę udostępnienia danych z art. 29 ust. 2 ustawy. Zgodnie z jego brzmieniem, dane osobowe nie mogą być udostępnione w trybie przewidzianym w tym przepisie, jeżeli miałyby to spowodować naruszenie praw i wolności osoby, której dane dotyczą. Generalny Inspektor Ochrony Danych Osobowych

¹⁸⁰ Decyzja z dnia 31 października 2008 r. o sygn. DOLiS/DEC-710/09 - nieprawomocna, sprawa oczekuje na rozpatrzenie przez WSA w Warszawie.

¹⁸¹ Np. DOLiS-440-47/08, DOLiS-440-66/08.

¹⁸² Zgodnie z art. 29 ust. 2 ustawy o ochronie danych osobowych, dane osobowe, z wyłączeniem danych, o których mowa w art. 27 ust. 1, mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w ust. 1, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

stał na stanowisku, że uznanie, iż udostępnienie danych osoby, przeciwko której chce się wytoczyć powództwo cywilne miałyby godzić w jej prawa i wolności, prowadzi do nieuzasadnionej ochrony takiej osoby przed ewentualną odpowiedzialnością za swoje działania, zwłaszcza że może ona w czasie takiego postępowania sądowego w pełni korzystać ze swoich praw zagwarantowanych przepisami Kodeksu postępowania cywilnego.

Generalny Inspektor Ochrony Danych Osobowych wystąpił również z pismem sygnalizującym do jednego z posłów do Parlamentu Europejskiego, który na swojej stronie internetowej umieścił formularz do wypełnienia przez osoby zainteresowane kierowaniem do niego korespondencji drogą elektroniczną.¹⁸³ Warunkiem wysłania owej korespondencji było nie tylko podanie danych obejmujących podstawowe informacje, takie jak imię, nazwisko i adres e-mail, ale również informację o wieku oraz nazwie miejscowości i województwa, w którym dana osoba zamieszkuje. Ponadto konieczne do przesłania korespondencji było wyrażenie ogólnej zgody na przetwarzanie danych osobowych przez jedną z partii politycznych. W tym przypadku organ uznał za konieczne dostosowanie procesu przetwarzania pozyskiwanych w ten sposób danych do wymogów ustawy o ochronie danych osobowych, w szczególności poprzez umieszczenie w formularzu informacji, w jakim celu dane będą przetwarzane. Ponadto zwrócono uwagę na zasadę adekwatności (dostosowania zakresu przetwarzania danych do celu) i wskazano, że skoro dane pozyskane z formularza wymagane były jedynie do przesyłania korespondencji, to pozyskiwanie danych dotyczących wieku oraz miejscowości i województwa zamieszkania nadawcy korespondencji, prowadzić może do naruszenia wspomnianej zasady.¹⁸⁴ W związku z wystąpieniem Generalnego Inspektora Ochrony Danych Osobowych zaprzestano kwestionowanej praktyki.

Organ interweniował również w sprawie przetwarzania danych osobowych przez Polski Komitet Narodowy UNICEF za pomocą formularza umieszczonego na stronie internetowej www.unicef.pl. Każda osoba, która chciała dokonać wpłat na wsparcie kampanii prowadzonych przez tę organizację, musiała wyrazić zgodę na przetwarzanie danych pozyskanych za pomocą owego formularza „w celu obsługi transakcji oraz w celach marketingowych.” W tym wypadku GODO wystąpił do ww. podmiotu o sprecyzowanie, czy zgoda dotyczy marketingu własnych produktów bądź usług, czy marketingu produktów bądź usług podmiotów trzecich, oraz wskazał, że przypadku, gdy ma miejsce ta druga okoliczność, konieczne jest umieszczenie stosownej informacji w tym zakresie w treści formularza.¹⁸⁵ Uwagi organu zostały uwzględnione przez ww. podmiot.¹⁸⁶

Generalny Inspektor Ochrony Danych Osobowych wystąpił również z wnioskiem do dyrektora zespołu szkół z oddziałami integracyjnymi o nieudostępnianie poradni neurologicznej niepublicznego zakładu opieki zdrowotnej¹⁸⁷ danych osobowych ucznia bez zgody jego ustawowego przedstawiciela. Generalny Inspektor Ochrony Danych Osobowych zaakcentował w tej sprawie, że wszelkie działania związane z przetwarzaniem danych osobowych dla potrzeb organizowania przedsięwzięć mających na celu ułatwianie dzieciom dostępu do specjalistycznych, bezpłatnych badań i terapii, powinny znajdować oparcie w obowiązujących przepisach prawa, w tym przepisach ustawy o ochronie danych osobowych. W sytuacji braku innej przesłanki niż zgoda, przy przetwarzaniu danych osób nie posiadających pełnej zdolności do czynności prawnych, administrator zachować powinien zasady wynikające z przepisu definicji zgody (art. 7 pkt 5 ustawy) oraz zasadę zabezpieczenia danych osobowych z art. 36 ustawy. Adresat wystąpienia Generalnego Inspektora Ochrony Danych Osobowych uwzględnił wskazania co do legalności przetwarzania danych osobowych.¹⁸⁸

Warto ponadto wspomnieć o tym, że Generalny Inspektor Ochrony Danych Osobowych wystąpił z zawiadomieniem o podejrzeniu popełnienia przestępstwa określonego w art. 49 ust. 1 i 51 ust. 1 ustawy o ochronie danych osobowych, polegającego na przetwarzaniu danych osobowych skarżącego bez podstawy prawnej oraz udostępnienia (umożliwienia dostępu) jego danych osobowych osobom nieuprawnionym.¹⁸⁹ Zawiadomienie zostało skierowane na skutek skargi uczestnika wypadku samochodowego, który został przewieziony do Samodzielnego Publicznego Zakładu Opieki Zdrowotnej, gdzie na izbie przyjęć zostały spisane jego dane osobowe w celu założenia karty informacyjnej. Po około 2 tygodniach od zdarzenia, do osoby skarżącej zadzwoniono ze stowarzyszenia pomocy osobom poszkodowanym w wypadkach z ofertą pomocy w uzyskaniu odszkodowania

¹⁸³ DOLiS-035-47/07.

¹⁸⁴ Pismo z dnia 8 stycznia 2008 r. o sygn. DOLiS-035-47/07/330/08.

¹⁸⁵ Pismo z dnia 15 stycznia 2008 r. o sygn. DOLiS-440-221/07/873/08.

¹⁸⁶ GODO został poinformowany pismem z dnia 29 września 2008 r.

¹⁸⁷ Sygnalizacja z dnia 30 kwietnia 2008 r. o sygn. DOLiS-440-109/08.

¹⁸⁸ Pismo z dnia 3 września 2008 r.

¹⁸⁹ Zawiadomienie z dnia 17 czerwca 2008 r. o sygn. DOLiS/ZAW-13/08.

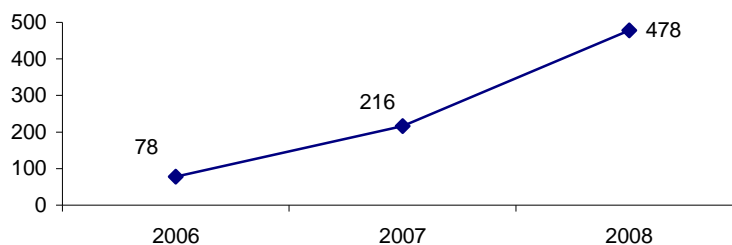
od ubezpieczyciela oraz poinformowano, że jego dane pozyskano ze szpitala, w którym udzielono mu pomocy medycznej po wypadku. Rozmówczyni miała być pracownikiem tego szpitala (tak poinformowała osobę skarżącą). Na podstawie zgromadzonego w sprawie materiału dowodowego Generalny Inspektor Ochrony Danych Osobowych przyjął, że w sprawie zachodzi uzasadnione podejrzenie popełnienia przestępstwa spenalizowanego w art. 49 ust. 1 oraz art. 51 ust. 1 ustawy, gdyż osoba skarżąca bez wątplenia udostępniła swoje dane szpitalowi, ale nie udzieliła temu podmiotowi zgody na udostępnienie jego danych osobowych podmiotom trzecim, co mogło mieć miejsce w tym przypadku. Prokuratura umorzyła dochodzenie w niniejszej sprawie.¹⁹⁰ Generalny Inspektor Ochrony Danych Osobowych nie dysponuje ustawowymi instrumentami do spowodowania weryfikacji tego postanowienia.

Podobnie organ postąpił w sprawie podejrzenia bezprawnego udostępniania przez szpital danych osobowych ofiar wypadków komunikacyjnych firmie, która przedstawiała tym pacjentom ofertę reprezentowania ich w postępowaniu odszkodowawczym wobec sprawcy wypadku.¹⁹¹ Prokuratura odmówiła wszczęcia dochodzenia, gdyż postępowanie o ten sam czyn zostało prawomocnie zakończone umorzeniem.¹⁹²

W 2008 r. Generalny Inspektor Ochrony Danych Osobowych wystąpił do prezesa zarządu spółki akcyjnej o zmianę klauzuli zgody wprowadzonej w kuponie rabatowym, będącym elementem reklamy podpisu elektronicznego.¹⁹³ Wskazał przy tym, że pozyskiwanie zgody na przetwarzanie danych osobowych w celu marketingowym na potrzeby reklamy własnych usług i produktów nie jest niezbędne, natomiast obowiązek taki istnieje, jeżeli dane mają być przetwarzane dla ww. wskazanych celów innych podmiotów niż spółka, lub też, gdy mają być tym podmiotom przekazywane. W wystąpieniu tym wskazano również, że prawidłowe wykonanie obowiązku informacyjnego z art. 24 ust. 1 ustawy polega na przekazaniu wszelkich informacji, o których mowa w tym przepisie. Spółka w odpowiedzi na ww. pismo¹⁹⁴ podziękowała za wskazanie uchybień i przekazanie informacji, które stanowią dla niej cenną wskazówkę zarówno w bieżących, jak i przyszłych działaniach. Poinformowała również, że akcja promocyjna prowadzona za pomocą przedmiotowego kuponu została zakończona, a uzyskiwanie zgody na podstawie błędnie sformułowanej klauzuli nie jest i nie będzie prowadzone.

We wrześniu 2008 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną nakazującą okręgowemu zarządowi działkowców udostępnienie burmistrzowi danych osobowych wszystkich użytkowników działek rodzinnego ogrodu działkowego w zakresie imienia, nazwiska, adresu zamieszkania oraz powierzchni użytkowanych przez nich domków. Organ podjął takie rozstrzygnięcie, gdyż dane te były burmistrzowi niezbędne w celu wszczęcia postępowania podatkowego (w trybie art. 82 Ordynacji podatkowej), mającego w szczególności doprowadzić do ustalenia, czy ww. użytkownicy działek podlegają opodatkowaniu podatkiem od nieruchomości domków wybudowanych na terenie ogrodu działkowego.¹⁹⁵

W analizowanym okresie, w stosunku do roku poprzedniego, ponad dwukrotnie wzrosła liczba skarg dotyczących przetwarzania danych osobowych w szeroko rozumianym sektorze „Inne”, co przedstawia poniższy Wykres 12.



Wykres 12.
Zestawienie porównawcze liczby skarg z sektora „Inne”, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006–2008.

¹⁹⁰ Postanowienie Prokuratury z dnia 30 czerwca 2008 r.

¹⁹¹ Pismo z dnia 1 grudnia 2008 r. o sygn. DOLiS/ZAW-26/08/33059.

¹⁹² Postanowienie Prokuratury z dnia 17 grudnia 2008 r. sygn. akt 2 Ds 507/08

¹⁹³ Wystąpienie z dnia 7 sierpnia 2008 r. o sygn. DOLiS-440-579/08.

¹⁹⁴ Pismo (bez daty), które wpłynęło do GIODO w dniu 3 września 2008 r. znak: AO/0805-03/2008.

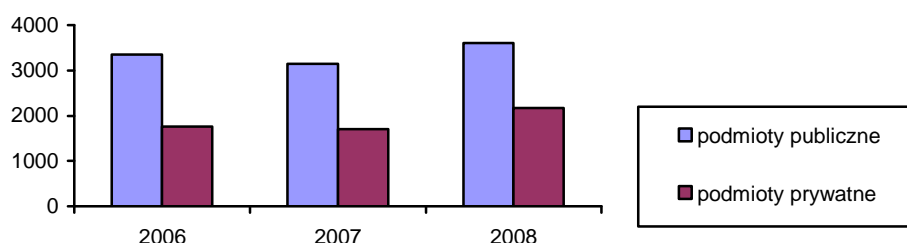
¹⁹⁵ Decyzja z dnia 17 września 2008 r. o sygn. DOLiS/DEC-546/08 – nieprawomocna; wyrok WSA w Warszawie z dnia 27 kwietnia 2009 r. sygn. akt II SA/Wa 1614/08 – nieprawomocny.

Podsumowując powyższy rozdział należy odnotować, iż mimo dużej liczby skarg, które wpłynęły do GIODO 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 GIODO zmierzającej do upowszechnienia wiedzy o prawach i obowiązkach zarówno administratorów danych, jak i osób, których dane dotyczą.

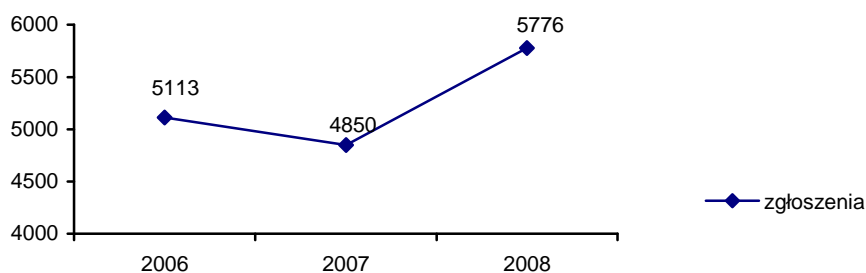
4. Prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach

Generalny Inspektor Ochrony Danych Osobowych w ramach swoich ustawowych zadań prowadzi rejestr zbiorów danych oraz udziela informacji o zarejestrowanych zbiorach.¹⁹⁶ Zadanie to, realizowane w Departamencie Rejestracji Zbiorów Danych Osobowych, skorelowane zostało z nałożonym na administratorów danych obowiązkiem zgłaszania zbiorów danych osobowych do rejestracji.¹⁹⁷ Prowadzenie ogólnokrajowego rejestru umożliwia Generalnemu Inspektorowi Ochrony Danych Osobowych 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 Generalnego Inspektora Ochrony Danych Osobowych (www.giodo.gov.pl) w ramach Platformy e-GIODO, zamieszczone są informacje o zarejestrowanych zbiorach danych osobowych, umożliwiające wyszukiwanie zbiorów danych według podstawowych kryteriów, m.in. nazwy administratora danych, miejscowości czy też nazwy zbioru danych.

W roku 2008 r. administratorzy danych zgłosili do rejestracji **5776 zbiorów**, z czego podmioty z sektora administracji publicznej zgłosiły 3602 zbiory, co stanowi 62% ogólnej liczby zgłoszeń dokonanych w tym okresie, a podmioty z sektora prywatnego 2174 zbiory, co stanowi 38% ogólniej liczby zgłoszonych zbiorów.



Wykres 13.
Zestawienie zbiorów danych zgłoszonych do rejestracji przez podmioty z sektora publicznego i sektora prywatnego w latach 2006-2008.



Wykres 14.
Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2006-2008.

¹⁹⁶ Zadania Generalnego Inspektora Ochrony Danych Osobowych zostały określone w art. 12 ustawy.

¹⁹⁷ Zgodnie z art. 40 ustawy o ochronie danych osobowych, administrator danych obowiązany jest zgłosić zbiór danych do rejestracji, z wyjątkiem przypadków określonych w art. 43 ust. 1 ustawy.

Zauważalny jest zatem znaczny wzrost liczby zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych, w porównaniu z ubiegłymi latami. Wynika on ze wzrostu świadomości prawnej w zakresie ochrony danych osobowych, w tym obowiązku rejestracji zbiorów danych osobowych. Dzięki możliwości zgłaszania zbiorów drogą elektroniczną, spełnienie tego obowiązku stało się łatwiejsze i szybsze.

Wśród zgłoszeń dokonanych przez podmioty z sektora publicznego dominującymi pod względem ilościowym były zgłoszenia zbiorów danych prowadzone na podstawie przepisów ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów.¹⁹⁸ Przepisy powołanej ustawy wprowadziły nowe zasady przyznawania świadczeń alimentacyjnych, co z kolei doprowadziło w analizowanym roku sprawozdawczym do wzrostu liczby zgłoszeń zbiorów danych osobowych dotyczących danych osób uprawnionych do alimentów.

W porównaniu z ubiegłymi latami odnotować należy liczne zgłoszenia pochodzące od jednostek samorządu terytorialnego (gmin i powiatów). Zanotowano wzrost zgłoszeń zbiorów danych osobowych przesyłanych przez przedsiębiorców, którzy - przetwarzając dane osobowe - wykorzystują sieć Internet. Przedsiębiorcy dostrzegają, iż prowadząc swoją działalność z wykorzystaniem Internetu gromadzą dane osobowe i tworzą zbiory danych osobowych podlegające obowiązkowi zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. W 2008 r. zbiory związane z siecią Internet dotyczyły głównie sklepów internetowych, newsletterów i serwisów randkowych.

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 o ochronie danych osobowych. Z obowiązku rejestracji byli wyłączeni np. administratorzy danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, zbiorów dotyczących osób korzystających z usług medycznych administratora danych, jak również zbiorów danych osobowych obecnych i byłych pracowników administratora danych, zbiory danych osób ubiegających się o zatrudnienie u administratora danych (kandydaci do pracy) i zbiorów danych osób uczących się. W 2008 roku Generalny Inspektor Ochrony Danych Osobowych przygotował **135 pism** informujących administratorów danych o braku obowiązku rejestracji zbioru, wynikającym z jednej z przesłanek określonych we wspomnianym art. 43 ustawy.

Zgłoszenia do rejestracji nadesłało również **75** podmiotów, które nie są administratorami danych zgromadzonych w zgłoszonych zbiorach. Przede wszystkim były to podmioty, którym administratorzy danych powierzyli przetwarzanie danych na podstawie art. 31 ustawy. Do tych wnioskodawców Generalny Inspektor Ochrony Danych Osobowych kierował pisma informujące o braku obowiązku rejestracyjnego z ich strony.

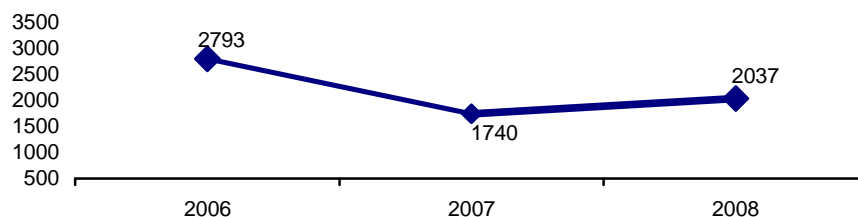
Do GODO wpłynęło ponadto **18** zgłoszeń zbiorów danych, w stosunku do których przepisy ustawy o ochronie danych osobowych nie mają zastosowania. Były to zgłoszenia zbiorów danych przedsiębiorców ściśle związanych z prowadzoną przez nich działalnością gospodarczą,¹⁹⁹ a także zgłoszenia zbiorów pochodzące od podmiotów, które nie mają siedziby na terytorium Rzeczypospolitej Polskiej, ani w państwie trzecim, tj. nienależącym do Europejskiego Obszaru Gospodarczego.²⁰⁰

Należy zauważyć, iż w dalszym ciągu administratorzy danych przetwarzanych w zbiorach podlegających obowiązkowi zgłoszenia do rejestracji przy wypełnianiu formularza zgłoszenia popełniają wiele błędów. W okresie sprawozdawczym, w toku prowadzonych postępowań rejestracyjnych, skierowano do wnioskodawców **2037 pism** wskazujących braki w nadesłanych zgłoszeniach.

¹⁹⁸ Dz. U. Nr 192, poz. 1378 z późn. zm.

¹⁹⁹ W myśl art. 6 ust. 1 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Oznacza to, że zakresem przedmiotowym ustawy o ochronie danych osobowych objęte są wyłącznie dane dotyczące osób fizycznych. Dlatego w sytuacji, gdy w zbiorach zawarte są informacje dotyczące przedsiębiorców i nie wykraczają one poza zakres identyfikujący przedsiębiorców (znajdujące się w jawnych rejestrach, tj. Krajowym Rejestrze Sądowym oraz w ewidencji działalności gospodarczej oraz są ściśle związane z prowadzoną przez nich działalnością gospodarczą) to wobec takich zbiorów ustawa o ochronie danych osobowych nie ma zastosowania. Natomiast, jeżeli administrator przetwarza więcej danych niż jest to niezbędne do identyfikacji przedsiębiorcy, zbiór takich danych podlega ochronie na podstawie przepisów ustawy o ochronie danych osobowych, a administrator danych jest zobowiązany zgłosić go do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

²⁰⁰ Zgłoszenie nr R 005155/08.



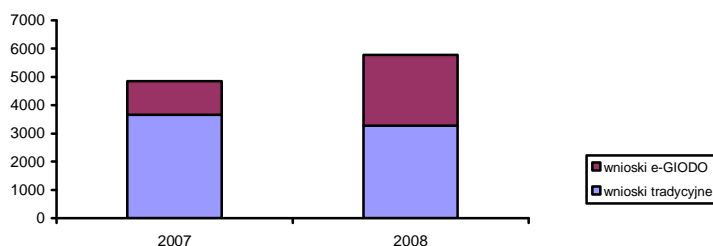
Wykres 15.
Zestawienie liczby pism wysłanych w toku postępowania rejestracyjnego w latach 2006-2008 r.

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 każda z powołanych danych w sposób jednoznaczny umożliwia identyfikację 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 ustawy²⁰¹ - 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 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 korespondencji wysyłanej w toku postępowania rejestracyjnego zamieszczana była informacja o możliwości wypełniania zgłoszeń przy użyciu tego programu. Ponadto podczas konsultacji telefonicznych GODO informował o sposobie korzystania z tego programu. Wobec powyższego, w okresie sprawozdawczym zanotowano znaczny wzrost liczby zgłoszeń zbiorów danych osobowych wypełnionych przy użyciu ww. programu. Od momentu uruchomienia programu do końca 2006 r. odsetek zgłoszeń wypełnionych z użyciem programu udostępnionego na platformie e-GIODO wyniósł 16% (370 zgłoszeń), w roku 2007 r. 25% (1189). Natomiast w 2008 roku, na 5776 zgłoszeń 2499 zostało wypełnionych z zastosowaniem programu wspomagającego wypełnianie formularza zgłoszenia, co stanowi 43% wszystkich zgłoszeń dokonanych w omawianym okresie sprawozdawczym. W roku 2008 zanotowano wzrost (w porównaniu do roku 2007 r. o 18%) liczby zgłoszeń zbiorów danych osobowych wypełnionych przy użyciu ww. programu.

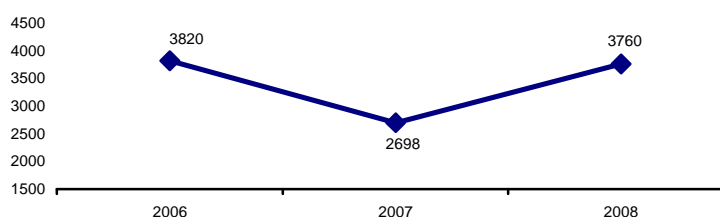
²⁰¹ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).



Wykres 16.
Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2007-2008 w formie tradycyjnej i przy użyciu programu wspomagającego, udostępnionego na stronie www.giodo.gov.pl

Mimo iż program wspomagający wypełnianie formularza zgłoszenia cieszy się dużym zainteresowaniem administratorów danych, to jednak należy zauważyć, iż tylko 308 zgłoszeń w roku sprawozdawczym zostało złożonych z użyciem bezpiecznego podpisu elektronicznego, co stanowi zaledwie 12% zgłoszeń wypełnionych przy użyciu tego programu. W większości przypadków zgłoszenia wypełnione z wykorzystaniem tego programu, po wydrukowaniu były przysyłane przez wnioskodawców w formie papierowej za pośrednictwem poczty lub składane osobiście w siedzibie Generalnego Inspektora. Dlatego też w roku sprawozdawczym 2008 dokonano modyfikacji programu wspomagającego wypełnianie formularza zgłoszenia, która polega na tym, iż zgłoszenie wnioskodawca może wysłać drogą elektroniczną również wtedy, gdy nie dysponuje bezpiecznym podpisem elektronicznym. Jednakże w takim przypadku należy opatrzyć wydruk zgłoszenia przesłanego elektronicznie podpisem i pieczętą wnioskodawcy, i następnie przesłać pocztą lub złożyć w siedzibie Generalnego Inspektora.²⁰²

W okresie sprawozdawczym 2008 do rejestru prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych zostało wpisanych 3760 zbiorów danych.



Wykres 17.
Zestawienie porównawcze zarejestrowanych przez GIODO zbiorów danych osobowych w latach 2006 - 2008.

Wypełnianie formularza przy użyciu programu wspomagającego pozwala uniknąć popełnienia wielu błędów, w szczególności dotyczących spełniania wymagań technicznych i organizacyjnych zastosowanych w celu zabezpieczenia zbioru danych osobowych - część E i F zgłoszenia. Niemniej jednak ww. program nie jest w stanie wyeliminować wszystkich uchybień. Nadal znaczna liczba zgłoszeń zawiera nieprawidłowości, zarówno formalne (np. brak podpisu pod treścią zgłoszenia), jak i merytoryczne.

²⁰² Zgodnie z treścią z art. 63 § 3 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.), podanie wniesione pisemnie (...) powinno być podpisane przez wnoszącego.

W 2008 r. Generalny Inspektor Ochrony Danych Osobowych najczęściej odmawiał rejestracji zgłoszonego zbioru ze względu na:

- naruszenie zasad ochrony danych osobowych, np. brak przesłanki legalności przetwarzania danych, nieadekwatność przetwarzania danych w stosunku do celu ich przetwarzania,²⁰³ przetwarzanie danych wrażliwych²⁰⁴ bez podstawy prawnej,
- niespełnienie wymogów rozporządzenia wykonawczego do ustawy,²⁰⁵ tj. deklarowany w zgłoszeniu przez administratorów danych poziom bezpieczeństwa przetwarzania danych w systemie informatycznym nie spełniał warunków określonych w przepisach rozporządzenia wydanego na podstawie art. 39a ustawy o ochronie danych osobowych,
- brak wyczerpującego opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy o ochronie danych osobowych, w szczególności informacji dotyczących opracowania i wdrożenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki ich ochrony, wyznaczenia administratora bezpieczeństwa informacji, nadania upoważnień osobom dopuszczonym do przetwarzania danych osobowych, a także prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

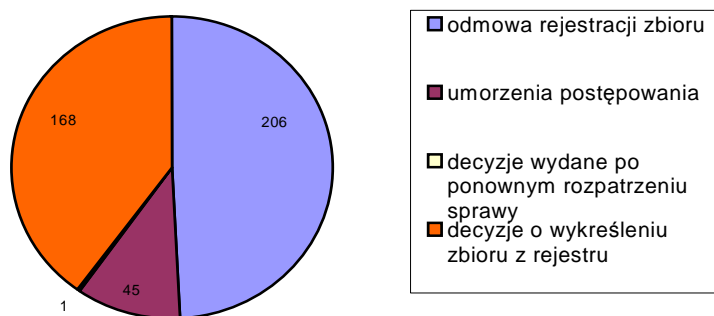
Na dokumentację opisującą sposób przetwarzania danych osobowych oraz środki ich ochrony składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym, jeśli dane są przetwarzane w takim systemie. Administratorzy danych, dokonując zgłoszenia zbioru danych do rejestracji, często mylnie przyjmują, że obowiązek opracowania i wdrożenia polityki bezpieczeństwa nie dotyczy zbiorów danych prowadzonych w formie papierowej. Tymczasem obowiązek ten, przewidziany w art. 36 ust. 2 ustawy o ochronie danych osobowych w związku z § 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych, dotyczy zarówno zbiorów danych prowadzonych w formie elektronicznej, jak i papierowej. Przy czym zakres informacji zawartych w polityce bezpieczeństwa będzie inny w odniesieniu do zbiorów danych prowadzonych w formie papierowej, inny zaś – w przypadku zbiorów danych prowadzonych w formie elektronicznej. Dla przykładu, w polityce bezpieczeństwa opracowanej dla zbioru danych prowadzonego w formie papierowej nie znajdują się informacje o sposobie przepływu danych pomiędzy poszczególnymi systemami.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **206 decyzji o odmowie rejestracji zbioru danych** oraz **45 decyzji o umorzeniu postępowania** (np. ze względu na zaprzestanie przetwarzania danych w zbiorze niewpisanym jeszcze do rejestru czy też rezygnację z utworzenia zbioru). W 2008 roku GODO przygotował także projekty **100 postanowień**.

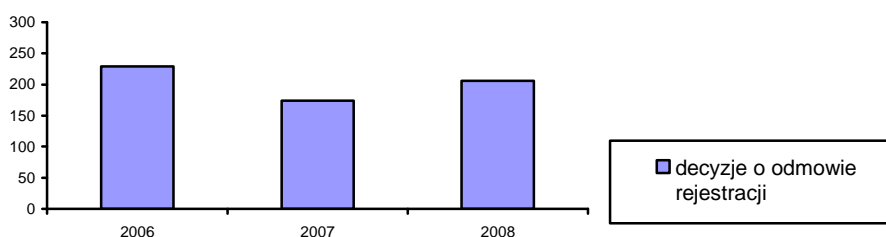
²⁰³ Zgłoszenie nr R 003041/08.

²⁰⁴ Dane osobowe wrażliwe to 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 nalogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

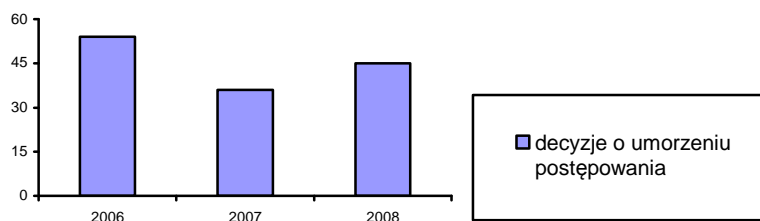
²⁰⁵ Zgodnie z § 6 rozporządzenia, wprowadzone zostały trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: podstawowy, podwyższony oraz wysoki. Brak odpowiedniego poziomu bezpieczeństwa stanowi przesłankę odmowy rejestracji zgłoszonego zbioru danych, o której mowa w art. 44 ust. 1 pkt 3 ustawy. Przetwarzanie danych osobowych przy użyciu sieci Internet powoduje obowiązek zastosowania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych w prowadzonych zbiorach. Poziom wysoki stosuje się bowiem wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną (§ 6 ust. 4 rozporządzenia).



Wykres 18.
Liczbowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2008 r.

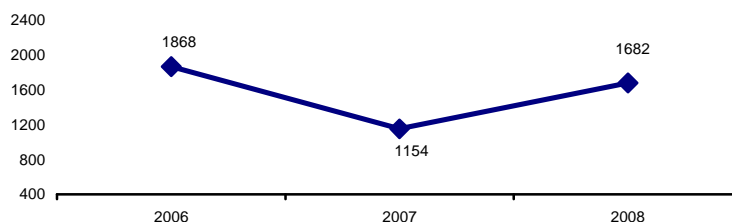


Wykres 19.
Zestawienie porównawcze decyzji o odmowie rejestracji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.



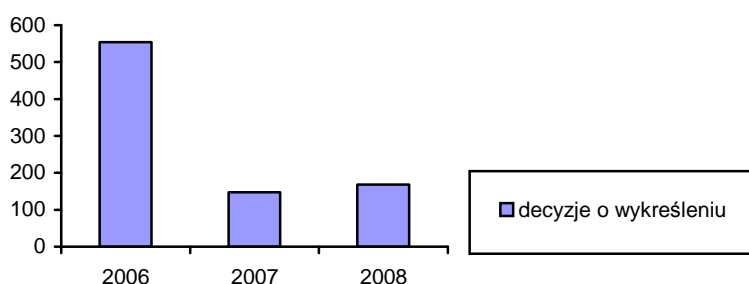
Wykres 20.
Zestawienie porównawcze decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

W roku sprawozdawczym 2008, GODO rozpatrzył **1682 zgłoszenia aktualizacyjne** dokonane przez administratorów danych w trybie art. 41 ust. 2 ustawy o ochronie danych osobowych. Aktualizacje najczęściej dotyczyły zmiany siedziby administratora danych, zmiany zakresu przetwarzanych danych, a także zmian dotyczących środków technicznych i organizacyjnych zastosowanych w celu ochrony przetwarzanych danych osobowych (głównie chodziło 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).



Wykres 21.
Zestawienie porównawcze zgłoszeń aktualizacyjnych rozpatrzonych przez GIODO w latach 2006–2008.

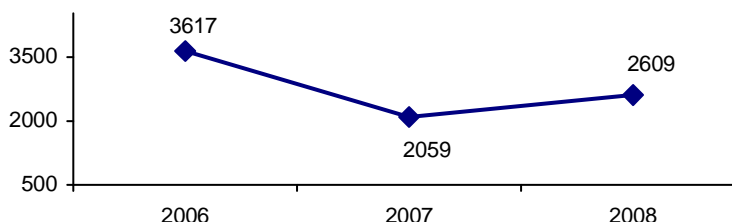
W analizowanym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **168 decyzji o wykreśleniu** zbioru danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych. We wszystkich tych decyzjach przesłanką wykreślenia było zaprzestanie przetwarzania danych w zarejestrowanym zbiorze.



Wykres 22.
Zestawienie porównawcze decyzji o wykreśleniu zbioru danych z rejestru zbiorów danych osobowych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2006–2008.

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 zbiorów danych osobowych realizowana jest poprzez zapewnienie możliwości przeglądania rejestru w Internecie lub w siedzibie Biura Generalnego Inspektora Ochrony Danych Osobowych.

W omawianym okresie Generalny Inspektor Ochrony Danych Osobowych wydał ponadto z urzędu bądź na żądanie administratora danych **2609 zaświadczeń o zarejestrowaniu zbioru**.



Wykres 23.
Zestawienie porównawcze liczby zaświadczeń o zarejestrowaniu zbioru danych osobowych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2006–2008.

Ze względu na duże zainteresowanie problematyką ochrony danych osobowych, w 2008 roku wpływało - głównie drogą elektroniczną - wiele pytań dotyczących rejestracji zbiorów danych osobowych. Wobec powyższego, w okresie tym DRZDO przygotował **40 odpowiedzi na zapytania** dotyczące problematyki rejestracji zbiorów.

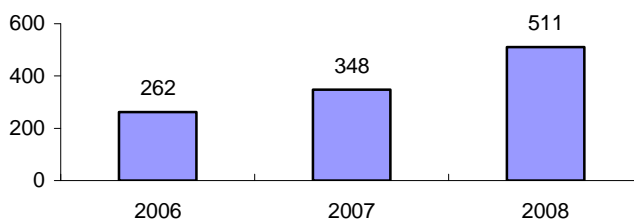
Przepisy o ochronie danych osobowych określają elementy, które pozwalają scharakteryzować zbiór danych osobowych, m.in. cel, dla którego zbiór danych osobowych jest tworzony, podstawę prawną upoważniającą do prowadzenia zbioru, jak również

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 roku sprawozdawczym w praktyce reguła ta przysparzała administratorom danych wiele trudności. Nadsyłane do rejestracji zgłoszenia często faktycznie dotyczyły kilku zbiorów danych osobowych. Postępowania wyjaśniające w takich sprawach miały więc na celu spowodowanie, aby administrator danych prawidłowo dokonał zgłoszenia zbiorów, czyli zgłosił każdy z nich na odrębnym formularzu. Tylko wówczas można mówić, że administrator danych wykonał ciążący na nim z mocy art. 40 ustawy o ochronie danych osobowych, obowiązek zgłoszenia zbioru do rejestracji.

5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych

Na wyeliminowanie licznych – jak wskazuje praktyka – nieprawidłowości już na etapie samego procesu tworzenia prawa pozwala uprawnienie zastrzeżone na rzecz Generalnego Inspektora w art. 12 ust. 4 ustawy o ochronie danych osobowych. Stosownie do treści tego przepisu, do zadań Generalnego Inspektora należy m.in. opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych.

W analizowanym okresie sprawozdawczym do Biura Generalnego Inspektora wpłynęło do zaopiniowania **511 projektów aktów prawnych**, a zatem o 163 więcej niż w roku poprzednim.



Wykres 24.

Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2006-2008.

Jak co roku, nieprawidłowości z punktu widzenia przepisów ustawy o ochronie danych osobowych najczęściej dotyczyły braku doprecyzowania zakresu przetwarzania danych osobowych. Projektodawcy wychodzili bowiem z założenia, że sformułowanie takie, jak np. „wniosek zawiera dane osobowe wnioskodawcy”, „do rejestru wpisuje się dane osobowe” jest wystarczający dla uznania prawidłowości jego brzmienia z punktu widzenia ochrony danych osobowych.²⁰⁶ Generalny Inspektor w takich sytuacjach podkreślał, iż każdorazowo przepis prawa odnoszący się do przetwarzania danych osobowych powinien wprost wskazywać zakres informacji, jakie na jego podstawie mają być przetwarzane. W przeciwnym razie zachodzi ryzyko przedkładania przez osoby, których dane dotyczą, lub żądania przez administratorów danych, informacji nieadekwatnych do rzeczywistego celu przetwarzania danych i tym samym naruszenia jednej z naczelnnych zasad wynikających z przepisów o ich ochronie, a mianowicie zasady adekwatności danych w stosunku do celów ich przetwarzania.²⁰⁷

W okresie objętym sprawozdaniem Generalny Inspektor opiniował m.in. **projekt ustawy o zmianie ustawy – Prawo o postępowaniu przed sądami administracyjnymi**.²⁰⁸ Z zadowoleniem przyjął zawartą w przygotowanym przez Ministerstwo

²⁰⁶ Np. projekt ustawy o emeryturach pomostowych (o sygn. DOLiS-033-187/08) w art. 35 ust. 3 pkt 2 przewidywał, iż centralny rejestr pracowników wykonujących prace w szczególnych warunkach lub o szczególnym charakterze zawiera dane dotyczące pracownika, za którego istniał obowiązek opłacania składek na Fundusz Emerytur Pomostowych; uwagę Generalnego Inspektora uwzględniono, a projekt opublikowano w Dzienniku Ustaw z 2008 r. Nr 237, poz. 1656; lub projekt rozporządzenia Ministra Infrastruktury w sprawie wymagań dotyczących prowadzenia ośrodka doskonalenia techniki jazdy, egzaminowania kandydatów na instruktorów techniki jazdy, postępowania z dokumentacją związaną z prowadzeniem szkoleń oraz wzorów stosownych dokumentów (o sygn. DOLiS-033-61/08), który nie określał danych osobowych członków Komisji Egzaminacyjnej, jakie mają być zamieszczane w protokole sporządzanym po zakończeniu egzaminu instruktorskiego (§ 12 ust. 1 pkt 1b); uwagi Generalnego Inspektora zostały uwzględnione, zaś projekt opublikowano w Dzienniku Ustaw z 2008 r. Nr 77, poz. 458.

²⁰⁷ Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

²⁰⁸ DOLiS-033-126/08.

Sprawiedliwości projekcie ustawy propozycję²⁰⁹ przyznania organowi do spraw ochrony danych osobowych kompetencji występowania do Naczelnego Sądu Administracyjnego z wnioskiem o podjęcie uchwały mającej na celu wyjaśnienie przepisów prawnych, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych.²¹⁰

W projekcie uzasadnienia do nowelizacji ww. przepisu, przygotowanego na prośbę Ministerstwa Sprawiedliwości, Generalny Inspektor podkreślił, iż standardy ochrony danych osobowych są wypracowywane także w drodze orzeczeń sądów administracyjnych. Przypomnił choćby istniejące w orzecznictwie tych sądów rozbieżności w kwestii dopuszczalności przetwarzania danych osobowych w związku z przelewem wierzycelności, rozstrzygnięte dopiero wyrokiem składu Siedmiu Sędziów Naczelnego Sądu Administracyjnego.²¹¹ Jednocześnie zaznaczył, iż nie ulega wątpliwości, że wraz z rozszerzaniem się kompetencji organu do spraw ochrony danych osobowych na kolejne dziedziny obrotu prawnego,²¹² liczba zagadnień spornych dotyczących zasad ochrony danych osobowych będzie systematycznie rosła. Wobec powyższego przyznanie GODO kompetencji do występowania do Naczelnego Sądu Administracyjnego o podjęcie uchwał o charakterze abstrakcyjnym, czyli oderwanym od realiów konkretnej sprawy sądowo-administracyjnej, zdecydowanie przyspieszy opracowanie standardów ochrony danych w tych nowych działaniach.

Generalny Inspektor wypowiedział się również w kwestii zgodności z przepisami o ochronie danych osobowych **projektu ustawy o zmianie ustawy o ewidencji ludności i dowodach osobistych**.²¹³ W projekcie tym zaproponowane zostało rozwiązanie polegające na przyznaniu podmiotom, o których mowa w art. 44h ust. 1 i ust. 2 pkt 1 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych²¹⁴ możliwości weryfikacji danych przez nie posiadanych (w zakresie informacji znajdujących się w dowodach osobistych wraz z danymi adresowymi) z informacjami znajdującymi się w zbiorze PESEL oraz ogólnokrajowej ewidencji wydanych i unieważnionych dowodów osobistych prowadzonych przez Ministra Spraw Wewnętrznych i Administracji. Powyższy projekt nie wyjaśniał, jak należy rozumieć proponowany system weryfikacji, tzn. czy w przypadku, kiedy podmiot zwracający się o dokonanie weryfikacji do ministra właściwego do spraw wewnętrznych poda nieprawdziwe lub nieaktualne dane osobowe, to raport zwrotny zawierał będzie dane poprawne, czy też jedynie „suchy” komunikat odnośnie zgodności albo niezgodności nadesłanych danych ze zgromadzonymi w rejestrach MSWiA. Wobec tego Generalny Inspektor wyraził sceptyczny stosunek do zaproponowanego rozwiązania. Jednakże z uwagi na okoliczność, iż w toku prac legislacyjnych nad projektem okazało się, iż w procesie weryfikacji MSWiA przekazywać będzie podmiotowi prywatnemu krótki raport wyłącznie o zgodności lub braku zgodności podanych danych ze zgromadzonymi w rejestrach oraz zwracając uwagę na przewidzianą w projektowanych przepisach konieczność spełnienia przez podmioty zainteresowane weryfikacją szeregu warunków, by stała się ona możliwa,²¹⁵ ostatecznie Generalny Inspektor dopuścił wprowadzenie proponowanego rozwiązania.²¹⁶

Z kolei w trakcie opiniowania projektu ustawy o kierujących pojazdami,²¹⁷ Generalny Inspektor negatywnie ustosunkował się do przewidzianego w jego treści rozwiązania polegającego na przyznaniu osobie upoważnionej przez starostę uprawnienia

²⁰⁹ Projektowany art. 264 § 2 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1270, z późn. zm.) w brzmieniu nadanym przez art. 1 nowelizacji.

²¹⁰ W myśl art. 15 § 1 pkt 2 ustawy Prawo o postępowaniu przed sądami administracyjnymi, Naczelny Sąd Administracyjny podejmuje uchwały mające na celu wyjaśnienie przepisów prawnych, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych. Stosownie do treści art. 264 § 2 cyt. ustawy, wymienione wyżej uchwały Naczelny Sąd Administracyjny podejmuje na wniosek Prezesa Naczelnego Sądu Administracyjnego, Prokuratora Generalnego oraz Rzecznika Praw Obywatelskich.

²¹¹ Wyrok z dnia 6 czerwca 2005 r. o sygn. akt I OPS 2/2005.

²¹² Np. ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz. U. Nr 165, poz. 1170 z późn. zm.).

²¹³ DOLiS-033-110/08.

²¹⁴ Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm. Stosownie do treści tych przepisów, dane ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i unieważnionych dowodów osobistych udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, następującym podmiotom: 1) organom administracji publicznej, sądom i prokuraturze; 2) Policji, Straży Granicznej, Służbie Więziennej, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Służbie Celnej, Żandarmerii Wojskowej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Biuru Ochrony Rządu, Centralnemu Biuru Antykorupcyjnemu i strażom gminnym (miejskim); 3) organom kontroli skarbowej i wywiadu skarbowego; 4) państwowym i komunalnym jednostkom organizacyjnym oraz innym podmiotom - w zakresie niezbędnym do realizacji zadań publicznych określonych w odrębnych przepisach; 5) Polskiemu Czerwonemu Krzyżowi - w zakresie danych osób poszukiwanych. Dane, o których mowa w ust. 1 pkt 1 – zgodnie z jego ust. 2 – mogą być udostępnione: osobom i jednostkom organizacyjnym – jeżeli wykażą w tym interes prawny.

²¹⁵ Zgodnie z projektowanym art. 44h ust. 5, podmioty te muszą posiadać urządzenia umożliwiające identyfikację osoby uzyskującej dane w systemie oraz zakresu, daty i celu ich uzyskania, zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania, sprawdzenia, czy uzyskanie danych jest uzasadnione specyfiką lub zakresem wykonywanych zadań lub prowadzonej działalności, a ponadto podmioty te złożą wnioszek i uzyskają stosowne rozstrzygnięcie.

²¹⁶ DOLiS-033-110/08, projekt opublikowano w Dzienniku Ustaw z 2008 r. Nr 195, poz. 1198.

²¹⁷ DOLiS-033-135/08.

do niejawnej obserwacji i rejestracji za pomocą urządzenia technicznego służącego do zapisu obrazu i dźwięku szkolenia osób ubiegających się o wydanie prawa jazdy,²¹⁸ jak również przyznaniu podobnego uprawnienia w odniesieniu do części praktycznej egzaminu państwowego osobie upoważnionej przez marszałka województwa.²¹⁹ Organ do spraw ochrony danych osobowych podkreślił, iż stosowanie technik operacyjnych powinno być domeną odpowiednio przeszkolonych i właściwie nadzorowanych funkcjonariuszy Policji oraz służb specjalnych i brak jest jakiegokolwiek uzasadnienia dla rozszerzania kompetencji do stosowania tych technik na inne podmioty.

Jednocześnie Generalny Inspektor zakwestionował brzmienie art. 80 ust. 2 projektu, według którego osoba posiadająca prawo jazdy lub pozwolenie na kierowanie tramwajem miałaby być zobowiązana do zgłaszania staroście zmian dotyczących jej stanu zdrowia. Projekt przewidywał konieczność składania przez osobę podlegającą badaniu lekarskiemu oświadczenia o stanie jej zdrowia w formie ankiety, pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia. Generalny Inspektor wskazał na oczywistą wadliwość tej regulacji. Podkreślił, że godzi ona w chronione przez art. 47 Konstytucji Rzeczypospolitej Polskiej prawo do prywatności osób posiadających prawa jazdy (pozwolenia na kierowanie tramwajem), jak również prawo tych osób do szczególnej ochrony danych o stanie zdrowia.²²⁰

Istotnym z punktu widzenia prawa do ochrony danych osobowych okazał się również **projekt ustawy o zmianie ustawy o udostępnianiu informacji gospodarczych oraz niektórych innych ustaw**.²²¹ Generalny Inspektor opiniując przedłożony mu projekt wskazał, że zawiera on rozwiązania nie do zaakceptowania zarówno z punktu widzenia chronionego przez art. 47 Konstytucji Rzeczypospolitej Polskiej prawa do prywatności, jak i przepisów ustawy o ochronie danych osobowych. Podkreślił, iż w świetle utrwalonego orzecznictwa Trybunału Konstytucyjnego²²² prawo do ochrony życia prywatnego obejmuje swoim zakresem m.in. ochronę danych dotyczących sytuacji majątkowej obywatela, a więc odnosi się także do dokonywanych przez niego transakcji. W tym stanie rzeczy ingerencja ustawodawcy prowadząca w konsekwencji do ograniczenia zakresu prywatności obywateli, musi – zgodnie z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej²²³ – spełniać konstytucyjne wymogi niezbędności i proporcjonalności. Dokonując interwencji w sferę prawa do ochrony życia prywatnego obywateli ustawodawca winien również uwzględnić fakt, iż osoba fizyczna jest obiektywnie słabszą stroną stosunku prawnego łączącego ją z przedsiębiorcą.

Autor projektu zdawał się ignorować wskazane wyżej uwarunkowania i powołując się na konieczność lepszej ochrony wierzycieli oraz poprawy funkcjonowania systemu wymiany informacji gospodarczych i warunków funkcjonowania biur informacji gospodarczej, podjął próbę rezygnacji z istniejących w ustawie z dnia 14 lutego 2003 r. o udostępnianiu informacji gospodarczych²²⁴ gwarancji ochrony praw dłużników będących osobami fizycznymi. Na zamiar taki wskazywało projektowane brzmienie art. 7 ust. 2 ustawy o udostępnianiu informacji gospodarczych.²²⁵ Przepis ten w punkcie 1 wprowadzał możliwość przekazywania do biur informacji gospodarczej danych (wskazanych w art. 2 ust. 1 pkt 2 ustawy) dłużników będących osobami fizycznymi w związku z jakimikolwiek ich zobowiązaniami o charakterze cywilnoprawnym, w punkcie 2 praktycznie uniezależniał dopuszczalność przekazania danych od wysokości zadłużenia (w przypadku, gdy ogólna kwota zobowiązań dłużnika wynosi co najmniej 200 zł, pozostawanie przez niego w zwłoce co do nawet najmniejszej sumy daje wierzycielowi uprawnienie do przekazania danych), zaś w pkt. 4 *de facto* likwidował obowiązek wierzyciela zawiadomienia dłużnika o zamiarze przekazania jego danych do biura informacji gospodarczej (fakt wysłania zwykłej przesyłki listowej nie podlega odnotowaniu w żadnej ewidencji, a zatem nie może być skontrolowany). Generalny Inspektor podniósł, że zważywszy, iż opiniowany projekt ustawy dopuszcza

²¹⁸ Art. 46 ust. 4 pkt 4 projektu.

²¹⁹ Art. 70 ust. 4 pkt 5 projektu.

²²⁰ Art. 27 ust. 1 ustawy o ochronie danych osobowych.

²²¹ DOLiS-033-121/08.

²²² Np. orzeczenie Trybunału Konstytucyjnego z dnia 24 czerwca 1997 roku, sygn. akt K. 21/96 – uzasadnienie, opubl. OTK ZU z 1997 r. zesz. 2, poz. 23; wyrok Trybunału Konstytucyjnego z dnia 11 kwietnia 2000 roku, sygn. akt K. 15/98 – uzasadnienie, opubl. OTK ZU z 2000 r. zesz. 3, poz. 86.

²²³ Zgodnie z treścią powołanego przepisu, ograniczenia w zakresie korzystania z konstytucyjnych praw i wolności 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.

²²⁴ Dz. U. Nr 50, poz. 424 z późn. zm.

²²⁵ Nadane przez art. 1 pkt 8 przedłożonej Generalnemu Inspektorowi nowelizacji.

przetwarzanie przez biura informacji gospodarczej bez zgody osoby, której dane dotyczą, informacji archiwalnych²²⁶ w celu oceny wiarygodności płatniczej oraz dla stosowania metod statystycznych,²²⁷ zakres przyznanego biur informacji gospodarczej uprawnienia do przetwarzania danych osobowych daleko wykracza poza istniejące dotychczas unormowania odnoszące się do podmiotów prawa prywatnego.

Ponadto Generalny Inspektor podkreślił, że w jego opinii wskazane w uzasadnieniu cele nowelizacji w żadnym razie nie uzasadniają proponowanego stopnia uprzywilejowania biur informacji gospodarczej, a opisane unormowania w sposób bezpośredni i z naruszeniem zasady proporcjonalności godzą w prawo do ochrony życia prywatnego dłużników będących osobami fizycznymi.

W dalszej części swojej opinii Generalny Inspektor odniósł się już wyłącznie do zgodności projektu z przepisami o ochronie danych osobowych. I tak, w pierwszej kolejności zauważył, iż całkowicie burzy on dotychczasową konstrukcję ustawy o udostępnianiu informacji gospodarczych. W dotychczasowym modelu przedsiębiorca, który zawarł z biurem informacji gospodarczej pisemną umowę o udostępnianie informacji gospodarczych, był jedynym dysponentem (administratorem) informacji przekazanych do biura. Konsekwentnie zatem to do niego kierowane były wnioski osoby, której dane dotyczą, o uzupełnienie, uaktualnienie lub sprostowanie danych niekompletnych, nieaktualnych, nieprawdziwych oraz usunięcie danych udostępnionych lub przechowywanych z naruszeniem ustawy.²²⁸ Biuro informacji gospodarczej pełniło jedynie funkcję pośrednika w udostępnianiu informacji gospodarczych, tj. ich przyjmowaniu, przechowywaniu i ujawnianiu na zasadach określonych w ustawie.²²⁹ Przyznanie biur informacji gospodarczej uprawnienia do przetwarzania informacji przekazanych im przez wierzycieli jako tzw. informacji archiwalnych²³⁰ prowadzi do nadania im statusu nieznanego ustawie o ochronie danych osobowych. Biura informacji gospodarczej, które w dalszym ciągu miałyby pozyskiwać dane na podstawie umów zawartych z wierzycielami,²³¹ zyskują bowiem możliwość przetwarzania informacji, których sami wierzyciele nie mogliby przetwarzać. Natomiast z przepisów ustawy o ochronie danych osobowych wynika obowiązek wierzycieli (dysponentów informacji) zapewnienia legalności przetwarzania danych, ich merytorycznej poprawności i adekwatności oraz zakaz przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.²³² Są oni zatem zobowiązani uzupełnić, uaktualnić lub sprostować dane z różnych przyczyn nieprawidłowe oraz usunąć dane zbędne lub zebrane w sposób nielegalny. Regulacje zawarte w nowelizacji ustawy o udostępnianiu informacji gospodarczych²³³ zezwalały zaś biur informacji gospodarczej na dalsze przechowywanie bez zgody osób, których dotyczą, informacji nieaktualnych oraz ich przetwarzanie w celu oceny wiarygodności płatniczej oraz dla stosowania metod statystycznych. Powyższe pozostaje w jaskrawej sprzeczności z – określonymi w ustawie o ochronie danych osobowych – zasadami przetwarzania tych danych oraz czyni zupełnie iluzorycznym zachowane w art. 21 ust. 2 ustawy o udostępnianiu informacji gospodarczych uprawnienie osoby, której dane dotyczą, do żądania uzupełnienia, uaktualnienia lub sprostowania danych niekompletnych, nieaktualnych, nieprawdziwych oraz usunięcia danych udostępnionych lub przechowywanych z naruszeniem ustawy.

Oprócz przedstawionych zastrzeżeń o charakterze generalnym nie mogła zyskać akceptacji organu do spraw ochrony danych osobowych propozycja pominięcia w nowym art. 13 ustawy o udostępnianiu informacji gospodarczych²³⁴ samoistnej przesłanki usunięcia informacji gospodarczych, jaką jest upływ czasu.²³⁵ Biorąc pod uwagę, iż zobowiązania cywilne co do zasady ulegają przedawnieniu,²³⁶ brak jest uzasadnienia dla bezterminowego przechowywania przez biura informacji gospodarczej danych

²²⁶ Definicję tego pojęcia zawierał art. 13a ust. 3.

²²⁷ Art. 13b ust. 1, 3 i 4 w zw. z art. 5a.

²²⁸ Art. 21 ustawy o udostępnianiu informacji gospodarczych.

²²⁹ Art. 4 ust. 5 ustawy o udostępnianiu informacji gospodarczych.

²³⁰ Art. 5a ustawy o udostępnianiu informacji gospodarczych dodany przez art. 1 pkt 3 projektu ustawy.

²³¹ Art. 6 ust. 1 ustawy o udostępnianiu informacji gospodarczych w brzmieniu nadanym przez art. 1 pkt 6 nowelizacji.

²³² Art. 26 ust. 1 ustawy o ochronie danych osobowych.

²³³ Art. 13a ust. 3 i art. 13b ust. 1, 3 i 4 nowelizacji.

²³⁴ W brzmieniu ustalonym przez art. 1 pkt 14 nowelizacji.

²³⁵ 3 lata od ostatniej aktualizacji oraz 10 lat od otrzymania informacji przez biuro – art. 13 ust. 2 pkt 4 ustawy o udostępnianiu informacji gospodarczych.

²³⁶ Art. 117 § 1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.).

dotyczących takich zobowiązań. Powyższe mogłoby jednocześnie prowadzić do naruszenia wynikającej z ustawy o ochronie danych osobowych zasady tzw. ograniczenia czasowego.²³⁷

Generalny Inspektor zasygnalizował również wątpliwość co do kryteriów, jakie zdecydowały o doborze podmiotów, które znalazły się w zawartym w art. 16 ust. 1 ustawy o udostępnianiu informacji gospodarczych, katalogu uprawnionych do otrzymywania informacji gospodarczych.²³⁸ Podał pod rozagę, czy wśród organów uprawnionych nie powinien być również wymieniony Generalny Inspektor Ochrony Danych Osobowych wykonujący zadania określone w ustawie o ochronie danych osobowych.

W omawianym okresie sprawozdawczym Generalny Inspektor wydał również opinię na temat zgodności z przepisami o ochronie danych osobowych **projektu ustawy o zmianie ustawy o Centralnym Biurze Antykorupcyjnym oraz o zmianie niektórych innych ustaw**.²³⁹

I tak, Generalny Inspektor wskazał, iż w świetle dyspozycji art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych²⁴⁰ za nieprawidłowy uznać należy projektowany art. 22 ust. 6a ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym,²⁴¹ dodany przez art. 1 pkt 13 lit. d opiniowanego projektu.²⁴² Organ do spraw ochrony danych osobowych wskazał, iż skoro zadaniem Centralnego Biura Antykorupcyjnego jest – w głównej mierze – rozpoznawanie, zapobieganie i wykrywanie przestępstw,²⁴³ nie sposób wskazać celu dalszego przechowywania zebranych w toku czynności informacji (w tym danych osobowych) po upływie okresu karalności przestępstw, które Centralne Biuro Antykorupcyjne ma ścigać. Proponowana regulacja nie przewiduje jakiegokolwiek ograniczenia dopuszczalnego okresu przechowywania danych przez Centralne Biuro Antykorupcyjne za zgodą Prokuratora Generalnego, co nie tylko pozostaje w sprzeczności z powołanym już wcześniej art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych, lecz łamie także ograniczenia okresu przechowywania danych wprowadzone w art. 22 ust. 6 ustawy o Centralnym Biurze Antykorupcyjnym (w brzmieniu nadanym przez art. 1 pkt 13 lit. c opiniowanego projektu ustawy).²⁴⁴ W uzasadnieniu projektu ustawy nie wskazano tymczasem żadnych argumentów przemawiających za wprowadzeniem do ustawy o Centralnym Biurze Antykorupcyjnym szczególnego unormowania z art. 22 ust. 6a.

Generalny Inspektor poparł jednak²⁴⁵ wprowadzenie do ustawy o Centralnym Biurze Antykorupcyjnym²⁴⁶ normy gwarancyjnej nakazującej informować Prokuratora Generalnego o zniszczeniu materiałów z czynności operacyjno-rozpoznawczych, które nie zawierają informacji potwierdzających popełnienie przestępstwa lub przestępstwa skarbowego.²⁴⁷ Zauważył wszakże, iż podniesione w uzasadnieniu projektu ustawy nowelizującej racje przemawiające za wprowadzeniem takiego rozwiązania, znajdują pełne zastosowanie także w odniesieniu do art. 22 ust. 7 ustawy o Centralnym Biurze Antykorupcyjnym²⁴⁸ oraz art. 23 ust. 13 tejże ustawy²⁴⁹. Konsekwentnie zatem wyżej wskazane przepisy ustawy o Centralnym Biurze Antykorupcyjnym powinny również zostać uzupełnione o regulację nakazującą informowanie Prokuratora Generalnego o zniszczeniu przez Centralne Biuro Antykorupcyjne zebranych materiałów.

²³⁷ Zgodnie z art. 26 ust. 1 pkt 4 tej ustawy, administrator danych powinien zapewnić m.in., aby dane osobowe były przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

²³⁸ W brzmieniu nadanym przez art. 1 pkt 14 nowelizacji.

²³⁹ DOLiS-033-175/08.

²⁴⁰ Przepis ten zakazuje przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

²⁴¹ Dz. U. Nr 104, poz. 708 z późn. zm.

²⁴² Przepis ten stanowił, iż w szczególnie uzasadnionych przypadkach, po uzyskaniu zgody Prokuratora Generalnego, dane o których mowa w ust. 6 (czyli zebrane w celu wykrycia przestępstw) mogą być przechowywane przez okres dłuższy.

²⁴³ Tak stanowi art. 2 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym.

²⁴⁴ Przepis ten przewidywał, iż dane osobowe zebrane w celu wykrycia przestępstwa przechowuje się przez okres, w którym są one niezbędne dla realizacji ustawowych zadań wykonywanych przez CBA jednak nie dłużej niż do czasu przedawnienia jego karalności. Funkcjonariusze CBA dokonują weryfikacji tych danych nie rzadziej niż co 10 lat od dnia uzyskania informacji, usuwając dane zbędne.

²⁴⁵ Pismo GIOO z dnia 17 lipca 2008 r. o sygn. DOLiS-033-175/08.

²⁴⁶ Na podstawie art. 1 pkt 11 opiniowanego projektu ustawy.

²⁴⁷ Art. 14 ust. 8 zdanie trzecie ustawy o Centralnym Biurze Antykorupcyjnym.

²⁴⁸ Przepis ten dotyczy usuwania danych sensytywnych osób podejrzanych o popełnienie przestępstw, które nie zostały skazane za te przestępstwa.

²⁴⁹ Artykuł reguluje niszczenie materiałów zawierających informacje objęte tajemnicą bankową, ubezpieczeniową lub związaną z prowadzeniem rachunku papierów wartościowych niestanowiących dowodu zaistnienia przestępstwa.

Ponadto w okresie objętym sprawozdaniem, Generalny Inspektor opiniując **projekt ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy**²⁵⁰ podniósł, iż nie może zgodzić się na przyjęcie proponowanych w jego treści rozwiązań naruszających prawa osób bezrobotnych wynikające z przepisów o ochronie danych osobowych. W pierwszej kolejności zasadnicze zastrzeżenia budziła dopuszczalność swobodnego przekazywania podmiotom niepublicznym realizującym zadania publiczne (na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia ich realizacji przez podmiot publiczny) danych zgromadzonych w projektowanym centralnym rejestrze bezrobotnych i poszukujących pracy.²⁵¹ W ocenie Generalnego Inspektora przyjęcie zaproponowanego rozwiązania doprowadziłoby do całkowicie niekontrolowanego obrotu danymi bezrobotnych (poszukujących pracy) i przetwarzania tych danych bez zgody osób, których dotyczą, także po utracie przez nie statusu bezrobotnych. Projektowana ustawa nie określała bowiem zasad udostępniania danych przez administratora danych (tj. ministra właściwego do spraw pracy) i nie przewidywała możliwości weryfikowania przez tego administratora zasadności i celowości pozyskania danych, a nawet nie pozwalała na jednoznaczne ustalenie kręgu podmiotów, które do danych w centralnym rejestrze uzyskują dostęp. Co więcej, kwestionowane przepisy uzależniały dostęp do wielu informacji o osobach fizycznych (czyli wkroczenie w sferę prawa do prywatności tych osób) jedynie od spełnienia – niemających charakteru normatywnego – wymogów technicznych i organizacyjnych określonych przez kierownika jednostki organizacyjnej prowadzącej rejestr,²⁵² co budzi uzasadnione wątpliwości w kwestii zgodności takiego rozwiązania z przepisami Konstytucji Rzeczypospolitej Polskiej.

Generalny Inspektor zwrócił ponadto uwagę, iż w świetle dyspozycji art. 38 ustawy o ochronie danych osobowych²⁵³ nie sposób także zgodzić się z zawartą w przepisach projektu propozycją odstąpienia od obowiązku składania wniosków przez podmioty ubiegające się o udostępnienie danych zgromadzonych przez powiatowe urzędy pracy.²⁵⁴ Tymczasem tylko tryb wnioskowy udostępniania danych gwarantuje realne sprawowanie przez administratorów danych kontroli celowości i zasadności ich pozyskiwania i może być uznany za dopuszczalny z punktu widzenia unormowań zawartych w ustawie o ochronie danych osobowych.

Organ do spraw ochrony danych osobowych nie znalazł również uzasadnienia dla przyznania agencjom zatrudnienia uprawnienia do weryfikacji kandydatów do pracy z zastosowaniem narzędzi i metod psychologicznych w sytuacji, gdy obowiązujące przepisy Kodeksu pracy nie przewidują pozyskiwania przez pracodawców danych tego rodzaju. Zwrócił też uwagę na nieprawidłowe użycie w art. 19 ust. 3 ustawy o promocji zatrudnienia i instytucjach rynku pracy²⁵⁵ trybu oznajmującego: „Przetwarzanie danych przez agencję zatrudnienia odbywa się zgodnie z przepisami o ochronie danych osobowych” sugerującego, iż każda czynność na danych osobowych dokonana przez agencję zatrudnienia jest zawsze zgodna z przepisami o ochronie danych osobowych, a co za tym idzie – wyłączona spod kontroli Generalnego Inspektora sprawowanej na podstawie art. 12 ustawy o ochronie danych osobowych.

Kolejną uwagę podniesioną w stosunku do ww. projektu była przewidziana w jego treści możliwość dopuszczalności zastosowania wobec dłużnika alimentacyjnego, który uchylił się od spełnienia obowiązków wymienionych w art. 5 ust. 3 ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów,²⁵⁶ sankcji w postaci zatrzymania prawa jazdy przez starostę.²⁵⁷ Nie sposób bowiem wykazać, że niewykonanie przez dłużnika alimentacyjnego obowiązków przewidzianych w ustawie o pomocy osobom uprawnionym do alimentów rzutuje w jakikolwiek sposób na posiadane przez niego umiejętności w zakresie prowadzenia pojazdów mechanicznych, których formalnym potwierdzeniem jest prawo jazdy. Brak jest bowiem związku między czynem dłużnika alimentacyjnego a przewidzianą w ustawie o pomocy osobom uprawnionym do alimentów sankcją za to zachowanie.²⁵⁸

²⁵⁰ DOLiS-033-186/08.

²⁵¹ Art. 4 ust. 4 – 4b ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2008 r. Nr 69, poz. 415 z późn. zm.) w brzmieniu nadanym przez art. 1 pkt 4 lit. c i d opiniowanego projektu ustawy.

²⁵² Art. 4b ustawy o promocji zatrudnienia i instytucjach rynku pracy dodany przez art. 1 pkt 4 lit. d opiniowanego projektu.

²⁵³ Stosownie do jego treści, administrator danych jest obowiązany zapewnić kontrolę nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

²⁵⁴ Propozycja zawarta w art. 33 ust. 5c ustawy o promocji zatrudnienia i instytucjach rynku pracy (dodany przez art. 1 pkt 13 lit. e opiniowanego projektu ustawy).

²⁵⁵ W brzmieniu nadanym przez art. 1 pkt 10 opiniowanego projektu.

²⁵⁶ W brzmieniu nadanym przez art. 12 pkt 1 opiniowanego projektu ustawy (Dz. U. Nr 192, poz. 1378).

²⁵⁷ Art. 5 ust. 5 ustawy o pomocy osobom uprawnionym do alimentów w brzmieniu nadanym przez art. 12 pkt 3 opiniowanego projektu.

²⁵⁸ Uwagi Generalnego Inspektora zostały uwzględnione częściowo, a projekt opublikowano w Dzienniku Ustaw z 2009 r. Nr 6, poz. 33.

W omawianym okresie Generalny Inspektor analizował m.in. **projekt rozporządzenia Ministra Infrastruktury w sprawie obsługi naziemnej w portach lotniczych**.²⁵⁹ W swojej opinii wskazał, że zastrzeżenia co do jego zgodności z przepisami ustawy o ochronie danych osobowych budzi nałożenie na przedsiębiorców przystępujących do konkursu o udzielenie zezwolenia na wykonywanie usług obsługi naziemnej obowiązku składania zaświadczeń o niekaralności osób zarządzających ich działalnością – § 14 ust. 1 pkt 1 lit. e opiniowanego projektu rozporządzenia. Składanie takich zaświadczeń stanowi przetwarzanie danych o karalności w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych,²⁶⁰ a nałożenie na przedsiębiorców wskazanego wyżej obowiązku w akcie prawnym o randze niższej niż ustawa, nie może być uznane za rozwiązanie prawidłowe.

Ponadto organ do spraw ochrony danych osobowych uznał za błędne rozwiązanie przewidziane w § 4 pkt 3 projektu rozporządzenia dotyczące wymogu załączania do wniosków o udzielenie zezwolenia na wykonywanie usług obsługi naziemnej kopii dokumentów potwierdzających tożsamość przedsiębiorców będących osobami fizycznymi. Istnieje bowiem wysokie prawdopodobieństwo, że w skopiowanych dokumentach znajdują się dane niezwiązane z działalnością gospodarczą tych osób (np. imiona rodziców, nazwisko rodowe matki, data i miejsce urodzenia, wizerunek, rysopis). Przetwarzanie zaś – w tym zbieranie – danych w szerszym zakresie, aniżeli niezbędny dla osiągnięcia celu przetwarzania, stanowi naruszenie art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.²⁶¹ Należałoby zatem rozważyć możliwość zastosowania innej metody, niż załączanie do dokumentacji kopii dokumentów potwierdzających tożsamość.

Opiniując z kolei **projekt ustawy o zmianie ustawy o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz niektórych innych ustaw**,²⁶² Generalny Inspektor wskazał projektodawcy, że nie znajduje uzasadnienia przewidziana w art. 1 pkt 2 projektu zmiana art. 18 ust. 2 ustawy z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych,²⁶³ skutkująca pozbawieniem osób, których dane dotyczą, uprawnień z art. 32 ust. 1 pkt. 1, 2, 4 i 6 oraz art. 33 ust. 1 pkt. 1–3 ustawy o ochronie danych osobowych w stosunku do informacji kryminalnych przetwarzanych przez Szefa Krajowego Centrum Informacji Kryminalnych (Komendanta Głównego Policji). Wiążące Rzeczpospolitą Polską przepisy prawa wspólnotowego nie przewidują całkowitego wyłączenia uprawnień osób, których dane dotyczą, do kontroli tego, na jakiej podstawie i jakie ich dane są przetwarzane przez władze publiczne. Ponadto zachowanie w ustawie o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych praw osób, których dane dotyczą, wynikających z przytoczonych powyżej przepisów ustawy o ochronie danych osobowych, nie wpłynie negatywnie na działalność Krajowego Centrum Informacji Kryminalnych. W dalszym ciągu bowiem Szef Krajowego Centrum Informacji Kryminalnych będzie miał możliwość odmowy spełnienia obowiązku informacyjnego wobec tych osób, w przypadku zaistnienia przesłanek z art. 30 ustawy o ochronie danych osobowych (art. 34 ustawy o ochronie danych osobowych w zw. z art. 18 ust. 2 ustawy o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych w aktualnie obowiązującym brzmieniu).²⁶⁴ W tym stanie rzeczy Generalny Inspektor nie podzielił, przedstawionego w uzasadnieniu do opiniowanego projektu ustawy, stanowiska w kwestii celowości zmiany art. 18 ust. 2 ustawy o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych i zdecydowanie zaoponował przeciwko regulacji zawartej w art. 1 pkt 2 opiniowanego projektu.

W roku sprawozdawczym 2008, do Generalnego Inspektora wpłynął również **projekt ustawy o narodowym spisie powszechnym ludności i mieszkań w 2011 r.** wraz z dwoma rozporządzeniami wykonawczymi – **rozporządzeniem Rady**

²⁵⁹ DOLiS-033-232/08.

²⁶⁰ Stosownie do treści tego przepisu, zabrania się przetwarzania 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, nalogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

²⁶¹ Stosownie do treści tego przepisu, 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.

²⁶² DOLiS-033-190/08. *Projekt ustawy o zmianie ustawy o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz niektórych innych ustaw* opublikowany został z całościowym uwzględnieniem uwag GIODO w Dz.U. z 2009 r. Nr 69, poz. 595.

²⁶³ Dz. U. z 2006 r. Nr 216, poz. 1585 z późn. zm.

²⁶⁴ Z art. 30 ustawy wynika, iż administrator danych odmawia udostępnienia danych osobowych ze zbioru danych podmiotom i osobom innym niż wymienione w art. 29 ust. 1, jeżeli spowodowałoby to:

- 1) ujawnienie wiadomości stanowiących tajemnicę państwową,
- 2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
- 3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,

Ministrów w sprawie szczegółowego wykazu danych dotyczących tematów objętych narodowym spisem powszechnym ludności i mieszkań w 2011 r. oraz rozporządzeniem Rady Ministrów w sprawie szczegółowego wykazu danych zbieranych w narodowym spisie powszechnym ludności i mieszkań w 2011 r. z systemów informacyjnych.²⁶⁵

Dokonując oceny jego zgodności z przepisami o ochronie danych osobowych, Generalny Inspektor zwrócił uwagę na okoliczność, iż zarówno z punktu widzenia tych przepisów, jak i regulacji zawartych w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej,²⁶⁶ nie może zyskać akceptacji przewidziana w opiniowanym projekcie konstrukcja, zgodnie z którą ustawa o narodowym spisie powszechnym ludności i mieszkań w 2011 r. miałaby zawierać jedynie przykładowe wyliczenie danych osobowych, jakie mogą być pozyskiwane na potrzeby Narodowego Spisu Powszechnego Ludności i Mieszkań 2011 [NSP 2011], zaś określenie szczegółowego zakresu przetwarzanych danych pozostawiono by rozporządzeniom wykonawczym.²⁶⁷ Generalny Inspektor przypomniał, iż art. 9 ust. 1 ustawy o statystyce publicznej w sposób kategoryczny wprowadza wymóg regulacji ustawowej dla przeprowadzenia spisu powszechnego, w którym nakłada się na osoby fizyczne obowiązek udzielania informacji, zaś art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych zawiera takie samo wymaganie odnośnie przetwarzania bez zgody osoby, której dane dotyczą, danych sensytywnych. Wobec powyższego wskazał, iż w istniejącym stanie prawnym, zawarty w art. 7 ust. 2 projektu ustawy o narodowym spisie powszechnym ludności i mieszkań w 2011 r. katalog danych osobowych przetwarzanych w ramach NSP 2011 musi mieć charakter zamknięty, zaś (ewentualne) rozporządzenia wykonawcze wydane na podstawie art. 7 ust. 3 i art. 29 opiniowanego projektu ustawy nie mogą uprawniać służb spisowych do przetwarzania danych w szerszym zakresie, aniżeli przewidziany w przepisie rangi ustawowej. Brak respektowania tych zasad w przedstawionym do zaopiniowania projekcie rodzi wątpliwość, co do jego zgodności z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.²⁶⁸

Ponadto w opiniowanym projekcie Generalny Inspektor podtrzymał wyrażony już kilkakrotnie pogląd, zgodnie z którym informacje o istnieniu (nieistnieniu) niepełnosprawności i jej stopniu, jako dane o stanie zdrowia podlegające szczególnej ochronie²⁶⁹ mogą być pozyskiwane na potrzeby NSP 2011 jedynie w oparciu o swobodnie wyrażoną zgodę respondentów. Dodatkowego argumentu za tym stanowiskiem dostarcza rozporządzenie nr 763/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie spisów powszechnych ludności i mieszkań, który to akt prawa europejskiego zobowiązuje Państwa Członkowskie do podejmowania wszelkich środków w celu ochrony danych w trakcie sporządzania spisów,²⁷⁰ jak również nie nakłada obowiązku przekazywania Eurostatowi informacji o niepełnosprawności mieszkańców tych Państw.²⁷¹ W tym stanie rzeczy Generalny Inspektor zakwestionował wszystkie przepisy projektu ustawy nakładające obowiązek przekazywania Prezesowi Głównego Urzędu Statystycznego informacji o niepełnosprawności. Organ do spraw ochrony danych osobowych zasugerował przy tym także stosowną zmianę art. 9 ust. 2 projektu ustawy, by w sposób jednoznaczny wynikało z jego treści, że dane o niepełnosprawności²⁷² mogą być zbierane wyłącznie na zasadzie dobrowolności.

Przechodząc do szczegółowych rozwiązań zawartych w opiniowanym projekcie, Generalny Inspektor zgłosił zastrzeżenia co do adekwatności danych pozyskiwanych przez służby spisowe w ramach NSP 2011. Biorąc pod uwagę wymienione w art. 4 ust. 1 projektu ustawy formy przeprowadzenia spisu,²⁷³ powstała bowiem wątpliwość co do celowości i zasadności pozyskiwania od respondentów adresu do korespondencji.²⁷⁴ Generalny Inspektor wskazał, iż przydatność danej tego rodzaju dla celów statystycznych jawi się jako tym bardziej wątpliwa, jeśli zważyć, że osoba fizyczna może posiadać adres do korespondencji w budynku czy lokalu, w którym nie przebywa i przebywać nie ma zamiaru (np. tzw. adres grzecznościowy u przyjaciela czy przyjaciółki). Generalny Inspektor podniósł, iż informacja o adresie do korespondencji może być nie tylko nieprzydatna

4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

²⁶⁵ DOLIS-033-207/08.

²⁶⁶ Dz. U. Nr 88, poz. 439 z późn. zm.

²⁶⁷ Art. 7 ust. 2 i 3 oraz art. 29 projektu ustawy o narodowym spisie powszechnym ludności i mieszkań w 2011 r.

²⁶⁸ Stosownie do treści tego przepisu, 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.

²⁶⁹ Art. 27 ust. 1 i 2 ustawy o ochronie danych osobowych.

²⁷⁰ Art. 4 ust. 2.

²⁷¹ Załącznik do rozporządzenia nakazuje objąć spisem jedynie zagadnienie bieżącej aktywności ekonomicznej ludności.

²⁷² Art. 7 ust. 2 pkt 20.

²⁷³ Wykorzystanie danych z rejestrów administracyjnych, Internet, wywiad telefoniczny, wywiad bezpośredni w budynku.

²⁷⁴ Art. 7 ust. 2 pkt 12 projektu.

dla celów NSP 2011, lecz wręcz zafałszowywać inne dane spisowe (np. odnośnie liczby osób realnie przebywających w budynku lub lokalu). Generalny Inspektor zwrócił się zatem o ponowne rozważenie przez projektodawcę kwestii zbierania na potrzeby NSP 2011 adresów do korespondencji respondentów i – w razie podzielenia jego zastrzeżeń – odpowiednią zmianę niektórych proponowanych przepisów poprzez likwidację obowiązku pozyskiwania i przekazywania tej danej, zaś w przypadku podtrzymania stanowiska zaprezentowanego w projekcie, jego wszechstronne uzasadnienie.

Jeszcze poważniejsze zastrzeżenia organu do spraw ochrony danych osobowych wzbudziła kwestia nałożenia na Ministra Finansów w art. 13 projektu ustawy, obowiązku przekazania Prezesowi Głównego Urzędu Statystycznego informacji o kosztach uzyskania przychodów i źródłach przychodów osób fizycznych prowadzących i nieprowadzących samodzielnie działalności gospodarczej.

W uzasadnieniu projektu ustawy brak było bowiem jakiegokolwiek wyjaśnienia przydatności tych danych dla celów spisowych. Uwzględniając, iż pozyskiwanie danych zbędnych dla osiągnięcia założonego celu narusza w sposób bezpośredni zasadę adekwatności danych, Generalny Inspektor stanowczo zaoponował przeciw tej regulacji i wniósł o jej wykreślenie.

Wobec wyrażenia przez Generalnego Inspektora negatywnego stanowiska wobec przyjętej w projekcie ustawy o narodowym spisie powszechnym ludności i mieszkań w 2011 r. – konstrukcji przekazania do uregulowania w rozporządzeniach szczegółowego zakresu danych przetwarzanych na potrzeby NSP 2011, organ ten podkreślił niecelowość wyrażania na tym etapie prac, opinii wobec **projektów rozporządzenia Rady Ministrów w sprawie szczegółowego wykazu danych dotyczących tematów objętych narodowym spisem powszechnym ludności i mieszkań w 2011 r. i rozporządzenia Rady Ministrów w sprawie szczegółowego wykazu danych zbieranych w narodowym spisie powszechnym ludności i mieszkań w 2011 r. z systemów informacyjnych**. Tytułem sygnalizacji Generalny Inspektor Ochrony Danych Osobowych wskazał, iż pierwszy z wymienionych wyżej projektów przewiduje pozyskiwanie informacji o związkach partnerskich respondentów²⁷⁵ (wbrew jednoznacznie negatywnemu stanowisku wyrażonemu przez organ do spraw ochrony danych osobowych)²⁷⁶, drugi zaś – pozyskiwanie na zasadzie obowiązku z rejestrów prowadzonych przez organy administracji publicznej, danych o niepełnosprawności respondentów bez ich zgody, przeciwko czemu Generalny Inspektor oponował zarówno w przeszłości,²⁷⁷ jak również przy okazji opiniowania wyżej wskazanych aktów prawnych.

Kolejnym aktem prawnym, do którego organ do spraw ochrony danych osobowych wniósł uwagi w okresie sprawozdawczym, był **projekt ustawy o zmianie ustawy o przeciwdziałaniu przemocy w rodzinie oraz niektórych innych ustaw**.²⁷⁸ Zastrzeżenia Generalnego Inspektora wzbudziła propozycja brzmienia art. 9b ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie.²⁷⁹ W myśl powołanego przepisu, członkowie zespołów interdyscyplinarnych mieliby otrzymać uprawnienie do przetwarzania danych osobowych sensytywnych²⁸⁰ ofiar i sprawców przemocy w rodzinie, bez zgody osób, których dane te dotyczą. Nie kwestionując potrzeby przetwarzania przez członków tych zespołów niektórych kategorii danych wymienionych w art. 27 ust. 1 ustawy o ochronie danych osobowych dla realizacji zadań wskazanych w art. 9a ust. 4 ustawy o przeciwdziałaniu przemocy w rodzinie, Generalny Inspektor nie znalazł uzasadnienia dla przyznania organom mającym zapobiegać i przeciwdziałać przemocy w rodzinie tak szerokich kompetencji do przetwarzania danych szczególnie ingerujących w sferę prywatności. W ocenie organu do spraw ochrony danych osobowych, biorąc pod uwagę ustawowe zadania zespołów interdyscyplinarnych, przetwarzanie przez ich członków takich danych ofiar i sprawców przemocy w rodzinie, jak: poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna lub związkowa, kod genetyczny nie powinno być dopuszczalne. Dlatego Generalny Inspektor zwrócił się do projektodawców o stosowne zawężenie dyspozycji art. 9b ustawy o przeciwdziałaniu przemocy w rodzinie i wyjaśnienie w uzasadnieniu ustawy nowelizującej, przetwarzanie których kategorii danych sensytywnych jest rzeczywiście niezbędne dla realizacji ustawowych zadań zespołów interdyscyplinarnych.

²⁷⁵ Ust. 1 pkt 13 załącznika do rozporządzenia.

²⁷⁶ Pismo GIODO z dnia 4 lutego 2008 r. o sygn. DOLiS-033-31/08/2682.

²⁷⁷ Np. GI-DOLiS-023/227/07/206, DOLiS-033-31/08/2682.

²⁷⁸ DOLiS-033-279/08.

²⁷⁹ Dz. U. Nr 180, poz. 1493. Propozycję zawierał art. 1 pkt 8 tego projektu.

²⁸⁰ Art. 27 ust. 1 ustawy o ochronie danych osobowych.

W toku wykonywania w 2008 r. swych ustawowych zadań, Generalny Inspektor wyraził również stanowisko wobec **ustawy zmieniającej ustawę o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej**.²⁸¹ Analizując przepisy tego aktu prawnego Generalny Inspektor stwierdził, że wdrożenie Systemu Informacyjnego Schengen drugiej generacji (SIS II) skutkować ma – jak wynika z ich treści – utratą mocy obowiązującej Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 roku między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach [Konwencja Wykonawcza]. Tymczasem art. 34 ust. 2 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej,²⁸² nakazuje stosowanie zakresu i trybu określonego w art. 29 ust. 2 i 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, które to przepisy w swojej treści odsyłają do art. 92 ust. 2 Konwencji Wykonawczej. Biorąc pod uwagę, iż art. 1 pkt 11 ustawy zmieniającej ustawę o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej wejdzie w życie z dniem wskazanym przez Radę Unii Europejskiej jako dzień wdrożenia SIS II²⁸³ (będącym jednocześnie dniem utraty mocy obowiązującej Konwencji Wykonawczej), zaproponowane w opiniowanym projekcie brzmienie art. 34 ust. 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej będzie nieprawidłowe. Przepis ten nakazywałby bowiem stosowanie zakresu i trybu określonego w art. 29 ust. 2 i 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, które to przepisy odsyłać wówczas będą do nieobowiązującego aktu prawnego – Konwencji Wykonawczej. Zachodzi zatem konieczność stosownej zmiany art. 29 ust. 2 i 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej polegającej na zamianie zawartego w tych przepisach odesłania do art. 92 ust. 2 Konwencji Wykonawczej na odesłanie do odpowiednich unormowań rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II).

Z kolei w **projekcie ustawy o zmianie ustawy o cudzoziemcach oraz niektórych innych ustaw**²⁸⁴ zastrzeżenia organu do spraw ochrony danych osobowych wzbudziła w pierwszej kolejności propozycja nowego brzmienia art. 11a ust. 2 ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach. Powołany przepis ustawy o cudzoziemcach²⁸⁵ przewidywał możliwość doręczania pism w miejscu pracy adresata osobie upoważnionej przez pracodawcę do odbioru korespondencji. Tymczasem zarówno Sąd Najwyższy, jak i Naczelny Sąd Administracyjny wypowiedziały się w kwestii skuteczności doręczania osobie fizycznej przesyłek w miejscu jej pracy.²⁸⁶ W związku z utrwalonym stanowiskiem judykatury, zawartą w projekcie propozycję brzmienia art. 11a ust. 2 ustawy o cudzoziemcach trudno było uznać za zgodną z literą prawa.

Negatywnie organ do spraw ochrony danych osobowych ustosunkował się również do możliwości dokonywania przez funkcjonariuszy „sprawdzenia lokalu” (art. 11c ust. 2 ustawy o cudzoziemcach).²⁸⁷ W świetle dotychczas obowiązujących przepisów ustawy o cudzoziemcach, na cudzoziemcu ciąży obowiązek przedstawiania tytułu prawnego do zajmowanego lokalu mieszkalnego, w którym przebywa lub zamierza przebywać, np. przy składaniu wniosku o zezwolenie na osiedlenie się, zezwolenie na pobyt rezydenta długoterminowego,²⁸⁸ czy zezwolenie na zamieszkanie na czas oznaczony.²⁸⁹ W tym stanie

²⁸¹ DOLiS-033-287/08.

²⁸² Dz. U. Nr 165, poz. 1170. Dodany przez art. 1 pkt 11 projektu ustawy zmieniającej ustawę o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej.

²⁸³ Art. 55 ust. 2 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II).

²⁸⁴ DOLiS-033-225/08.

²⁸⁵ W brzmieniu nadanym przez art. 1 pkt 3 opiniowanej ustawy.

²⁸⁶ Z treści postanowienia Sądu Najwyższego – Izby Administracyjnej, Pracy i Ubezpieczeń Społecznych z dnia 14 listopada 2002 r. znak: III RN 115/2002, wynika, iż doręczenie pisma osobie fizycznej w jej miejscu pracy może być dokonane wyłącznie adresatowi. Z kolei w postanowieniu Naczelnego Sądu Administracyjnego z dnia 29 sierpnia 2005 roku, znak: II FZ 515/2005, czytamy „[...] W przypadku, gdy osoba fizyczna wskazała miejsce pracy jako adres do doręczeń, doręczenie w tym miejscu dokonywane w trybie art. 69 ustawy z dnia 30 sierpnia 2002 roku – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2002 r. Nr 153, poz. 1270 z późn. zm.) jest skuteczne tylko wówczas, gdy pismo odbierze ta osoba fizyczna, nie zaś inna osoba uprawniona do odbioru pism w tym miejscu (zakładzie pracy) [...]”.

²⁸⁷ Wprowadzonej przez art. 1 pkt 4 opiniowanego projektu.

²⁸⁸ Art. 71 ust. 5 pkt 3.

²⁸⁹ Art. 60 ust. 5a pkt 1.

prawnym Generalny Inspektor zakwestionował dokonywanie przez funkcjonariuszy dodatkowego „sprawdzenia”, o którym mowa jest w projektowanych przepisach. Wprawdzie projektodawca uzależnił dokonanie „sprawdzenia” od zgody cudzoziemca²⁹⁰ to powstaje jednakże zasadnicza wątpliwość w zakresie możliwości niewyrażenia zgody lub skutków odmowy. W sytuacji, w jakiej znajduje się cudzoziemiec, trudno mówić o swobodzie podjęcia decyzji w zakresie wyrażenia zgody.

Odnosząc się do kwestii prowadzenia przez Komendanta placówki Straży Granicznej ewidencji, w której odnotowuje się wydanie, przedłużenie oraz unieważnienie przepustki wydawanej cudzoziemcowi będącemu członkiem załogi morskiej przyprawiającej do polskiego portu morskiego, w celu zejścia na ląd i pobytu w granicach miasta portowego, Generalny Inspektor zwrócił uwagę na dwa problemy.²⁹¹ W pierwszej kolejności brak jest przepisu materialnego, który bezpośrednio przyznawałby komendantowi uprawnienie do prowadzenia takiej ewidencji.²⁹² Po wtóre zaś, należałoby określić zakres danych przetwarzanych w ewidencji przepustek celem uniknięcia sytuacji przetwarzania w niej danych „nadmiernych”.²⁹³

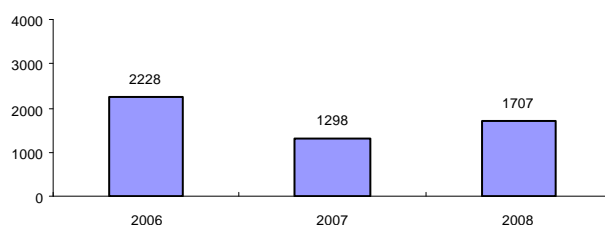
Podsumowując uchybienia popełniane przez projektodawców w procesie tworzenia prawa należy zaznaczyć, iż mają one charakter różnorodny. Niektóre z nich w małym stopniu naruszają przepisy ustawy o ochronie danych osobowych, inne zaś burzą wręcz porządek konstytucyjny, a nawet obowiązujące przepisy Unii Europejskiej. Powyższe umacnia i potwierdza jednocześnie funkcję Generalnego Inspektora, jaką organ ten spełnia w procesie tworzenia prawa.

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

Wraz z rozwojem nowych technologii, problem ochrony danych osobowych i prawa do prywatności zyskuje coraz większe znaczenie. Osoby, których dane dotyczą, z jednej strony coraz bardziej zainteresowane są korzystaniem z różnego rodzaju osiągnięć technologicznych, z drugiej zaś – świadome swoich praw wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych liczą na zachowanie anonimowości.

W społeczeństwie informacyjnym coraz trudniej wyważyć często sprzeczne interesy podmiotów przetwarzających dane osobowe oraz tych, których dane są przetwarzane. Zadanie to nie należy do łatwych - często ani jedna, ani druga z wymienionych wyżej kategorii podmiotów nie jest w stanie samodzielnie rozstrzygnąć nurtujących je wątpliwości. Dlatego zwracają się z pytaniami do Generalnego Inspektora Ochrony Danych Osobowych, do zadań którego – zgodnie z art. 12 pkt 5 ustawy o ochronie danych osobowych – należy 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 2008 do GIODO wpłynęło **1707 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 2006–2008 przedstawia Wykres 25.



Wykres 25.
Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GIODO w latach 2006–2008.

²⁹⁰ Art. 11c ust. 5 ustawy o cudzoziemcach dodany przez art. 1 pkt 4 projektu ustawy nowelizującej.

²⁹¹ Art. 13a ust. 11 ustawy o cudzoziemcach dodany przez art. 1 pkt 4 opiniowanego projektu.

²⁹² Z brzmienia art. 13a ust. 11 projektu można wysnuć wniosek, że ewidencja taka będzie prowadzona, jednakże nie wynika to wprost z żadnego przepisu.

²⁹³ Uwagi GIODO nie zostały uwzględnione, a projekt opublikowano w Dzienniku Ustaw z 2008 r. Nr 216, poz. 1367.

W porównaniu z ubiegłym rokiem, w okresie objętym sprawozdaniem zwiększyła się liczba pytań wpływających do organu do spraw ochrony danych osobowych. 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 przedstawione w dalszej części Sprawozdania zatytułowanej „Działalność informacyjna”.

Biorąc pod uwagę przedmiot kierowanych do Generalnego Inspektora pytań, należy zauważyć, że utrzymującą się od lat tendencją była 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.

Zagadnienia poruszane przez pytających oraz rozstrzygane przez organ do spraw ochrony danych osobowych w roku 2008 – podobnie jak w dotychczasowej działalności Generalnego Inspektora – dotyczyły sfery działalności tak podmiotów prywatnych, jak i publicznych i kierowane były zarówno przez podmioty przetwarzające dane osobowe, jak i osoby, których dane dotyczą.

6.1 Interpretacja przepisów

Przetwarzanie danych osobowych stanowi integralną część funkcjonowania niemalże wszystkich podmiotów ze sfery publicznej. Problemy, jakie wynikają ze stosowania przepisów o ochronie danych osobowych przez te podmioty pojawiają się rokrocznie i wiążą się z podejmowaniem przez Generalnego Inspektora Ochrony Danych Osobowych takich form aktywności, jak wystąpienia do jednostek przetwarzających dane. Wystąpienia te sygnalizują konieczność zmiany stosowanej przez podmioty sektora publicznego praktyki, celem dostosowania procesu przetwarzania danych do wymogów wynikających z przepisów regulujących kwestie ich ochrony.

Z uwagi na to, że tematyka ochrony danych osobowych zajmuje istotne miejsce wśród ogółu spraw sygnalizowanych również na łamach prasy, niejednokrotnie impulsem do wystąpień organu do spraw ochrony danych osobowych były informacje pochodzące właśnie z tego źródła. Tego rodzaju sygnalizacje problemów kierowane były m.in. do **podmiotów z sektora publicznego**. Część spraw wskazywała na problem przetwarzania danych osobowych w zakresie nieadekwatnym do celu przetwarzania zarówno w sytuacji, gdy nie było to przewidziane w przepisach szczególnych, jak również wykraczania poza zakres przewidziany przepisami prawa.

Ze stosowaniem przepisów o ochronie danych osobowych w kontekście zakresu ich ujawniania problemy miał jeden z wójtów. Urząd, w którym sprawował on swoją funkcję, publikował na stronach Biuletynu Informacji Publicznej i zamieszczał na tablicach ogłoszeń w siedzibie urzędu gminy szerszy, niż wynikający z przepisów prawa, zakres danych osobowych osób, które wygrały przetarg na zakup nieruchomości stanowiących własność gminy. Dane tych osób obejmowały imię (imiona), nazwisko oraz adres zamieszkania, podczas gdy regulujące powyższą kwestię przepisy prawa²⁹⁴ wskazywały wyraźnie, iż w takiej sytuacji publikacji podlegają wyłącznie informacje identyfikujące zwycięzcę przetargu obejmujące imię, nazwisko albo nazwę lub firmę osoby ustalonej jako nabywca.²⁹⁵ W skierowanym do wójta gminy wystąpieniu²⁹⁶ organ do spraw ochrony danych osobowych podkreślił, iż brak uwzględnienia powyższych przepisów w działalności urzędu skutkuje naruszeniem art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, z którego wynika, iż w sytuacji obowiązywania przepisów prawa regulujących przetwarzanie

²⁹⁴ Rozporządzenie Rady Ministrów z dnia 14 września 2004 r. w sprawie sposobu i trybu przeprowadzania przetargów oraz rokowań na zbycie nieruchomości (Dz. U. Nr 207, poz. 2108) oraz ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (Dz. U. z 2000 r. Nr 46, poz. 543 z późn. zm.).

²⁹⁵ Zgodnie z § 12 rozporządzenia, o którym mowa, wydanego na podstawie art. 42 ustawy o gospodarce nieruchomościami, w przypadku niezaskarżenia w wyznaczonym terminie czynności związanych z przeprowadzeniem przetargu albo w razie uznania skargi za niezasadną, właściwy organ podaje do publicznej wiadomości, wywieszając w siedzibie właściwego urzędu na okres 7 dni, informację o wyniku przetargu, która powinna zawierać: datę i miejsce oraz rodzaj przeprowadzonego przetargu; oznaczenie nieruchomości będącej przedmiotem przetargu według katastru nieruchomości i księgi wieczystej; liczbę osób dopuszczonych oraz osób niedopuszczonych do uczestniczenia w przetargu; cenę wywoławczą nieruchomości oraz najwyższą cenę osiągniętą w przetargu albo informację o złożonych ofertach lub o niewybraniu żadnej z ofert; imię, nazwisko albo nazwę lub firmę osoby ustalonej jako nabywca nieruchomości.

²⁹⁶ Wystąpienie GIODO z dnia 28 marca 2008 r. o sygn. DOLiS-035-331/08.

danych przez dany podmiot, jego działanie będzie zgodne z przepisami ustawy o ochronie danych osobowych, o ile odbywa się – m.in. – w granicach określonych w tych przepisach.

W odpowiedzi na powyższe wójt gminy wskazał, iż powstałe nieprawidłowości miały charakter incydentalny i zapewnił, iż w przyszłości gmina przestrzegać będzie zasad wynikających z ustawy o ochronie danych osobowych.²⁹⁷

Nieprawidłowości w procesie przetwarzania danych osobowych w poszczególnych jednostkach samorządu terytorialnego w okresie objętym sprawozdaniem występowały dość często i nie dotyczyły tylko zakresu danych osobowych, ale także kwestii realizacji obowiązku informacyjnego, czego dowodem jest kolejna interwencja podjęta w tym czasie przez Generalnego Inspektora Ochrony Danych Osobowych.

W związku z uzyskaniem informacji, iż w procesie rejestrowania dzieci do przedszkoli samorządowych prowadzonych przez jedną z gmin za pomocą strony internetowej nie realizowano obowiązku informacyjnego nałożonego na administratora danych w art. 24 ust. 1 ustawy o ochronie danych osobowych,²⁹⁸ Generalny Inspektor w wystąpieniu skierowanym do podmiotu za to odpowiedzialnego (prezydenta miasta) zwrócił uwagę na konieczność podejmowania w przyszłości działań mających na celu zapewnienie zgodności przetwarzania danych osobowych z przepisami dotyczącymi ich ochrony, w sytuacji prowadzenia postępowań rekrutacyjnych z użyciem formularza wypełnianego drogą elektroniczną.²⁹⁹ Organ do spraw ochrony danych osobowych poinformował również prezydenta miasta o pozostałych obowiązkach spoczywających na każdym administratorze danych.³⁰⁰

Kontynuując analizę problemów w stosowaniu przepisów o ochronie danych osobowych przez niektóre organy jednostek samorządu terytorialnego, należy zwrócić uwagę na budzącą wątpliwości kwestię dotyczącą obowiązku przedkładania komisji powoływanej przez dyrektora szkoły dokumentacji przebytego leczenia (historii choroby), w sytuacji starania się przez nauczyciela czynnego zawodowo lub pozostającego na emeryturze o przyznanie mu pomocy zdrowotnej z funduszu tworzonego corocznie na ten cel w budżecie organu prowadzącego szkołę. Regulacje takie wprowadzała uchwała jednej z rad miejskich, a na jej treść powoływali się dyrektorzy szkół mający obowiązek bezpośredniego przyznania świadczenia.

W wystąpieniu skierowanym do przewodniczącego rady miejskiej³⁰¹ Generalny Inspektor zasygnalizował nie tylko konieczność zmiany takiej uchwały, ale przede wszystkim zwrócił uwagę na okoliczność, iż każdorazowo zakres żądanych danych powinien spełniać wymogi art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. W pełni uzasadnione jest żądanie przedstawienia zaświadczenia lekarskiego stwierdzającego stan zdrowia osoby wnioskującej o przyznanie jej finansowej pomocy zdrowotnej, gdyż komisja przyznająca owe świadczenia uzależnione od stanu zdrowia wnioskodawcy, powinna mieć podstawę dla przyznania tej pomocy. Jednak żądanie przedstawienia dokumentacji medycznej (historii choroby) jest nieadekwatne do celu, któremu ma służyć. Otrzymywanie przez komisję tak szczegółowych informacji na temat stanu zdrowia osoby wnioskującej o przyznanie świadczenia i poddawanie ich analizie przez osoby nieposiadające odpowiedniego przygotowania medycznego było sprzeczne z zasadą adekwatności danych do celu ich przetwarzania. Generalny Inspektor zasygnalizował jednocześnie

²⁹⁷ Pismo wójta gminy z dnia 23 maja 2008 r.

²⁹⁸ Zgodnie z tym przepisem, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku; celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych; prawie dostępu do treści swoich danych oraz ich poprawiania; dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

²⁹⁹ Wystąpienie GIODO z dnia 18 kwietnia 2008 r. o sygn. DOLiS-035-468/08.

³⁰⁰ Wśród tych obowiązków znajdują się: obowiązek legitymowania się jedną spośród wskazanych w art. 23 ust. 1 pkt. 1 – 5 oraz art. 27 ust. 2 pkt. 1–10 wyżej powołanej ustawy przesłanek legalizujących przetwarzanie danych; wskazany w jej art. 26 ust. 1 obowiązek zapewnienia, aby dane były przetwarzane zgodnie z prawem; zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 tego przepisu; merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane; przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania; obowiązek respektowania praw osób, których dane dotyczą, określonych w rozdziale 4 ustawy; obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, o których mowa w rozdziale 5 ustawy o ochronie danych osobowych, zaś w przypadku przetwarzania danych w systemie informatycznym – w przepisach 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 (Dz. U. Nr 100, poz. 1024); wynikający z art. 40 ustawy obowiązek zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 pkt. 1–11 powołanego aktu prawnego.

³⁰¹ Pismo GIODO z dnia 28 maja 2008 r. o sygn. DOLiS-035-570/08.

konieczność dostosowania tworzonego w przyszłości prawa miejscowego do wymogów regulacji prawnych dotyczących ochrony danych osobowych.

Kolejna sprawa dotyczyła stosowania w jednym z urzędów miejskich praktyki polegającej na potwierdzaniu przez telefon przez pracowników urzędu, danych osobowych gapowicza, na prośbę osoby dokonującej kontroli dokumentów przewozu.³⁰²

Interweniując w tej sprawie Generalny Inspektor wskazał, iż o zgodnym z prawem przetwarzaniu danych osobowych mówić można jedynie w sytuacji, gdy ich administrator dopełnia wszystkich, określonych przepisami o ochronie danych osobowych, obowiązków, m.in. obowiązku zabezpieczenia danych osobowych.³⁰³ Niewywiązywanie się z niego skutkuje naruszeniem zasady „dłożenia należytej staranności”, wskazanej w art. 26 ust. 1³⁰⁴ ustawy, a ponadto prowadzić może do powstania odpowiedzialności karnej na podstawie jej art. 51 i 52³⁰⁵. Wskazał jednocześnie, iż ustalanie tożsamości podróżnego w takich przypadkach powinno odbywać w trybie art. 33a ust. 4 pkt 2 ustawy z dnia 15 listopada 1984 r. Prawo przewozowe.³⁰⁶ Prezydent miasta uznał zastrzeżenia organu do spraw ochrony danych osobowych i zrezygnował ze stosowania kwestionowanej praktyki.³⁰⁷

W okresie objętym sprawozdaniem Generalny Inspektor stwierdził również nieprawidłowości w sposobie wykonywania przez Policję niektórych jej zadań. Uzyskał on bowiem informacje, iż na stronie internetowej Komendy Głównej Policji (www.policja.pl), dostępne były wizerunki roznegliżowanych mężczyzn. Zdjęcia zostały nie tylko udostępnione w sposób tradycyjny, ale zapewniono jednocześnie możliwość ich pobrania. W wystąpieniu do Komendanta Głównego Policji organ powołany do spraw ochrony danych osobowych zwrócił uwagę na niecelowość i brak podstawy prawnej do stosowania takich praktyk.³⁰⁸ Generalny Inspektor podniósł, iż rozpowszechnianie wizerunku osób w podobnych sytuacjach jest działaniem nagannym, naruszającym sferę prywatności osób, których wizerunek dotyczy oraz pozbawionym racjonalnego celu. Przywołał przy tym Konwencję o Ochronie Praw Człowieka i Podstawowych Wolności (art. 8 nakazujący poszanowanie życia prywatnego i rodzinnego³⁰⁹), Konstytucję Rzeczypospolitej Polskiej (art. 7 formułujący zasadę legalizmu działania organów władzy publicznej³¹⁰) i zwrócił uwagę na treść jednego z wyroków Sądu Apelacyjnego.³¹¹ W odpowiedzi Komendant Główny Policji zapewnił, że podjęcie działania mające na celu podniesienie świadomości rzeczników prasowych Policji w zakresie ochrony prywatności osób, których dotyczą przekazywane mediom informacje – w ramach materiałów pochodzących z monitoringu miejskiego.³¹²

Niemniej jednak w dniu 22 grudnia 2008 r. fotografie pochodzące z monitoringu miejskiego nadal pozostawały na stronie www.policja.pl, dlatego Generalny Inspektor zwrócił się do Komendanta Głównego Policji o podanie przyczyn zaistniałego stanu

³⁰² Wystąpienie GIODO z dnia 25 lipca 2008 r. o sygn. DOLiS-035-919/08.

³⁰³ Przepis ten stanowi, iż administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

³⁰⁴ Z przepisu tego wynika, iż administrator danych powinien dolożyć należytej staranności w celu ochrony interesów osób, których dane dotyczą.

³⁰⁵ W myśl pierwszego ze wskazanych przepisów, 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). Zgodnie natomiast z art. 52 ustawy, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

³⁰⁶ Zgodnie z tym przepisem, przewoźnik lub osoba przez niego upoważniona ma prawo - w razie odmowy zapłacenia należności i niemożności ustalenia tożsamości podróżnego - zwrócić się do funkcjonariusza Policji i innych organów porządkowych, które mają, zgodnie z przepisami prawa, uprawnienia do ustalania tożsamości osób, o podjęcie czynności zmierzających do ustalenia tożsamości podróżnego, Dz. U. z 2000 r. Nr 50, poz. 601 z późn. zm.

³⁰⁷ Pismo prezydenta miasta z dnia 11 grudnia 2008 r. o sygn. OrN.II.0561-36/08.

³⁰⁸ Wystąpienie GIODO z dnia 11 czerwca 2008 r. o sygn. DOLiS-035-748/08.

³⁰⁹ Zgodnie z tym przepisem, każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Ust. 2 tego przepisu stanowi z kolei, iż niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarcy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

³¹⁰ Zgodnie z tym przepisem, organy władzy publicznej działają w granicach i na podstawie prawa.

³¹¹ Wyrok z 2005 r. (sygn. akt VI ACa 455/2005), w którym Sąd ten zwrócił uwagę na okoliczność, iż zgodnie z art. 47 Konstytucji RP każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W dalszej części wyroku czytamy: „(...) także przepisy o ochronie dóbr osobistych (art. 23 i 24 K.c.) obejmują dobra ze sfery życia prywatnego, rodzinnego czy intymności. Natomiast zgodnie z art. 14 ust. 6 prawa prasowego „nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba, że wiąże się to bezpośrednio z działalnością publiczną danej osoby (...)”.

³¹² Pismo Komendanta Głównego Policji z dnia 14 sierpnia 2008 r. o sygn. Grp-409/08/AH.

rzeczy.³¹³ W odpowiedzi na powyższe Komendant Główny Policji poinformował GİODO o podjęciu przez Policję czynności zmierzających do definitywnego usunięcia kwestionowanego materiału ze strony internetowej KGP.³¹⁴

Generalny Inspektor interweniował także w sprawie wymiany danych o DNA pomiędzy polską Policją a Interpolem, za pomocą międzynarodowego portalu DNA. W wystąpieniu skierowanym do Komendanta Głównego Policji organ do spraw ochrony danych osobowych zwrócił uwagę na okoliczność, iż wszelkie działania ograniczające prawo ochrony życia prywatnego lub ochrony danych osobowych zaliczanych do konstytucyjnych wolności i praw osobistych człowieka i obywatela,³¹⁵ powinny znajdować ustawową podstawę.³¹⁶ W odpowiedzi Komendant Główny Policji powołał się na podpisany w dniu 14 lipca 2008 r. dokument „Interpol Charter – International DNA Gateway”, którego postanowienia pozwoliły na uzyskanie przez Policję dostępu do bazy danych DNA prowadzonej przez Sekretariat Generalny w Lyonie.³¹⁷ W związku z powyższym, wobec uzasadnionych wątpliwości co do tego, czy dokument ten w istocie uprawnia powołane podmioty do wymiany informacji o DNA, organ ds. ochrony danych osobowych zasygnalizował Ministrowi Spraw Wewnętrznych i Administracji³¹⁸ oraz Komendantowi Głównemu Policji³¹⁹ konieczność podjęcia działań zmierzających do wprowadzenia do porządku prawnego przepisów stanowiących podstawę prawną do wymiany przez polską Policję danych o DNA z innymi państwami członkowskimi za pomocą międzynarodowego portalu DNA, deklarując jednocześnie chęć współpracy w tym zakresie. Generalny Inspektor aktualnie oczekuje na informacje w niniejszej sprawie.

Innym, odnotowanym w roku 2008 problemem związanym z przetwarzaniem danych osobowych przez Policję było stosowanie przez tę formację urządzenia o nazwie „morforapid”, służącego do szybkiej identyfikacji odcisków palców.³²⁰ Okazało się, że Policja nie utożsamia procesu pozyskiwania i przesyłania informacji w oparciu o powyższy system urządzeń z przetwarzaniem danych osobowych wskazując, iż do systemu w tym przypadku wpisuje się zapytanie zawierające informacje dotyczące pięci osób oraz układu minucji zakodowanego wektorowo w postaci ciągu cyfr, który jest zrozumiały tylko przez jedną aplikację – i nie można go powtórnie odszyfrować – a „odpowiedź z systemu do urządzenia w przypadku pozytywnego wyniku przeszukania zawiera jedynie określony numer ID i płeć osoby.”³²¹ Konieczne było zatem wskazanie Komendantowi Głównemu Policji,³²² iż proces przetwarzania informacji podlega w tym przypadku wymogom ustawy o ochronie danych osobowych, gdyż informacje te mogą stanowić dane osobowe.³²³

Impulsem do kolejnego wystąpienia Generalnego Inspektora stały się wątpliwości zgłaszane przez przedsiębiorców telekomunikacyjnych.³²⁴ Dotyczyły one kwestii sposobu pozyskiwania danych abonentów (konstrukcji klauzuli zgody) na potrzeby opracowania Ogólnokrajowego Spisu Abonentów. Generalny Inspektor wystąpił w tej sprawie do Prezesa Urzędu Komunikacji Elektronicznej informując, jakie warunki powinna spełniać prawidłowo skonstruowana klauzula zgody.³²⁵ Podniósł, iż nie znajduje uzasadnienia stanowisko wyrażone w jednej z decyzji wydanej przez Prezesa Urzędu Komunikacji Elektronicznej,³²⁶ dopuszczające w stosunku do abonentów będących osobami fizycznymi, którzy umowę z dostawcą usług zawarli przed wejściem w życie ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne,³²⁷ przyjęcie konstrukcji zgody domniemanej na zamieszczenie ich danych w publicznie dostępnym spisie abonentów, a także udostępnianie tych danych za pośrednictwem służb informacyjnych przedsiębiorcy telekomunikacyjnego (usługa biura numerów). Generalny Inspektor zauważył, że ustawa z dnia 21 lipca 2000 r.

³¹³ Wystąpienie GİODO z dnia 23 grudnia 2008 r. o sygn. DOLiS-035-748/08.

³¹⁴ Pismo Komendanta Głównego Policji z dnia 4 lutego 2009 r. o sygn. akt Is-1320/41/09/TM.

³¹⁵ Art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej.

³¹⁶ Wystąpienie GİODO z dnia 16 września 2008 r. o sygn. DOLiS-035-996/08.

³¹⁷ Pismo Komendanta Głównego Policji z dnia 17 października 2008 r. o sygn. Nt-1332/1197/08/.

³¹⁸ Pismo GİODO z dnia 15 maja 2009 r. o sygn. DOLiS-035-996/08.

³¹⁹ Pismo GİODO z dnia 15 maja 2009 r. o sygn. DOLiS-35-996/08.

³²⁰ Wystąpienie GİODO z dnia 14 listopada 2008 r. o sygn. DOLiS-035-1457/08.

³²¹ Pismo Komendanta Głównego Policji z dnia 25 listopada 2008 r. znak H-L-VI-2099/1982/08.

³²² Wystąpienie GİODO z dnia 23 grudnia 2008 r. o sygn. DOLiS-035-1457/08.

³²³ Zgodnie z art. 6 ust. 1 ustawy o ochronie danych osobowych, za dane osobowe uważa się także informacje dotyczące możliwej do zidentyfikowania osoby fizycznej, a nie tylko te dotyczące już zidentyfikowanej osoby.

³²⁴ Wystąpienie Generalnego Inspektora Ochrony Danych Osobowych z dnia 23 stycznia 2008 r. o sygn. DOLiS-035-23/08.

³²⁵ Art. 7 pkt 5 ustawy o ochronie danych osobowych.

³²⁶ Decyzja z dnia 28 sierpnia 2007 r. o sygn. Nr DRTD-WUD-60503-10/06(45).

³²⁷ Dz. U. Nr 171, poz. 1800 z późn. zm.

Prawo telekomunikacyjne³²⁸ zezwalająca w art. 70 ust. 1 na zamieszczenie danych abonentów w spisie oraz udostępnianie tych danych za pośrednictwem służb informacyjnych przedsiębiorcy telekomunikacyjnego - o ile nie złożyli oni zastrzeżenia z art. 70 ust. 3 tej ustawy - utraciła moc (w zasadniczej części) 3 września 2004 r. Aktualnie obowiązująca ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, uzależniła zaś zamieszczenie w nowo utworzonym spisie wskazanych w jej art. 169 ust. 1³²⁹ danych identyfikujących abonenta będącego osobą fizyczną od uprzedniego wyrażenia przez niego zgody (art. 169 ust. 3).³³⁰ Skoro zatem w ustawie z dnia 16 lipca 2004 r. brak jest przepisów intertemporalnych dotyczących wskazanej wyżej kwestii, to od dnia wejścia w życie tej ustawy zamieszczenie w nowo utworzonym spisie – wskazanych w art. 169 ust. 1 – danych identyfikujących abonenta będącego osobą fizyczną, wymaga jego swobodnie wyrażonej i jednoznacznej zgody. Powyższą zasadę stosować należy także w przypadku pozyskiwania danych na potrzeby utworzenia Ogólnokrajowego Spisu Abonentów. W świetle dyspozycji art. 169 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, każdy będący osobą fizyczną abonent powinien mieć możliwość podjęcia decyzji (złożenia oświadczenia woli), czy chce, by jego dane wskazane w ust. 1 tego artykułu znalazły się w przedmiotowym spisie. W przypadku braku takiego oświadczenia lub w przypadku decyzji negatywnej, przedsiębiorca telekomunikacyjny nie może udostępnić danych osobowych abonenta innemu przedsiębiorcy przygotowującemu – na podstawie decyzji Prezesa Urzędu Komunikacji Elektronicznej – Ogólnokrajowy Spis Abonentów oraz nie może świadczyć usługi ogólnokrajowej informacji o numerach telefonicznych. Pogląd taki znajduje pełne oparcie w treści art. 103 ust. 3 cytowanej ustawy.³³¹ Generalny Inspektor dodał również, że zgodnie z treścią art. 169 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, odrębnej zgody abonenta wymagać będzie zamieszczenie w Ogólnokrajowym Spisie Abonentów jego danych przekraczających zakres wskazany w ust. 1 tego artykułu. W odpowiedzi na powyższe, Prezes Urzędu Komunikacji Elektronicznej poinformował o zmianie swojego stanowiska dotyczącego odbierania zgód od abonentów i wydaniu w tej sprawie stosownego komunikatu.³³²

Ustawa o ochronie danych osobowych skonkretyzowała konstytucyjnie zagwarantowane każdemu prawo do decydowania o tym komu, w jakim zakresie oraz w jakim celu przekazywane są dotyczące go dane osobowe i określiła sytuacje, w których przetwarzanie danych jest dopuszczalne. Wśród sytuacji takich wymieniła m.in. istnienie przepisów prawa, które przyznają określonym podmiotom uprawnienie do wykonywania na danych osobowych pewnych operacji.³³³ Zważywszy, że inne niż ustawa o ochronie danych osobowych akty prawne mogą stanowić podstawę do przetwarzania danych osobowych istotne jest, aby treść ich przepisów pozostawała w zgodzie z przepisami wspomnianej ustawy. Jeżeli zatem w toku analizy określonych przepisów organ do spraw ochrony danych osobowych stwierdzi, iż są one sprzeczne z przepisami o ochronie danych osobowych, występuje do projektodawców o podjęcie prac legislacyjnych zmierzających do wyeliminowania zaistniałych rozbieżności.

Tytułem przykładu można wskazać pismo skierowane w 2008 r. do Ministra Zdrowia,³³⁴ w którym Generalny Inspektor wystąpił o podjęcie działań legislacyjnych mających na celu zmianę aktualnego brzmienia art. 20 ust. 2 pkt 3 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.³³⁵

³²⁸ Dz. U. Nr 73, poz. 852 z późn. zm.

³²⁹ Art. 169 ust. 1 tej ustawy stanowi, iż dane osobowe zawarte w publicznie dostępnym spisie abonentów, zwanym dalej spisem, 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.

³³⁰ Zgodnie z tym przepisem, zamieszczenie w spisie danych identyfikujących abonenta będącego osobą fizyczną może nastąpić wyłącznie po uprzednim wyrażeniu przez niego zgody na dokonanie tych czynności.

³³¹ Stosownie do jego treści, do usługi ogólnokrajowej informacji o numerach abonentów oraz do sporządzania ogólnokrajowego spisu abonentów i związanego z tym udostępniania danych stosuje się przepisy art. 161 i art. 169.

³³² Pismo Prezesa Urzędu Komunikacji Elektronicznej z dnia 3 marca 2008 r. znak DDRT-WUD-0746-1/08(2).

³³³ Art. 23 ust. 1 pkt 2 oraz art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

³³⁴ Wystąpienie GIODO z dnia 13 sierpnia 2008 r. o sygn. DOLIS-035-500/08.

³³⁵ Zgodnie z tym przepisem, świadczeniodawca, o którym mowa w ust. 1: 1) ustala kolejność udzielenia świadczenia opieki zdrowotnej na podstawie zgłoszeń świadczeniobiorcy; 2) informuje pisemnie świadczeniobiorcę o terminie udzielenia świadczenia oraz uzasadnia przyczyny wyboru tego terminu; 3) wpisuje za zgodą świadczeniobiorcy lub jego przedstawiciela ustawowego: a) numer kolejny, b) datę i godzinę wpisu, c) imię i nazwisko świadczeniobiorcy, d) numer PESEL, a w przypadku jego braku - numer dokumentu potwierdzającego tożsamość świadczeniobiorcy, e) rozpoznanie lub powód przyjęcia, f) adres świadczeniobiorcy, g) numer telefonu lub oznaczenie innego sposobu komunikacji ze świadczeniobiorcą lub jego opiekunem, h) termin udzielenia świadczenia, i) imię i nazwisko oraz podpis osoby dokonującej wpisu - w kolejnej pozycji prowadzonej przez siebie listy oczekujących na udzielenie świadczenia (Dz. U. Nr 210, poz. 2135 z późn. zm.)

Sprawa dotyczyła przypadku przetwarzania przez świadczeniodawców danych osobowych świadczeniobiorców w związku z prowadzeniem na podstawie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych tzw. „list oczekujących”. W treści swego wystąpienia organ do spraw ochrony danych osobowych podkreślił, iż w sytuacji, gdy podstawę przetwarzania danych osobowych stanowią przepisy prawa, pozyskiwanie od osób, których dane dotyczą, dodatkowej zgody na przetwarzanie tych danych jest zbędne i wprowadza w błąd co do możliwości i ewentualnie skutków jej niewyrażenia. Zatem zbędne jest odbieranie od świadczeniobiorców zgody³³⁶ w związku ze zgłoszeniem oczekiwania na udzielenie świadczenia w sytuacji, gdy świadczeniodawca i tak ma prawo do przetwarzania danych osobowych świadczeniobiorcy na podstawie art. 20 ust. 2 pkt 3 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Wymóg wyrażenia przez świadczeniobiorcę zgody byłby zrozumiały ewentualnie w sytuacji, gdyby zgoda ta oznaczała fakt zaakceptowania przez świadczeniobiorcę przedstawionych mu przez świadczeniodawcę warunków związanych z wpisem na listę oczekujących, na przykład co do terminu udzielenia świadczenia, przed jego dokonaniem. Generalny Inspektor wskazał na konieczność zmiany aktualnego brzmienia kwestionowanego przepisu tak, aby „wpisywanie” danych osobowych świadczeniobiorcy na prowadzoną przez świadczeniodawcę listę oczekujących na udzielenie świadczenia nie było uzależnione od wyrażenia zgody na ich przetwarzanie przez osobę, której dane dotyczą. W odpowiedzi Minister Zdrowia zapewnił, iż zgłoszona uwaga uwzględniona zostanie przy najbliższych pracach legislacyjnych dotyczących ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.³³⁷

Kierowanie przez Generalnego Inspektora wystąpień do podmiotów z sektora publicznego przetwarzających dane osobowe, nie jest jedyną formą kształtowania świadomości społecznej w zakresie podstawowych zasad przetwarzania danych osobowych wynikających z przepisów o ich ochronie oraz praw i obowiązków obu stron tego procesu. Równie ważne miejsce w tym zakresie zajmuje udzielanie przez organ do spraw ochrony danych osobowych odpowiedzi na indywidualne pytania. W analizowanym okresie Generalny Inspektor wielokrotnie wypowiadał się w związku z wątpliwościami podnoszonymi przez podmioty publiczne. Liczba i różnorodność pytań, które podlegały analizie w 2008 r. wskazuje, iż nadal ochrona danych osobowych jest materią skomplikowaną i jednocześnie ważną dla funkcjonowania tych podmiotów.

Wśród przesłanych do organu do spraw ochrony danych osobowych zapytań znalazła się m.in. prośba o wyjaśnienie statusu kierownika urzędu stanu cywilnego z punktu widzenia ustawy o ochronie danych osobowych. Pytanie dotyczyło kwestii, czy administratorem danych gromadzonych w związku z wykonywaniem działalności przez ww. urząd jest jego bezpośredni kierownik, czy może wójt, burmistrz, prezydent miasta.³³⁸ Wyjaśniając ten problem, Generalny Inspektor wskazał bezpośrednio na przepisy, z których wynika, iż administratorem danych w tym przypadku jest wójt (odpowiednio burmistrz lub prezydent miasta).³³⁹ Wskazał ponadto na istotny z punktu widzenia zasygnalizowanego problemu wyrok Naczelnego Sądu Administracyjnego³⁴⁰ oraz literaturę przedmiotu.³⁴¹

Zagadnienie obowiązków administratora danych pojawił się również w związku z realizacją ustawy z dnia 7 września 2007 r. o Karcie Polaka.³⁴² Rozstrzygając wątpliwości pytających, Generalny Inspektor wskazał, iż administratorem danych jest podmiot decydujący o celach i środkach przetwarzania danych osobowych.³⁴³ W przypadku podmiotów należących do sektora publicznego obowiązek przetwarzania określonych danych czy też tworzenia konkretnych zbiorów danych, wynikać powinien z przepisów

³³⁶ W rozumieniu art. 7 pkt 5 ustawy o ochronie danych osobowych.

³³⁷ Pismo Ministra Zdrowia z dnia 2 grudnia 2008 r. znak MZ-UZ-RP-71-13969-1/JC/08.

³³⁸ DOLiS-035-786/08.

³³⁹ Zgodnie z art. 5a ust. 1 ustawy z dnia 29 września 1986 r. Prawo o aktach stanu cywilnego (Dz. U. z 2004 r. Nr 161, poz. 1688 z późn. zm.), urzędy stanu cywilnego wchodziły w skład urzędu gminy. Gmina stanowiła okręg urzędu stanu cywilnego (ust. 2). Stosownie do art. 6 ust. 1 tej ustawy, czynności z zakresu rejestracji stanu cywilnego dokonuje kierownik urzędu stanu cywilnego lub jego zastępca (zastępcy). Kierownikiem urzędu stanu cywilnego jest wójt lub burmistrz (prezydent) (ust. 2). Ze względu na szeroki zakres obowiązków wójtów i burmistrzów, ust. 3 stanowi, że rada gminy może powołać innego kierownika urzędu stanu cywilnego i jego zastępcę albo zastępców.

³⁴⁰ Wyrok Naczelnego Sądu Administracyjnego z 2007 r. o sygn. akt II OSK 1324/2007, z którego wynika, iż wójt jest z mocy prawa kierownikiem urzędu stanu cywilnego. Zachowuje on swe uprawnienia także wtedy, gdy rada gminy powoła innego kierownika urzędu stanu cywilnego.

³⁴¹ W praktyce w większości gmin działają odrębnie powoływani kierownicy, zaś wójt lub burmistrz wykonują czynności najczęściej w przypadku nieobecności kierownika urzędu i jego zastępcy albo też w celu nadania czynności szczególnie uroczystego charakteru (Zob.: A. Czajkowska, E. Pachniewska, *Prawo o aktach stanu cywilnego. Komentarz, orzecznictwo, wzory dokumentów i pism*, Warszawa 2005, Wydawnictwo Prawnicze LexisNexis, wydanie III, ss. 496).

³⁴² Dz. U. Nr 180, poz. 1280 z późn. zm. Sprawa o sygn. DOLiS-035-698/08.

³⁴³ Art. 7 pkt 4 ustawy o ochronie danych osobowych.

prawa³⁴⁴, natomiast to regulacje zawarte w przywołanej ustawie o Karcie Polaka wprost przesądzają, który z podmiotów jest administratorem danych pozyskanych w związku z realizacją jej postanowień. Skoro w art. 23 ust. 1 ustawy o Karcie Polaka nałożono na konsula obowiązek prowadzenia, w zakresie swojej właściwości, rejestrów złożonych wniosków o przyznanie Karty Polaka, decyzji wydanych w tych sprawach oraz przyznanych i unieważnionych Kart Polaka, tym samym organ ten uznać należy za administratora danych zgromadzonych w tym rejestrze. Za takim stanowiskiem jednoznacznie przemawia treść § 2 rozporządzenia Rady Ministrów z dnia 21 marca 2008 r. w sprawie rejestrów Kart Polaka.³⁴⁵

Konsekwentnie w odniesieniu do danych w centralnym rejestrze przyznanych i unieważnionych Kart Polaka³⁴⁶ administratorem danych jest Rada do Spraw Polaków na Wschodzie; organ administracji publicznej powołany w celu rozpatrywania odwołań od decyzji w sprawach Karty Polaka³⁴⁷ i właściwy w sprawach wznowienia postępowania, uchylenia, zmiany lub stwierdzenia nieważności wydanych przez siebie decyzji lub postanowień³⁴⁸. Uznanie Rady do Spraw Polaków na Wschodzie za administratora danych zgromadzonych w centralnym rejestrze przyznanych i unieważnionych Kart Polaka znajduje dodatkowe uzasadnienie w brzmieniu § 7 rozporządzenia Rady Ministrów w sprawie rejestrów Kart Polaka.³⁴⁹

W 2008 r. Generalny Inspektor wypowiedział się również³⁵⁰ co do możliwości powierzenia – w drodze decyzji – przez Komendanta Głównego Straży Granicznej przetwarzania danych osobowych komendantom oddziałów i ośrodków szkolenia oraz komendantom placówek i dywizjonów Straży Granicznej, na podstawie art. 31 ustawy o ochronie danych osobowych³⁵¹ oraz wydawania przez te podmioty upoważnień wskazanych w art. 37 tej ustawy.³⁵² W pierwszej kolejności ustalenia wymagało, któremu z ww. podmiotów przysługuje w tym przypadku status administratora danych.³⁵³ Było to o tyle istotne, iż na ten właśnie podmiot ustawa o ochronie danych osobowych nakłada najwięcej obowiązków związanych z przetwarzaniem danych osobowych. W odniesieniu do podmiotów publicznych o tym, czy dany organ jest administratorem danych decydują przede wszystkim rodzaj i charakter nadanych mu przez prawo kompetencji z zakresu spraw publicznych oraz wyznaczone ustawowo zadania. Z przepisów ustawy z dnia 12 października 1990 r. o Straży Granicznej³⁵⁴ – m.in. art. 3 ust. 1 i ust. 4³⁵⁵, jak i z wielu innych, w tym z art. 3a pkt 3 oraz pkt 5³⁵⁶ – wynika, iż administratorem danych przetwarzanych przez Straż Graniczną w związku z realizacją jej ustawowych zadań związanych z ochroną granicy państwowej jest Komendant Główny Straży Granicznej. Co za tym idzie, to ten podmiot jest zobowiązany m.in. do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.³⁵⁷ Komendant Główny Straży Granicznej powinien zatem prowadzić dokumentację opisującą sposób przetwarzania danych oraz środki, o których wyżej mowa, jak również wydawać upoważnienia do przetwarzania danych osobowych, albowiem jedynie osoby je posiadające – stosownie do treści art. 37 ustawy o ochronie danych osobowych – mogą być dopuszczone do przetwarzania danych osobowych. Na nim także spoczywa obowiązek

³⁴⁴ Art. 7 Konstytucji Rzeczypospolitej Polskiej.

³⁴⁵ Zgodnie z tym przepisem, rejestr konsularny jest prowadzony przez konsula w formie elektronicznej (Dz. U. Nr 53, poz. 314).

³⁴⁶ Art. 23 ust. 3 ustawy o Karcie Polaka.

³⁴⁷ Art. 9 ust. 2 tej ustawy.

³⁴⁸ Art. 9 ust. 4 ustawy.

³⁴⁹ Rejestr centralny jest prowadzony przez Radę do Spraw Polaków na Wschodzie w formie elektronicznej.

³⁵⁰ Pismo GİODO z dnia 12 maja 2008 r. o sygn. DOLiS-035-353/08.

³⁵¹ Zgodnie z ust. 1 tego przepisu, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot, o którym mowa w ust. 1 – stosownie do treści ust. 2 – może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Jest on ponadto zobowiązany 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). Jak natomiast stanowi ust. 5 art. 31, do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.

³⁵² Stosownie do jego treści, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

³⁵³ Zgodnie z art. 7 pkt 4 ustawy o ochronie danych osobowych, administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych.

³⁵⁴ Dz. U. z 2005 r. Nr 234, poz. 1997 z późn. zm.

³⁵⁵ Jak stanowi art. 3 ust. 1 tej ustawy, centralnym organem administracji rządowej właściwym w sprawach ochrony granicy państwowej i kontroli ruchu granicznego jest Komendant Główny Straży Granicznej, podległy ministrowi właściwemu do spraw wewnętrznych. Komendant Główny Straży Granicznej jest przełożonym wszystkich funkcjonariuszy Straży Granicznej (ust. 4).

³⁵⁶ Zgodnie z art. 3a pkt. 3 i 5, do zakresu działania Komendanta Głównego Straży Granicznej należy w szczególności nadawanie regulaminów organizacyjnych komendom oddziałów Straży Granicznej oraz komórkom organizacyjnym Komendy Głównej Straży Granicznej, a także nadawanie statutów ośrodkom szkolenia Straży Granicznej oraz sprawowanie nadzoru nad terenowymi organami Straży Granicznej oraz nad ośrodkami szkolenia Straży Granicznej.

prowadzenia ewidencji osób upoważnionych do przetwarzania danych zawierającej imiona i nazwiska osób upoważnionych, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.³⁵⁸ Jednocześnie nic nie stoi na przeszkodzie, aby administrator danych wyznaczył administratora bezpieczeństwa informacji [ABI]. Może też ewentualnie wyznaczyć kilku administratorów bezpieczeństwa informacji, po jednym w każdej jednostce terenowej Straży Granicznej i upoważnić go (ich) do wykonywania w jego imieniu ww. czynności. W przypadku powołania kilku ABI, każdy byłby odpowiedzialny za przestrzeganie zasad ochrony danych osobowych na obszarze „swojej” jednostki. Upoważnienie, o którym mowa wyżej, może być wydane w formie zarządzenia lub decyzji Komendanta Głównego Straży Granicznej. Upoważnienie to obejmować może np. wydawanie upoważnień do przetwarzania danych w imieniu administratora danych (tu – Komendanta Głównego Straży Granicznej). Natomiast w tym przypadku nie jest możliwe zastosowanie konstrukcji powierzenia przetwarzania danych w drodze decyzji Komendanta Głównego Straży Granicznej, gdyż sprowadzałoby się to do uznania, iż jeden i ten sam podmiot – choć realizujący zadania publiczne w „strukturze rozproszonej” – powierzałby przetwarzanie danych swojej jednostce terenowej (wchodzącej w skład struktury organizacyjnej), której kadra niezależnie od ewentualnego istnienia umowy powierzenia, zobligowana jest ustawowo do przestrzegania zasad ochrony danych osobowych pod rygorem odpowiedzialności karnej.³⁵⁹ Ponadto wykluczyć należy możliwość zastosowania umowy powierzenia przetwarzania danych w drodze jednostronnego przekazania określonych zadań podmiotowi podległemu w stosunku do administratora danych.

Jak co roku, w pytaniach kierowanych do GIODO podnoszona była kwestia konieczności zgłoszenia określonych zbiorów danych do rejestracji Generalnemu Inspektorowi.³⁶⁰ Jedna z izb lekarskich zwróciła się z prośbą o dokonanie przez organ do spraw ochrony danych osobowych rozstrzygnięcia, co do obowiązku zarejestrowania przez nią ewidencji lekarzy zrzeszonych w tej izbie zgodnie z przepisami ustawy z dnia 17 maja 1989 r. o izbach lekarskich,³⁶¹ zbioru osób ubezpieczonych przez ten podmiot jako agenta pewnego towarzystwa ubezpieczeniowego oraz zbioru danych osobowych dotyczącego osób związanych ze sprawami prowadzonymi przez Okręgowego Rzecznika Odpowiedzialności Zawodowej Lekarzy oraz Okręgowy Sąd Lekarski.³⁶²

Generalny Inspektor wyjaśnił, że podstawę zwolnienia z obowiązku rejestracji zbioru danych stanowiącego ewidencję lekarzy zrzeszonych w izbie lekarskiej stanowi art. 43 ust. 1 pkt 4 ustawy.³⁶³ Zwolnienie określone w powołanym przepisie obejmuje m.in. zbiory danych prowadzone przez spółdzielnie, stowarzyszenia, a także izby zrzeszające osoby wykonujące ten sam zawód, np. aptekarskie, rolnicze czy lekarskie.³⁶⁴

W odniesieniu do zbioru „osób ubezpieczonych” Generalny Inspektor zaznaczył, iż obowiązek zgłoszenia zbioru danych do rejestracji spoczywa na administratorze danych,³⁶⁵ a nie na podmiocie, któremu przetwarzanie danych osobowych zostało powierzone w drodze umowy wynikającej z art. 31 ustawy o ochronie danych osobowych.³⁶⁶ Najistotniejszymi elementami takiej umowy pozostają wskazanie celu i zakresu przetwarzanych danych, albowiem podmiot, który je otrzymał może wykonywać na nich operacje wyłącznie w zakresie i celu wskazanym w umowie. Takie relacje łączą zakłady ubezpieczeniowe czy towarzystwa

³⁵⁷ Środki te wskazane zostały w rozdziale 5 ustawy o ochronie danych osobowych, zaś w przypadku przetwarzania danych w systemie informatycznym – w przepisach 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 osobowych.

³⁵⁸ Art. 38 ustawy.

³⁵⁹ Zgodnie bowiem z art. 51 ust. 1 ustawy o ochronie danych osobowych, 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).

³⁶⁰ Zgodnie z art. 40 ustawy o ochronie danych osobowych, administrator danych jest obowiązany zgłosić zbiór danych Generalnemu Inspektorowi do rejestracji z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 ustawy.

³⁶¹ Dz. U. Nr 30, poz. 158 z późn. zm.

³⁶² DOLiS-035-809/08.

³⁶³ Przepis ten stanowi, iż z obowiązku rejestracji zwolnieni są administratorzy danych przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się.

³⁶⁴ Zob. A. Drodz, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007, Wydawnictwo Prawnicze LexisNexis, wydanie III, ss. 504.

³⁶⁵ Art. 7 pkt 4 ustawy o ochronie danych osobowych.

³⁶⁶ Stosownie do treści tego przepisu, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot, o którym mowa, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Ponadto jest on 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. W przypadkach, o których mowa wyżej, odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę,

ubezpieczeniowe z ich agentami. Agent wykonuje bowiem swe zadania – ściśle określone w zawartej umowie – działając w imieniu i na rzecz zakładu lub towarzystwa. Natomiast nie decyduje o celu, w jakim przetwarza zgromadzone dane, stąd trudno uznać go za samodzielnego administratora danych.

Odmienne przedstawia się natomiast kwestia zbiorów danych osobowych przetwarzanych przez izbę lekarską w związku ze sprawami prowadzonymi przez Okręgowego Rzecznika Odpowiedzialności Zawodowej Lekarzy oraz Okręgowy Sąd Lekarski, o czym jest mowa w przepisach ustawy o izbach lekarskich. Wobec braku przesłanek zwalniających administratora danych z konieczności zgłoszenia Generalnemu Inspektorowi powstałych w powyższy sposób zbiorów danych do rejestracji, istnieje konieczność takiego zgłoszenia.

W omawianym okresie sprawozdawczym – podobnie jak w ubiegłych latach – Generalny Inspektor interweniował wielokrotnie w związku z wątpliwym, co do zgodności z literą prawa, przetwarzaniem danych osobowych przez **podmioty z sektora prywatnego**, wyjaśniając m.in., że także i te podmioty zobowiązane są do przestrzegania przepisów regulujących kwestie ochrony danych osobowych.

W związku z dokonaną analizą treści formularza oświadczenia o wyrażeniu zgody przez abonenta na zamieszczenie identyfikujących go danych w publicznym spisie abonentów oraz udostępnienie ich za pomocą tzw. biura numerów, konieczne stało się wyjaśnienie przez przedsiębiorcę telekomunikacyjnego, co należy rozumieć pod pojęciem zagranicznych przedsiębiorców telekomunikacyjnych, którym mają być przekazywane dane.³⁶⁷ W formularzu zawarta była informacja, że „dane będą przekazane innemu podmiotowi w celu zlecenia publikacji spisu abonentów (książki telefonicznej), a także innym przedsiębiorcom telekomunikacyjnym (w tym zagranicznym) w celu świadczenia przez nich usług informacji o numerach telefonicznych oraz publikacji spisu abonentów.”

W szczególności powstało pytanie, czy zagraniczni przedsiębiorcy telekomunikacyjni, którym mają być przekazywane dane, to przedsiębiorcy mający siedzibę na terenie Unii Europejskiej, czy chodzi również o przedsiębiorców telekomunikacyjnych spoza Unii, mających siedzibę w państwach nienależących do Europejskiego Obszaru Gospodarczego [EOG]. Jeśli przedsiębiorcy mają siedzibę poza EOG, to jakie są podstawy prawne przekazywania danych do operatorów znajdujących się w państwach trzecich.³⁶⁸ W przesłanym wyjaśnieniu Spółka wskazała, iż pojęcie zagranicznych przedsiębiorców telekomunikacyjnych odnosi się do jedynie do tych, którzy mają siedzibę na terytorium Europejskiego Obszaru Gospodarczego.³⁶⁹ Generalny Inspektor zwrócił się więc do Spółki o dokonanie stosownej modyfikacji formularzy zawierających ww. oświadczenia, aby z ich treści w sposób niebudzący wątpliwości wynikało, że w tym przypadku chodzi wyłącznie o przedsiębiorców z EOG.³⁷⁰ Spółka po dokonaniu stosownych modyfikacji przesała GODO nowo opracowany formularz do zaopiniowania. Aktualnie jego treść pozostaje przedmiotem analizy organu ds. ochrony danych osobowych.³⁷¹

W okresie objętym sprawozdaniem pojawiły się w publikacjach prasowych informacje, z których wynikało, iż jeden z przedsiębiorców uprawnionych do wykonywania działalności pocztowej gromadzi i przekazuje pewnemu funduszowi emerytalnemu dane osób, którym Zakład Ubezpieczeń Społecznych [ZUS] za pośrednictwem tegoż przedsiębiorcy wysyła korespondencję dotyczącą konieczności zawarcia umowy z otwartym funduszem emerytalnym, pod rygorem wyboru właściwego funduszu przez sam Zakład w drodze losowania.³⁷² Generalny Inspektor zwrócił się do Dyrektora Generalnego Poczty Polskiej

za przetwarzanie danych niezgodnie z tą umową. Do kontroli zgodności przetwarzania danych przez wskazany podmiot z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.

³⁶⁷ Wystąpienie GODO z dnia 24 lipca 2008 r. o sygn. DOLiS-035-950/08.

³⁶⁸ Jakkolwiek bowiem przetwarzanie, w tym przekazywanie danych osobowych podmiotom mającym siedzibę na terytorium Europejskiego Obszaru Gospodarczego podlega takim samym wymogom, jak przetwarzanie danych na obszarze Rzeczypospolitej Polskiej, tak już ich przekazywanie poza ten obszar obwarowane jest koniecznością respektowania – poza powyższymi – także zasad przekazywania danych zamieszczonych w rozdziale 7 ustawy o ochronie danych osobowych -Przekazywanie danych osobowych do państwa trzeciego.

³⁶⁹ Pismo z dnia 8 sierpnia 2008 r. o sygn. SPOV/SPOOA-074-260/KS/PB/08.

³⁷⁰ Wystąpienie GODO z dnia 29 sierpnia 2008 r. o sygn. DOLiS-035-950/08.

³⁷¹ Pismo GODO z dnia 28 maja 2009 r. o sygn. DOLiS-35-950/08.

³⁷² Zgodnie z art. 39 ust. 2 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2007 r. Nr 11, poz. 74 z późn. zm.), w przypadku gdy ubezpieczony nie dopełni obowiązku określonego w ust. 1, Zakład wzywa go na piśmie do zawarcia umowy z otwartym funduszem emerytalnym w terminie: 1) do dnia 10 stycznia - jeżeli od daty otrzymania wezwania do dnia losowania jest mniej niż 30 dni, termin ten mija 10 lipca; 2) do dnia 10 lipca - jeżeli od daty otrzymania wezwania do dnia losowania jest mniej niż 30 dni, termin ten mija 10 stycznia. Jeżeli ubezpieczony nie dopełni obowiązku zawarcia umowy w tych

o wskazanie podstawy prawnej tego typu działań³⁷³ podnosząc, że dopuszczalność gromadzenia i dalszego przetwarzania (w tym przekazywania) przez tego przedsiębiorcę danych osobowych ubezpieczonych, którzy nie dokonali wyboru otwartego funduszu emerytalnego, jest uzależniona od spełnienia jednej z przesłanek legalności przetwarzania danych.

Dyrektor przedsiębiorstwa poinformował Generalnego Inspektora, że przeprowadzone przez niego czynności wyjaśniające nie potwierdziły doniesień prasowych oraz podzielił pogląd, że działania pracowników przedsiębiorstwa polegające na ewentualnym przekazywaniu funduszowi emerytalnemu danych osób, do których kierowana jest przez ZUS korespondencja przypominająca o konieczności zawarcia umowy z funduszem, jako nie znajdujące podstaw w przepisach prawa, byłyby sprzeczne z ustawą o ochronie danych osobowych.³⁷⁴

W związku z uzyskaniem przez Generalnego Inspektora informacji, iż dane osobowe pozyskiwane przez jedną ze spółek zajmujących się świadczeniem usług informatycznych za pomocą formularza rejestracyjnego zamieszczonego na jej stronie internetowej nie są dostatecznie chronione przed dostępem osób nieupoważnionych, organ do spraw ochrony danych osobowych zwrócił się do tego podmiotu o zastosowanie odpowiednich środków technicznych i organizacyjnych, które zapewnią właściwą ochronę przetwarzanych danych.³⁷⁵ Zamieszczane w treści formularza rejestracyjnego przez klientów sklepu internetowego ich dane osobowe, były bowiem transmitowane za pośrednictwem sieci internetowej bez uprzedniego zaszyfrowania. Generalny Inspektor podkreślił, że administrator danych musi wywiązywać się z obowiązku dołożenia należytej staranności w celu ochrony interesów osób, których dane dotyczą,³⁷⁶ a także z postanowień art. 36 powołanego aktu prawnego.³⁷⁷ Ponadto wskazała na treść załącznika do 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 osobowych, który w punkcie XIII stanowi, iż administrator danych obowiązany jest do stosowania środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej. Ochronę danych umożliwia tu w szczególności zastosowanie środków szyfrujących. Powyższe nie powinno wpłynąć na ograniczenie możliwości prowadzenia przez Spółkę działalności, a bez wątpienia pozwoli na uniknięcie zarzutu niedopełnienia obowiązku zabezpieczenia danych osobowych jej klientów osobom do tego nieupoważnionym.

Wskutek uwag zgłoszonych przez Generalnego Inspektora, Spółka podjęła działania zmierzające do wyeliminowania zasygnalizowanych nieprawidłowości i wprowadziła odpowiednie protokoły szyfrujące dane osobowe przesyłane przez klientów za pośrednictwem „formularzy internetowych”.³⁷⁸

Generalny Inspektor zareagował również na pojawiające się w mediach informacje dotyczące wprowadzenia przez jedną ze spółdzielni mieszkaniowych systemu wideonadzoru, który umożliwiał odbiór na odpowiednim kanale telewizyjnym obrazu z kamery monitorującej teren wokół osiedla. Sygnał ten w sposób ciągły przesyłany był do około 5 tysięcy mieszkań i - jak wynikało z doniesień - „(...) Każda kobieta (...)” mogła „(...) włączyć telewizor na odpowiednim kanale, by zobaczyć, czy na placu nie upija się jej mąż lub syn (...).”³⁷⁹

Generalny Inspektor zwrócił uwagę zarządu spółdzielni przede wszystkim na przysługujące każdemu prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.³⁸⁰ Prawo to nie może doznawać ograniczeń także w stanach nadzwyczajnych.³⁸¹ Obowiązek poszanowania prawa do prywatności wynika również z faktu, iż Rzeczpospolita Polska, jako państwo członkowskie Unii Europejskiej, jest stroną europejskiej Konwencji o ochronie praw

terminach, Zakład wyznacza otwarty fundusz emerytalny w drodze losowania, spośród otwartych funduszy emerytalnych, które uzyskały stopy zwrotu wyższe niż średnie ważone stopy zwrotu w dwóch ostatnich okresach rozliczeniowych podawane do publicznej wiadomości zgodnie z przepisami ustawy o organizacji i funkcjonowaniu funduszy emerytalnych, z zastrzeżeniem ust. 2a, i których aktywa na koniec drugiego okresu rozliczeniowego z roku poprzedniego nie przekraczały 10 % wartości aktywów netto wszystkich otwartych funduszy. Komisja Nadzoru Finansowego przekazuje do Zakładu wykaz otwartych funduszy emerytalnych biorących udział w losowaniu, nie później niż 10 dnia roboczego przed terminem przeprowadzania losowania.

³⁷³ Wystąpienie Generalnego Inspektora Ochrony Danych Osobowych z dnia 9 stycznia 2008 r. o sygn. DOLiS-035-257/07.

³⁷⁴ Pismo dyrektora przedsiębiorstwa z dnia 15 lutego 2008 r.

³⁷⁵ Pismo GIODO z dnia 19 lutego 2008 r. o sygn. GI-DOLiS-035-207/08.

³⁷⁶ Art. 26 ust. 1 ustawy.

³⁷⁷ Obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym.

³⁷⁸ Pismo vice – prezesa Spółki z dnia 1 kwietnia 2008 r.

³⁷⁹ Wystąpienie GIODO z dnia 24 października 2008 r. o sygn. DOLiS-035-1368/08.

³⁸⁰ Art. 47 Konstytucji Rzeczypospolitej Polskiej.

człowieka i podstawowych wolności,³⁸² która w art. 8 ustanawia prawo do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji. Generalny Inspektor powołał także przyjętą w dniu 11 lutego 2004 r. opinię³⁸³ Grupy roboczej do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych.³⁸⁴ Istotne znaczenie ma również realizacja obowiązku informacyjnego wobec osób, których dane osobowe pozyskane zostały za pomocą nadzoru video, zgodnie z wymogami art. 10 i 11 ww. Dyrektywy 95/46/WE. Osoby te muszą mieć świadomość faktu prowadzenia czynności wideonadzoru. Tablice informacyjne o zainstalowaniu urządzeń video powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc oraz wskazywać cele działań nadzoru oraz administratora tego przetwarzania. Wobec zasygnalizowanych wątpliwości organu do spraw ochrony danych osobowych spółdzielnia zaprzestała stosowania monitoringu terenu.³⁸⁵

W 2008 r., wśród indywidualnych pytań kierowanych do GODO z sektora prywatnego, pojawiały się między innymi te dotyczące zatrudnienia.

W jednej ze spraw Generalny Inspektor wypowiedział się co do konieczności zamieszczania w treści CV klauzuli zgody na przetwarzanie danych osobowych przez kandydata do pracy w związku z prowadzonym przez pracodawcę postępowaniem rekrutacyjnym, konsekwencjami jej niezamieszczenia oraz dopuszczalności praktyki polegającej na przechowywaniu „na zapas” dokumentacji należącej do kandydata, który nie został wyłoniony w postępowaniu rekrutacyjnym.³⁸⁶ Generalny Inspektor wskazał, iż zgoda osoby ubiegającej się o zatrudnienie na przetwarzanie jej danych osobowych dla celów rekrutacji jest zbędna, o ile dokumenty składane potencjalnemu pracodawcy zawierają dane w zakresie przewidzianym art. 22¹ Kodeksu pracy.

W odniesieniu do przechowywania przez pracodawcę dokumentów złożonych przez kandydata do pracy, który nie został jednak zatrudniony, celem ich ewentualnego wykorzystania w przyszłości, zastosowanie znajdzie zasada ograniczenia czasowego zawarta w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych.³⁸⁷ W literaturze przedmiotu podkreśla się, iż nawet wówczas, gdy określone dane odpowiadają celowi, dla którego są zbierane i są dla tego celu adekwatne, to nie wynika z tego, iż mogą być one przetwarzane (...) *ad infinitum*. Czasowym wyznacznikiem jest tu osiągnięcie zamierzonego celu przetwarzania.³⁸⁸ Gdy rekrutacja na określone stanowisko została już zakończona, zaś osoba kandydująca nie została zatrudniona, dalsze przetwarzanie, w tym przechowywanie przez pracodawcę jej danych osobowych jest bezpodstawne z uwagi na ustanie celu, dla którego zostały one zebrane.

Odmienny tryb postępowania należy zaś przyjąć w przypadku, gdy zakres danych kandydata do pracy przetwarzany dla celów rekrutacji wykracza poza określony w przepisach prawa pracy. W takiej sytuacji konieczne jest uzyskanie zgody osoby ubiegającej się o zatrudnienie na przetwarzanie jej danych w zakresie szerszym, niż ramy ustawowe. Należy przy tym pamiętać o zachowaniu zasady adekwatności, o której mowa w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Przechowywanie danych osoby, która nie została zatrudniona, celem ich wykorzystania podczas kolejnych, przyszłych rekrutacji, będzie dopuszczalne tylko wtedy, jeżeli osoba ta wyrazi na to zgodę.

Generalny Inspektor wypowiedział się również w kwestii zgodności z przepisami o ochronie danych osobowych udostępniania przez pracodawców związkom zawodowym informacji w zakresie obejmującym wysokość przysługującego danemu pracownikowi

³⁸¹ Art. 233 ust. 1 Konstytucji RP.

³⁸² Dokument sporządzony w Rzymie w dniu 4 listopada 1950 r.

³⁸³ Opinia nr 4/2004, w której zwrócono uwagę między innymi na konieczność, by przy posługiwaniu się wideonadzorem respektowana była zasada proporcjonalności (dane muszą być adekwatne i istotne dla celów przetwarzania), która oznacza przede wszystkim, że urządzenia video – nadzoru mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, niewymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami. Ta sama zasada dotyczy również wyboru odpowiedniej technologii, kryteriów wykorzystywania urządzeń w konkretnych sytuacjach oraz ustaleń dotyczących przetwarzania danych, odnoszących się także do zasad dostępu i okresu przechowywania.

³⁸⁴ Grupa robocza do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana została na podstawie art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L.95.281.31).

³⁸⁵ Pismo z dnia 19 listopada 2008 r. o sygn. 6408/08.

³⁸⁶ DOLiS-035-62/08.

³⁸⁷ Zgodnie z tym przepisem, administrator danych przetwarzający dane powinien dolożyć należytej 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.

³⁸⁸ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*. Kraków 2007, s. 509 - 510.

wynagrodzenia.³⁸⁹ Kwestie dotyczące zasad prowadzenia działalności związkowej oraz uprawnień i obowiązków związków zawodowych określone zostały w przepisach prawa.³⁹⁰ Prawo związków zawodowych do uzyskiwania informacji oraz obowiązki pracodawcy w tym zakresie reguluje art. 28 ustawy o związkach zawodowych.³⁹¹ Powołany akt prawny nie precyzuje jednak, jakiego rodzaju informacje są niezbędne do prowadzenia działalności związkowej. A zatem zakres i rodzaj tych informacji determinowany jest zakresem ustawowych zadań związków zawodowych. Wyrażona w art. 28 ustawy o związkach zawodowych ogólna zasada, przyznająca związkom zawodowym dostęp do informacji niezbędnych do prowadzenia działalności związkowej, zobowiązuje pracodawcę do udzielenia im wszelkich informacji w zakresie objętym działaniem związku, określonym w przepisach ustawy o związkach zawodowych. W myśl powołanego artykułu pracodawca obowiązany jest między innymi do udzielenia związkowi zawodowemu informacji dotyczących zasad wynagradzania. Z powyższego wynika, iż pracodawca obowiązany jest do udzielenia informacji o wysokości funduszu płac i jego strukturze, przesłankach i wysokości kształtowania wynagrodzenia ogółu pracowników lub określonej grupy zawodowej oraz innych czynnikach warunkujących wysokość wynagrodzenia. Co do zasady, nie może mieć miejsca sytuacja udzielania przez pracodawcę informacji o wysokości wynagrodzenia poszczególnych pracowników bez ich zgody. Istotna jest w tym przypadku jedna z uchwał Sądu Najwyższego³⁹² stwierdzająca, iż informacje o wynagrodzeniu pracownika zaliczyć należy do tej grupy informacji, do których dostęp możliwy jest wyłącznie za zgodą osoby, której one dotyczą lub wówczas, gdy szczególny przepis prawa wprost upoważnia określone podmioty do ich uzyskania. Art. 27 ust. 3 ustawy o związkach zawodowych uprawnia je do współuczestnictwa w ustalaniu regulaminu nagród i premiowania. Nie wydaje się jednak, aby uprawnienie to można było utożsamiać choćby z prawem do żądania imiennych list pracowników z podaniem kwot wypłaconej im premii lub nagrody (nawet jeśli to będzie ujawnione, np. w procentach). Co do zasady, tego rodzaju działanie byłoby dopuszczalne w przypadku, gdyby każdy pracownik, którego informacja ta dotyczy, wyraził zgodę na jej udostępnienie.

Inna sytuacja w zakresie dopuszczalności pozyskiwania przez związki zawodowe powyższych informacji miałyby miejsce wyłącznie wówczas, gdyby u danego pracodawcy obowiązywały takie akty normatywne regulujące prawa i obowiązki pracowników oraz pracodawców o charakterze wewnętrznym (np. regulaminy), które w swej treści przewidują uprawnienie związków zawodowych do uczestnictwa w ustalaniu zasad przyznawania nagród i premii oraz do kontrolowania faktu ich przyznania lub nawet ich wysokości.

Niemniej powyższe zagadnienie nie było jedynym problemem nurtującym w 2008 r. związki zawodowe i pracodawców w kwestii przetwarzania danych osobowych. Wątpliwości budziła również sprawa legalności żądania przez związek zawodowy od pracodawcy listy aktualnie zatrudnionych u niego pracowników w celu zorganizowania przez związek referendum strajkowego.³⁹³

Wypowiadając się w tej sprawie, Generalny Inspektor zwrócił uwagę na art. 20 ust. 1 ustawy z dnia 23 maja 1991 r. o rozwiązywaniu sporów zbiorowych,³⁹⁴ z którego wynika, iż decyzja dotycząca strajku wymaga uprzedniej akceptacji pracowników wyrażonej w głosowaniu. Strajk wiąże się bowiem już z osobistym zaangażowaniem pracowników. Sposób głosowania określa organizacja związkowa – może ono być tajne bądź jawne, przeprowadzone na zebraniu lub przez złożenie podpisu na odpowiedniej liście, albo w inny jeszcze sposób. Istotne jest, aby wszyscy zainteresowani mieli możliwość wyrażenia osobiście swego stanowiska w tej sprawie.³⁹⁵ Skoro w myśl art. 18 powołanej ustawy, udział w strajku jest dobrowolny to żaden pracownik nie może być zmuszany do uczestnictwa w strajku ani do powstrzymania się od przystąpienia do strajku. Pozyskiwanie

³⁸⁹ DOLiS-035-1693/08.

³⁹⁰ Ustawa z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2001 r. Nr 79, poz. 854 z późn. zm.).

³⁹¹ Przepis powyższy stanowi, iż pracodawca jest obowiązany udzielić na żądanie związku zawodowego informacji niezbędnych do prowadzenia działalności związkowej, w szczególności informacji dotyczących warunków pracy i zasad wynagradzania.

³⁹² Sąd Najwyższy w uchwale z dnia 16 lipca 1993 r. o sygn. I PZP 28/93 orzekł, iż „(...) uprawnienie do kontrolowania przez związki zawodowe przestrzegania prawa pracy (...) nie oznacza (...) uprawnienia do żądania od pracodawcy udzielenia informacji o wysokości wynagrodzenia pracownika bez jego zgody”, zaś „ujawnienie przez pracodawcę bez zgody pracownika wysokości jego wynagrodzenia za pracę może stanowić naruszenie dobra osobistego w rozumieniu art. 23 i 24 Kodeksu cywilnego”.

³⁹³ DOLiS-035-1552/08.

³⁹⁴ Dz. U. Nr 55, poz. 236 z późn. zm. Zgodnie z treścią tego artykułu, strajk zakładowy ogłasza organizacja związkowa po uzyskaniu zgody większości głosujących pracowników, jeżeli w głosowaniu wzięło udział co najmniej 50% pracowników zakładu pracy.

³⁹⁵ Por. *Prawo pracy. Tom III*, Warszawa 1997-2005, Wydawnictwo Prawnicze LexisNexis.

przez związek zawodowy danych osobowych w zakresie dotyczącym imion i nazwisk pracowników w celu zorganizowania przez ten związek referendum strajkowego, stanowi realizację prawnie usprawiedliwionego celu administratora danych.³⁹⁶ Ważne jest jednak, aby pracownicy, których dane osobowe miały zostać udostępnione, mieli świadomość tego rodzaju działania oraz byli zainteresowani wypowiedzeniem się w głosowaniu w referendum strajkowym. Generalny Inspektor przywołał jeden z wyroków Sadu Najwyższego dotyczący omawianej materii.³⁹⁷

W omawianym okresie sprawozdawczym do Biura Generalnego Inspektora wpłynęło również zapytanie dotyczące możliwości skanowania dokumentów tożsamości osób wchodzących na teren jednego z warszawskich budynków, będących klientami najemców lokali znajdujących się w tym budynku oraz ewentualnej konieczności zgłoszenia powstałego w ten sposób zbioru danych Generalnemu Inspektorowi do rejestracji zgodnie z obowiązkiem wynikającym z art. 40 ustawy o ochronie danych osobowych.³⁹⁸

Generalny Inspektor wskazał, iż kopiowanie dokumentu tożsamości – np. poprzez wykonanie jego skanu – jest czynnością techniczną, która ze swojej istoty nie jest zakazana przepisami ustawy o ochronie danych osobowych. Z punktu widzenia przepisów tej ustawy istotne jest jedynie, aby podmiot, który czynności tej dokonuje, legitymował się jedną z przesłanek legalności przetwarzania, w tym gromadzenia danych osobowych, oraz aby kopiowanie dokumentów nie prowadziło do gromadzenia danych w zakresie szerszym, niż to jest konieczne dla realizacji celu, w jakim dane są przetwarzane. Powołał przy tym potwierdzające powyższe stanowisko wyroki sądowe.³⁹⁹ Znaczenie ma także, czy pozyskiwanie danych będzie dokonywane przez pracowników ochrony,⁴⁰⁰ czy też przez pracowników portierni niebędących pracownikami ochrony. Uprawnienie pracowników ochrony do legitymowania osób wchodzących na teren określonego budynku wynika z przepisów ustawy o ochronie osób i mienia.⁴⁰¹ Przetwarzanie danych osób wchodzących na teren określonego budynku przez pracowników portierni znajduje natomiast podstawę w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych. Pozyskiwanie danych osobowych klientów czy „gości” najemców lokali z określonego budynku, zarówno przez pracowników ochrony, jak i przez pracowników portierni niebędących pracownikami ochrony, nie będzie zatem uznane za niezgodne z przepisami ustawy o ochronie danych osobowych. Konieczne jest także pozyskiwanie wyłącznie takiego zakresu danych, jaki jest niezbędny do osiągnięcia celu przetwarzania.⁴⁰² Poprzez wykonywanie kopii dokumentu tożsamości za pomocą jego zeskanowania pozyskiwane są dane w zakresie znacznie szerszym (jak np. wizerunek, wzrost, kolor oczu, miejsce urodzenia czy imiona rodziców osoby wchodzącej na teren określonego budynku), niż jest to niezbędne do osiągnięcia zamierzonego celu (tzn. zapewnienia kontroli dostępu do budynku). Pozyskiwanie w analizowanym przypadku danych osobowych osób wchodzących na teren budynku przez podmioty, o których wyżej mowa, będzie działaniem dopuszczalnym, o ile zażądają one od osób, których dane dotyczą jedynie informacji w zakresie niezbędnym do osiągnięcia celu gromadzenia danych, obejmującym np. imię, nazwisko oraz numer dokumentu tożsamości wraz z jego nazwą.

³⁹⁶ Art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych. Przepis ten stanowi o dopuszczalności przetwarzania danych, gdy 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.

³⁹⁷ Zgodnie z wyrokiem Sadu Najwyższego - Izby Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z dnia 7 lutego 2007 r. o sygn. akt I PK 209/2006, prawo do strajku należy do podstawowych praw człowieka oraz wolności związkowych. Wobec tego wątpliwości związane z wykładnią przepisów regulujących strajk powinny być – zgodnie z zasadą *in dubio pro libertate* – rozstrzygane na rzecz, a nie przeciwko wolności strajku.

³⁹⁸ Stosownie do treści przywołanego przepisu, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

³⁹⁹ Naczelny Sąd Administracyjny w wyroku z dnia 19 grudnia 2001 r. o sygn. akt II SA 2869/00 orzekł, iż „(...) gromadzenie danych osobowych przez wykonanie kopii dokumentu zawierającego te dane jest kwestią techniczną, obojętną dla prawodawcy reglamentującego w ustawie o ochronie danych osobowych przetwarzanie tego rodzaju danych. Inaczej mówiąc, posługiwanie się taką czy inną techniką utrwalania danych (kopiowanie lub przepisywanie) nie przesądza samo przez się o legalności albo nielegalności tego utrwalania (przetwarzania). Dla takich ocen istotne znaczenie mają przede wszystkim: podstawa prawna przetwarzania danych (art. 23 ustawy), rodzaj przetwarzanych danych (art. 27) oraz granice przetwarzania (art. 26 ust. 1 pkt 3) (...).” Analogiczne stanowisko zajął Naczelny Sąd Administracyjny w wyroku z dnia 7 listopada 2003 r. (sygn. akt II SA 1432/02) stanowiącym, iż „(...) ustawa o ochronie danych osobowych nie zajmuje się określaniem techniki gromadzenia danych osobowych, lecz zakresem ich przetwarzania (...)”.

⁴⁰⁰ W rozumieniu przepisów ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2005 r. Nr 145, poz. 1221 z późn. zm.).

⁴⁰¹ Zgodnie z art. 36 ust. 1 pkt 1 tej ustawy, pracownik ochrony przy wykonywaniu zadań ochrony osób i mienia w granicach chronionych obiektów i obszarów ma prawo do ustalania uprawnień do przebywania na obszarach lub w obiektach chronionych oraz legitymowania osób, w celu ustalenia ich tożsamości.

⁴⁰² Zasada adekwatności danych w stosunku do celów ich przetwarzania określona w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Zgodnie z art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych,⁴⁰³ administrator danych obowiązuje także zasada ograniczenia czasowego przetwarzania danych oraz obowiązek właściwego ich zabezpieczenia.⁴⁰⁴

Odpowiadając na pytanie dotyczące konieczności zgłoszenia powstałego w zasygnalizowany sposób zbioru danych do rejestracji, Generalny Inspektor wskazał, iż działanie polegające na przetwarzaniu danych osób wchodzących na teren określonego budynku - z uwagi na cel przetwarzania - nie będzie związane z koniecznością rejestracji powstałego w ten sposób zbioru, albowiem przetwarzanie danych w celu zapewnienia kontroli ruchu osobowego służy usprawnieniu działalności administratora danych. Zatem zbiór, który je zawiera, ma charakter pomocniczy i tym samym dane w nim zawarte traktować można jako przetwarzane w zakresie drobnych, bieżących spraw życia codziennego, o czym jest mowa w cytowanym powyżej art. 43 ust. 1 pkt 11 ustawy o ochronie danych osobowych.⁴⁰⁵

W 2008 r. problemy z praktycznym stosowaniem przepisów ustawy o ochronie danych osobowych miały także stowarzyszenia. Tytułem przykładu wskazać można, że prezes zarządu jednego ze stowarzyszeń „przyszpitalnych” działających na obszarze Rzeczypospolitej Polskiej, wobec odmowy udzielenia mu przez dyrektora szpitala informacji o imionach, nazwiskach oraz miejscowości zamieszkania darczyńców, którzy zdecydowali się na przekazanie stowarzyszeniu 1% ze swego podatku dochodowego za rok 2007, uzupełnionych o nazwę i siedzibę Urzędu Skarbowego, zwrócił się z zapytaniem, czy w istocie informacje w powyższym zakresie stanowić mogą dane osobowe podlegające ochronie wynikającej z przepisów ustawy o ochronie danych osobowych.⁴⁰⁶

Generalny Inspektor wskazał, iż wnioskowany zakres danych pozwala na zidentyfikowanie osoby bez ponoszenia nadmiernych kosztów, czasu czy działań i tym samym można będzie je uznać za dane osobowe. Zakwalifikowanie określonych informacji do katalogu danych osobowych nie oznacza absolutnego zakazu ich przetwarzania, a dyrektor szpitala będzie uprawniony do przekazania stowarzyszeniu informacji o darczyńcach, o ile wyrażą oni na to zgodę.⁴⁰⁷

W okresie objętym sprawozdaniem, Generalny Inspektor ustosunkował się ponadto do wątpliwości związanych z legalnością przekazania przez zarząd spółdzielni mieszkaniowej jej radzie nadzorczej oraz radom osiedla, informacji o wynagrodzeniu kierowników osiedli i ich zastępców działających na terenie tejże spółdzielni.⁴⁰⁸ Działalność spółdzielni mieszkaniowych regulują przepisy ustawy z dnia 16 września 1982 r. Prawo spółdzielcze⁴⁰⁹ oraz przepisy ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych,⁴¹⁰ a także statut i sporządzone na jego podstawie regulaminy oraz uchwały podejmowane przez organy spółdzielni mieszkaniowych.⁴¹¹ Wskazane przepisy prawa nie stanowią podstawy prawnej dla przekazania powyższych informacji. Analiza statutu doprowadziła do podobnych wniosków. Mimo iż statut przewiduje możliwość powołania kierowników osiedli i ich zastępców, a także przesądza, że zarząd jest ich pracodawcą w rozumieniu Kodeksu pracy,⁴¹² to nie wskazuje jednak na jakąkolwiek konieczność posiadania przez radę nadzorczą i jej komisję oraz radę osiedla i jej komisję, szczegółowych informacji na temat wynagrodzenia kierowników osiedli i ich zastępców. Statut przedmiotowej spółdzielni mieszkaniowej stanowi jedynie, iż do zakresu działania rady nadzorczej należy uchwalanie planów gospodarczych i programów działalności społecznej, oświatowej, kulturalnej i sportowo – rekreacyjnej spółdzielni w oparciu o plany osiedli uchwalone przez rady osiedli oraz

⁴⁰³ Zgodnie z tym przepisem, administrator danych przetwarzający dane powinien dolożyć należytej 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.

⁴⁰⁴ Art. 36 ustawy o ochronie danych osobowych oraz przepisy 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 osobowych.

⁴⁰⁵ DOLiS-035-344/08.

⁴⁰⁶ GI-DOLiS-024/299/07/08.

⁴⁰⁷ Art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

⁴⁰⁸ DOLiS-035-781/08.

⁴⁰⁹ Dz. U. z 2003 r. Nr 188, poz. 1848 z późn. zm.

⁴¹⁰ Dz. U. z 2003 r. Nr 119, poz. 1116 z późn. zm.

⁴¹¹ Art. 1 § 1 Prawa spółdzielczego stanowi, iż spółdzielnia jest dobrowolnym zrzeszeniem nieograniczonej liczby osób, o zmiennym składzie osobowym i zmiennym funduszu udziałowym, które w interesie swoich członków prowadzi wspólną działalność gospodarczą. Stosownie do art. 3 tej ustawy, majątek spółdzielni jest prywatną własnością jej członków. W myśl art. 1 ust. 3 ustawy o spółdzielniach mieszkaniowych, spółdzielnia ma obowiązek zarządzania nieruchomościami stanowiącymi jej mienie lub nabyte na podstawie ustawy mienie jej członków. Zgodnie z art. 48 § 1 Prawa spółdzielczego to zarząd kieruje działalnością spółdzielni oraz reprezentuje ją na zewnątrz. Członków zarządu, w tym prezesa i jego zastępców, wybiera i odwołuje, stosownie do postanowień statutu, rada lub walne zgromadzenie.

⁴¹² § 84 pkt 3 ppkt 14 statutu.

uchwalanie planów kosztów administracji ogólnej, po uprzednim zasięgnięciu opinii rad osiedli.⁴¹³ Do wykonywania powyższych zadań nie jest konieczna szczegółowa wiedza na temat wynagrodzenia – a zwłaszcza jego poszczególnych składników – otrzymywanego przez kierowników osiedli i ich zastępców ani innych pracowników spółdzielni. Wobec tego, iż uregulowania prawne nie przewidują obowiązku przekazywania tego typu informacji przez zarząd innym organom spółdzielni, Generalny Inspektor poinformował spółdzielnię, iż w przypadku dostępu do informacji o wynagrodzeniu kierowników osiedli i ich zastępców, członków rady nadzorczej i jej komisji oraz rady osiedla i jej komisji, obowiązują takie same zasady, jak każdego innego członka spółdzielni mieszkaniowej.

6.2. Działalność informacyjna

W celu zapewnienia powszechnego dostępu do informacji, Generalny Inspektor Ochrony Danych Osobowych, 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 aktualizował informacje zawarte na stronie internetowej (www.giodo.gov.pl) będącej jednocześnie Biuletynem Informacji Publicznej. Duży krąg odbiorców informacji zapewniły również publikacje książkowe, szkolenia oraz konferencje o charakterze naukowym organizowane przez GIODO. W 2008 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 2008 r. upubliczniane i upowszechniane przez GIODO materiały obejmowały m.in. interpretację przepisów ustawy o ochronie danych osobowych, wystąpienia Generalnego Inspektora do podmiotów, którym sygnalizowano nieprawidłowości dotyczące stosowania przepisów o ochronie danych osobowych, a także odpowiedzi na kierowane do Biura pytania. Przekazywane informacje dotyczyły również rozstrzygnięć podejmowanych w indywidualnych sprawach oraz działalności GIODO zarówno na arenie międzynarodowej, jak i krajowej.

6.2.1 Współpraca ze środkami masowego przekazu

Stale kontakty z mediami

W 2008 r. Generalny Inspektor kontynuował stałą współpracę z prasą o zasięgu ogólnopolskim, zwłaszcza z „Rzeczpospolitą”, „Gazetą Prawną”, „Gazetą Samorządu i Administracji” i „Tina”, w których cyklicznie ukazują się rubryki poświęcone ochronie danych osobowych. Nawiązał także stałe kontakty z gazetą „Twoje Imperium” oraz miesięcznikiem „Bezpieczeństwo w Szkole”. Na łamach wymienionych tytułów prasowych GIODO publikował swoje opinie i wystąpienia wydawane na podstawie rozstrzygnięć konkretnych spraw oraz wszelkie inne informacje dotyczące ochrony danych osobowych. W roku sprawozdawczym 2008 ukazało się łącznie 85 takich artykułów.

Nowatorskim przedsięwzięciem było dokonywanie przez GIODO nagrań audycji radiowych w formacie mp3, które następnie w formie pisemnej lub jako nagrania radiowe publikowane były w Internecie na stronach www.giodo.gov.pl w cyklu pt. „Chroń swoje dane osobowe!”. Stamtąd wszyscy nadawcy mogli je bezpłatnie pobrać i emitować na swojej antenie. Taką współpracę z wykorzystaniem gotowych nagrań w 2008 r. zadeklarowało i prowadziło 8 lokalnych rozgłośni radiowych.

Na początku 2008 r. w fazę realizacji weszła nowa, dodatkowa forma współpracy z „Gazetą Samorządu i Administracji” [„GSiA”] polegająca na kolportowaniu razem z gazetą 6 broszur informacyjnych GIODO z serii „ABC ochrony danych osobowych...”. Od stycznia 2008 r. były one dołączane do każdego kolejnego numeru pisma. Dzięki temu do czytelników „GSiA” trafiły następujące broszury informacyjne: „ABC ochrony danych osobowych”, „ABC wybranych zagadnień z ustawy o ochronie danych osobowych”, „ABC rejestracji zbiorów danych osobowych”, „ABC zasad kontroli przetwarzania danych osobowych”,

⁴¹³ § 77 statutu.

„ABC zasad przekazywania danych osobowych do państw trzecich” i „ABC zasad bezpieczeństwa przetwarzania danych osobowych przy użyciu systemów informatycznych”. Ponadto współpraca ta była wsparta serią reklam promocyjnych. Dodatkowo do pierwszej broszury dołączona została wydana przez GODO ulotka informacyjna związana z przystąpieniem Polski do strefy Schengen.

Na okres wrzesień – grudzień 2008 r. Generalny Inspektor Ochrony Danych Osobowych zawarł z „Gazetą Samorządu i Administracji” umowę o współpracy, na mocy której w każdym numerze pisma publikowana była nie tylko jedna odpowiedź na konkretne pytanie dotyczące ochrony danych osobowych w sektorze administracji samorządowej, ale także reklama (o wymiarach 170x110 mm) poświęcona działaniom podejmowanym przez GODO.

Odpowiedzi na indywidualne pytania dziennikarzy

Stałą formą kontaktów Generalnego Inspektora z dziennikarzami było udzielanie odpowiedzi na pytania dotyczące ochrony danych osobowych. W 2008 r. GODO udzielił – pisemnie lub telefonicznie – około 250 takich odpowiedzi. Wśród problemów, z którymi najczęściej zgłaszali się przedstawiciele mediów, były m.in.:

- funkcjonowanie portali społecznościowych,
- zakres danych pozyskiwanych przez przewoźników, zwłaszcza na potrzeby wystawienia biletów elektronicznych lub internetowej rezerwacji biletów,
- wywieszanie w sklepach zdjęć złodziei,
- kradzież tożsamości i jej konsekwencje,
- ochrona danych osobowych na potrzeby zatrudnienia,
- odpowiedzialność karna za wyciek danych osobowych,
- dopuszczalność pozyskiwania danych biometrycznych,
- pozyskiwanie informacji publicznych,
- zabezpieczanie danych osobowych,
- jawność danych osób fizycznych będących przedsiębiorcami,
- upublicznianie danych osobowych przez jednostki samorządu terytorialnego.

Wywiady i wystąpienia

Stałą formą współpracy GODO z mediami jest udzielanie wywiadów i udział w programach radiowych i telewizyjnych. Dzięki aktywnej polityce informacyjnej Generalny Inspektor Ochrony Danych Osobowych udzielił w 2008 r. blisko 100 takich wywiadów. Ich tematyka dotyczyła:

- ochrony danych osobowych w dobie rozwoju nowoczesnych technologii,
- odpowiedzialności administratorów danych za właściwe przetwarzanie danych osobowych, w tym ich zabezpieczanie,
- zakresu danych osobowych pozyskiwanych na potrzeby zatrudnienia,
- podstawowych zasad ochrony danych osobowych w sektorze bankowym oraz w sektorze medycznym,
- dopuszczalności stosowania wideomonitoringu (wideonadзору).

Inne formy współpracy z mediami

Wśród innych form współpracy z mediami na odnotowanie zasługuje uczestnictwo GODO w czacie internetowym zorganizowanym we wrześniu 2008 r. przez redakcję „Gazety Bankowej” w portalu Wirtualna Polska. Mimo iż czat poświęcony był ochronie danych osobowych klientów instytucji finansowych, internauci pytali także o inne zagadnienia dotyczące ochrony danych osobowych. Relacja z czatu w pełnej wersji ukazała się na portalu wp.pl, a jej fragmenty - na łamach „Gazety Bankowej”.

GIODO 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. Odbýwał także dyżury telefoniczne w stacjach radiowych i telewizyjnych oraz w redakcjach gazet.

Konferencje prasowe

W związku z nagłośnieniem w mediach ważnych wydarzeń lub koniecznością zajęcia stanowiska w określonych sprawach, GIODO zorganizował w 2008 r. 5 konferencji prasowych.

- 16 stycznia 2008 r. w siedzibie Biura GIODO odbyła się konferencja prasowa, pt. „Czy nasze dane osobowe są bezpieczne na portalu Nasza-klasa.pl?” Na spotkaniu z dziennikarzami GIODO poinformował o planowanym rozpoczęciu czynności kontrolnych w portalu Nasza-klasa.pl pod kątem zgodności przetwarzania danych z przepisami o ochronie danych osobowych, ze szczególnym uwzględnieniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych,
- 28 stycznia 2008 r. miała miejsce konferencja prasowa poświęcona podpisaniu porozumienia między Generalnym Inspektorem Ochrony Danych Osobowych a Stowarzyszeniem Marketingu Bezpośredniego,
- 4 lutego 2008 r. w siedzibie Biura GIODO odbyła się konferencja prasowa Generalnego Inspektora, pt. „Co się stało z Naszą-klasą?”, w której uczestniczył także Prezes spółki Nasza-klasa.pl - Maciej Popowicz. GIODO przedstawił wyniki kontroli przeprowadzonej w tej spółce, wskazując, że portal spełnia wymogi dotyczące bezpieczeństwa danych osobowych, jednak z pewnymi zastrzeżeniami - konieczne jest zastosowanie dodatkowych środków bezpieczeństwa podczas logowania użytkowników na portalu Nasza-klasa.pl oraz wdrożenie pisemnych procedur rozpatrywania skarg.
- 12 listopada 2008 r. - zaraz po doniesieniach medialnych, iż AWB skanuje przesyłki pocztowe - GIODO niezwłocznie zorganizował konferencję prasową, podczas której zapowiedział przeprowadzenie kontroli w spółce Poczta Polska,
- 2 grudnia 2008 r. odbyła się konferencja prasowa związana ze współorganizowanym przez GIODO i Kolegium Prawa Akademii Leona Koźmińskiego seminarium naukowym, pt. „Granice ochrony danych osobowych w stosunkach pracy”.

Rezultatem konferencji prasowych były liczne materiały informacyjne i wystąpienia GIODO w audycjach radiowych i telewizyjnych.

Akcje informacyjno – promocyjne

Szczególne wydarzenia czy informacje związane z tematyką ochrony danych osobowych, Generalny Inspektor nagłaśnia, organizując specjalne akcje informacyjno - promocyjne. W 2008 r. 6 zagadnień zostało rozpropagowanych w ten właśnie sposób:

- styczeń to miesiąc, w którym GIODO popularyzuje informację o obchodzonym 28 stycznia europejskim Dniu Ochrony Danych Osobowych. To święto stanowi okazję do zwrócenia uwagi społeczeństwa na potrzebę ochrony danych osobowych. W analizowanym roku 2008 towarzyszyły mu liczne wydarzenia, jak Dzień Otwarty w Biurze GIODO, podpisanie Porozumienia pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych a Stowarzyszeniem Marketingu Bezpośredniego w sprawie współpracy na rzecz poprawy poziomu ochrony danych osobowych oraz zapewnienia prawa do prywatności obywatelom naszego kraju, seminarium „Śniadanie naukowe” w Wyższej Szkole Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego poświęcone ochronie danych osobowych w strefie Schengen, spotkanie GIODO z eurodeputowanymi w Brukseli i uroczystości w siedzibie Stałego Przedstawicielstwa Rzeczypospolitej Polskiej przy Unii Europejskiej.
- W kwietniu 2008 r. zorganizowana została akcja medialna z okazji 10. rocznicy wejścia w życie ustawy o ochronie danych osobowych. Generalny Inspektor zainicjował obchody 10. rocznicy wejścia w życie ustawy o ochronie danych osobowych na antenie Polskiego Radia, biorąc udział w trzygodzinnej audycji radiowej, pt. „Cztery pory roku”, poświęconej w całości prawu do prywatności i ochronie danych osobowych. W czasie audycji, zarówno w studiu Polskiego Radia, jak i w Biurze

GIODO uruchomiony został telefon dla słuchaczy. Dodatkową atrakcją był konkurs z nagrodami poświęcony zagadnieniom związanym ze stosowaniem przepisów ustawy o ochronie danych osobowych oraz Systemowi Informacyjnemu Schengen.

- W lipcu 2008 r. specjalną akcją informacyjną zorganizowano w związku z wyciekiem z Banku Pekao S.A. danych osobowych kandydatów do pracy. Polegała ona m.in. na rozpowszechnieniu w mediach apelu GIODO skierowanego do wszystkich, którzy weszli w posiadanie tych danych o ich niewykorzystywanie, nierozpowszechnianie oraz usuwanie.
- W sierpniu 2008 r. w związku z otrzymaniem najnowszych badań Eurobarometru, z których wynikało, że Polska, z 43-procentowym wynikiem, znalazła się na pierwszym miejscu wśród państw członkowskich Unii Europejskiej, deklarując najwyższą świadomość praw związanych z danymi osobowymi, GIODO zainicjował działania medialne mające na celu rozpowszechnienie tej informacji. Dzięki temu materiały na ten temat opublikowane zostały w mediach ogólnopolskich i regionalnych.
- W październiku 2008 r. - jak co roku - miała miejsce akcja edukacyjna „Tydzień Ochrony Tożsamości” organizowana przez Agencję Fleishman Hillard we współpracy z GIODO. W dniu 21 października 2008 r. w trakcie odbywającej się w siedzibie PAP specjalnej konferencji prasowej, ogłoszone zostały wyniki badań TNS OBOP dotyczące ochrony danych osobowych w Polsce. Tematyką świadomości ochrony danych osobowych oraz kwestią kradzieży tożsamości zainteresowały się liczne media, a GIODO był gościem wielu programów radiowych i telewizyjnych.
- Październik 2008 był miesiącem, w którym uruchomiony został nowy portal edukacyjny GIODO (tzw. platforma eduGIODO). W związku z tym zainicjowana została akcja informacyjna mająca na celu prezentację portalu i jego funkcjonalności.

6.2.2 Publikacje

W minionym roku sprawozdawczym 2008, Generalny Inspektor Ochrony Danych Osobowych rozpoczął - we współpracy z Wydawnictwem Sejmowym - druk serii broszur informacyjnych na temat ochrony danych osobowych. Są one przekazywane parlamentarzystom, dziennikarzom, eurodeputowanym oraz osobom zainteresowanym, z którymi GIODO współpracuje i dla których przeprowadza szkolenia. Dotychczas 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”,
- „ABC zasad kontroli przetwarzania danych osobowych”.

W drugiej połowie 2008 r. do druku skierowana została kolejna publikacja z tego cyklu, pt. „ABC przetwarzania danych osobowych w sektorze bankowym”.

W 2008 r. w Biurze GIODO podjęte zostały prace nad opracowaniem systemu identyfikacji wizualnej, dzięki któremu przekazywane informacje GIODO będą łatwiej zauważane i rozpoznawalne. Jednym z pierwszych efektów wdrażania systemu było opracowanie kolejnej broszury z serii „ABC ochrony danych osobowych...” poświęconej ochronie danych osobowych w sektorze bankowym.

6.2.3 Szkolenia, staże, wymiana pracowników

Szkolenia podmiotów zewnętrznych

W ramach działalności edukacyjnej Generalny Inspektor Ochrony Danych Osobowych organizował nieodpłatne szkolenia skierowane głównie do instytucji publicznych. Stanowiły one swego rodzaju odpowiedź na zgłaszane przez zainteresowane podmioty zapotrzebowanie na wiedzę z zakresu ochrony danych osobowych.

Na szkoleniach przeprowadzonych w 2008 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-GIODO,
- zasady funkcjonowania przepisów o ochronie danych osobowych w odniesieniu do innych regulacji prawnych, jak prawo do prywatności czy prawo do informacji,
- zasady funkcjonowania w Polsce Systemu Informacyjnego Schengen i Systemu Informacji Wizowej,
- nowe źródło informacji o ochronie danych osobowych: portal informacyjny – szkoleniowy eduGIODO.

Generalny Inspektor Ochrony Danych Osobowych przeprowadził szkolenia m.in.: sędziów i pracowników Sądu Rejonowego w Gdyni, sądów okręgowych i apelacyjnych z terenu całej Polski, radców prawnych, komorników sądowych, marszałków województw oraz przedstawicieli samorządu terytorialnego województwa mazowieckiego, małopolskiego, wielkopolskiego, świętokrzyskiego i warmińsko-mazurskiego, Urzędu Komisji Nadzoru Finansowego, Krajowej Izby Doradców Podatkowych, pracowników Poczty Polskiej, biur senatorskich, Fundacji Rozwoju Systemu Edukacji, Urzędu Zamówień Publicznych, Funduszu Gwarantowanych Świadczeń Pracowniczych, Komendy Głównej Policji, Komendy Głównej Straży Granicznej, słuchaczy szkół policyjnych z Piły, Szczytna, Słupska, Katowic i Legionowa, Kancelarii Prezydenta RP, Kancelarii Prezesa Rady Ministrów, Kancelarii Senatu, a także pracowników Ambasady RP w Brukseli, polskich eurodeputowanych do parlamentu w Brukseli oraz pracowników ich biur poselskich. Wśród podmiotów szkolonych przez Generalnego Inspektora Ochrony Danych Osobowych znaleźli się też pracownicy Ministerstwa Spraw Zagranicznych, Ministerstwa Infrastruktury, Ministerstwa Edukacji Narodowej, Ministerstwa Zdrowia i Ministerstwa Finansów. W 2008 r. odbyły się 63 takie szkolenia (zob. załącznik nr 6).

Szkolenia wewnętrzne pracowników Biura GIODO

W roku 2008 w Biurze Generalnego Inspektora Ochrony Danych Osobowych organizowane były szkolenia wewnętrzne dla 29 nowo zatrudnionych pracowników. Tematyka szkoleń obejmowała następujące zagadnienia: „Geneza ochrony danych osobowych”, „Status GIODO na tle organizacji i funkcjonowania organów władzy publicznej”, „Podstawy prawne SIS, CIS i Europolu”, „Europejskie standardy ochrony danych osobowych”, „Przekazywanie danych do państw trzecich”, „Podstawowe zasady ochrony danych osobowych”, „Prawa osoby, której dane dotyczą”, „Organizacyjne i techniczne środki zabezpieczania danych”, „Rejestracja zbiorów danych osobowych”. W szkoleniu przeprowadzonym w kwietniu 2008 r. udział brali nie tylko nowo zatrudnieni pracownicy, ale także 4 stażyści z Komendy Głównej Policji.

Natomiast w ramach szkolenia ustawicznego, którego celem jest podnoszenie kwalifikacji, pracownicy Biura GIODO uczestniczyli w szkoleniach z zakresu obsługi różnych programów komputerowych.

W związku z przystąpieniem Polski do strefy Schengen, Generalny Inspektor Ochrony Danych Osobowych opracował „Program szkoleń pracowników Biura GIODO w zakresie wdrożenia i funkcjonowania w Polsce Systemu Informacyjnego Schengen i Systemu Informacji Wizowej oraz roli w tym zakresie Generalnego Inspektora Ochrony Danych Osobowych”. Szkolenie odbywało się w trzech modułach. Pierwszy moduł miał charakter ogólny i skierowany był do wszystkich pracowników merytorycznych Biura GIODO. Celem szkolenia było zapoznanie pracowników z obowiązującymi regulacjami krajowymi i wspólnotowymi w zakresie przetwarzania danych osobowych w tych systemach i wynikającymi z nich uprawnieniami Generalnego Inspektora. Drugi moduł szkolenia adresowany był do inspektorów Departamentu Inspekcji i Departamentu Informatyki, w celu zapoznania ich z metodologią przeprowadzania czynności kontrolnych w odniesieniu do systemów informatycznych oraz kontroli na granicach po wejściu Polski do strefy Schengen. Trzeci moduł obejmował program szkolenia dla pracowników Departamentu Orzecznictwa, Legislacji i Skarg w zakresie podstaw prawnych wniesienia skargi w świetle regulacji ustawy z dnia 24 sierpnia 2007 r. o udziale RP w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej oraz procedury jej rozpatrywania.

W Biurze Generalnego Inspektora Ochrony Danych Osobowych w lipcu i wrześniu 2008 r. organizowane były też **praktyki** dla studentów wydziału prawa i wydziału administracji oraz dla aplikanta radcowskiego z Okręgowej Izby Radców Prawnych. Praktykanci mieli okazję zapoznać się 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 kadrę kierowniczą oraz pracowników Biura - szkoleniach organizowanych cyklicznie dla wszystkich nowo zatrudnionych pracowników.

Udział pracowników Biura Generalnego Inspektora Ochrony Danych Osobowych w szkoleniach organizowanych przez jednostki zewnętrzne

Pracownicy Biura GIODO korzystali z wielu szkoleń informatycznych, których celem było podnoszenie ich kompetencji w zakresie zarządzania i administrowania posiadaną infrastrukturą informatyczną. Do najważniejszych należały szkolenia organizowane nieodpłatnie przez Rządowe Centrum Reagowania na Incydenty Komputerowe CERT.GOV.PL działające w ramach Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego [ABW]. W roku 2008 ABW zorganizowała 8 takich szkoleń.

W ramach współpracy GIODO z KGP, administratorem systemu SIS i VIS, pracownicy Biura GIODO uczestniczyli w szkoleniu zorganizowanym przez Krajowe Centrum Informacji Kryminalnej i Biuro Sirene Komendy Głównej Policji. Celem szkolenia było przedstawienie zasad funkcjonowania Systemu Informacyjnego Schengen i Systemu Informacji Wizowej.

Projekt wymiany realizowany w ramach Programu Leonardo da Vinci

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

Dzięki wymianie pracowników zorganizowanej w ramach Programu uczestnicy wyjazdów 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 podniesienia umiejętności językowych.

6.2.4 Konkursy

II edycja konkursu plastycznego „Ochrona prywatności w świecie bez granic - Schengen”

W konkursie rysunkowym dla dzieci w wieku 7-13 lat, zorganizowanym przez Generalnego Inspektora z okazji Dnia Ochrony Danych Osobowych, swoje prace przedstawiło 13 uczniów z 4 warszawskich szkół:

- | | |
|--|-------------|
| 1. Szkoły Podstawowej Nr 255, ul. Kamionkowska 36/44 | - 4 uczniów |
| 2. Szkoły Podstawowej Nr 16, ul. Wilczy Dół 4 | - 7 uczniów |
| 3. Gimnazjum Nr 53 z Oddziałami Dwujęzycznymi im. Stefanii Sempołowskiej w Warszawie, ul. Ks. J. Popieluszki 5 | - 1 uczeń |
| 4. Szkoły Podstawowej im. I Batalionu Saperów Kościuszkowskich w Izabelinie, ul. Szkolna 1 | - 1 uczeń |

II edycja konkursu na najlepszą pracę magisterską i licencjacką

W czerwcu 2008 r. Generalny Inspektor Ochrony Danych Osobowych ogłosił II edycję konkursu na najlepszą pracę magisterską/licencjacką dotyczącą problematyki ochrony danych osobowych. Konkurs organizowany we współpracy z Europejskim Stowarzyszeniem Studentów Prawa – ELSA Poland, przeznaczony był dla studentów studiów dziennych, wieczorowych i zaocznych wszystkich wydziałów i kierunków. Celem konkursu było popularyzowanie wiedzy o ochronie danych osobowych, zwiększenie zainteresowania absolwentów szkół wyższych problematyką ochrony danych osobowych oraz wyróżnienie utalentowanych autorów nadesłanych prac, aby zachęcić ich do zgłębiania wiedzy z zakresu tej tematyki.

Autorzy i promotorzy mogli zgłaszać do Konkursu prace magisterskie i licencjackie obronione w latach 2004/2005, 2005/2006, 2006/2007 i 2007/2008. Nagrodą dla autora najlepszej pracy była opłata studiów podyplomowych „Ochrona danych osobowych” w Akademii Leona Koźmińskiego, zaś dla autorów wyróżnionych prac – miesięczny staż w kancelarii Wierzbowski Eversheds w Warszawie.

6.2.5 Konferencje i seminaria

W roku sprawozdawczym 2008, Generalny Inspektor Ochrony Danych Osobowych zarówno organizował konferencje i seminaria, jak i brał aktywny udział w konferencjach zorganizowanych przez inne podmioty.

1. II Dzień Ochrony Danych Osobowych – 28 stycznia 2008 r.

W dniu 28 stycznia 2008 r. Generalny Inspektor Ochrony Danych Osobowych już po raz drugi obchodził Dzień 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 miały miejsce następujące wydarzenia:

Dzień Otwarty w Biurze GIODO - umożliwił wszystkim chętnym zapoznanie się z tematyką ochrony danych osobowych oraz działalnością Biura. Filmy, wykłady, materiały informacyjne, porady i informacje uzyskane od pracowników Biura GIODO, przybliżyły uczestnikom Dnia Otwartego kwestie związane z działalnością GIODO. Przy 5 stolikach informacyjnych, przedstawiciele poszczególnych departamentów udzielali porad prawnych. Wszyscy przybyli na Dzień Otwarty otrzymali broszury z cyklu „ABC ochrony danych osobowych” oraz ulotki o działalności Biura i strefie Schengen. Można było również zapoznać się z najciekawszymi artykułami prasowymi dotyczącymi ochrony danych.

Dla najmłodszych przygotowany został konkurs rysunkowy pt.: „Ochrona prywatności w świecie bez granic – Schengen”, a dla dorosłych konkurs wiedzy o zagrożeniach w Internecie i ochronie danych osobowych. Wszyscy uczestnicy konkursu rysunkowego (tj. 13 uczniów) otrzymali upominki od Generalnego Inspektora Ochrony Danych Osobowych. Zaś trzem najbardziej aktywnym słuchaczom wykładu „Zagrożenia w Internecie” przyznano nagrody książkowe. Dyrektorzy Departamentów - Inspekcji oraz Orzecznictwa, Legislacji i Skarg przeprowadzili szkolenie uczestników obchodów Dnia Ochrony Danych Osobowych. Dzień 28 stycznia 2008 r. był dniem, w którym można było również zwiedzić Biuro GODO.

Seminarium „Śniadanie naukowe” w siedzibie Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego – poświęcone roli GODO w związku z przystąpieniem Polski w dniu 21 grudnia 2007 r. do strefy Schengen. Organizatorami śniadania byli Generalny Inspektor Ochrony Danych Osobowych i Rektor Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego. W śniadaniu naukowym udział wzięli przedstawiciele środowiska naukowego, Komendy Głównej Policji, Straży Granicznej, administracji publicznej oraz przedstawiciele instytucji unijnych w Polsce. Referaty wygłosili: prof. zw. dr hab. Jan Barcz, kierownik Katedry Prawa Międzynarodowego i Prawa Europejskiego WSPiZ im. L. Koźmińskiego, Michał Serzycki, Generalny Inspektor Ochrony Danych Osobowych oraz prof. dr hab. Joanna Sieńczyło – Chlabicz, opiekun naukowy studiów podyplomowych „Ochrona Danych Osobowych”.

Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z posłami do Parlamentu Europejskiego oraz pracownikami ich biur poselskich (Bruksela, 30 stycznia 2007 r.) - odbyło się ono w siedzibie Parlamentu Europejskiego. Wystąpienie Generalnego Inspektora Ochrony Danych Osobowych dotyczyło roli polskiego organu ochrony danych w Systemie Informacyjnym Schengen, oraz aspektów związanych ze stworzeniem europejskiego systemu zbierania danych osobowych pasażerów linii lotniczych zawartych w systemach rezerwacyjnych.

Uroczystości w Stałym Przedstawicielstwie Rzeczypospolitej Polskiej przy Unii Europejskiej w Brukseli, zorganizowane przez Generalnego Inspektora Ochrony Danych Osobowych i Ambasadora Jana Tombińskiego, Stałego Przedstawiciela RP przy Unii Europejskiej. Uroczystości poświęcone były ochronie danych osobowych w strefie Schengen, problematyce dotyczącej stworzenia europejskiego systemu zbierania danych osobowych pasażerów linii lotniczych zawartych w systemach rezerwacyjnych, a także pracom nad decyzją ramową w sprawie ochrony danych osobowych w III filarze UE. Referaty wygłosili: Francesco Pizzetti, Przewodniczący Grupy Roboczej do spraw Policji i Wymiaru Sprawiedliwości i Joaquin Bayo Delgado, zastępca Europejskiego Inspektora Ochrony Danych. Gośćmi spotkania byli polscy eurodeputowani, rzecznicy ochrony danych osobowych z państw Europy Środkowo-Wschodniej i ich pracownicy, a także przedstawiciele polskich instytucji mających siedzibę w Brukseli.

2. Seminarium „Jakość danych w systemach informatycznych zakładów ubezpieczeń” zorganizowane przez Polską Izbę Ubezpieczeń (Warszawa, 2 kwietnia 2008 r.).

Problematyka zarządzania jakością danych była motywem przewodnim wspomnianego seminarium, w którym udział wzięli głównie pracownicy zakładów ubezpieczeń odpowiedzialni za zarządzanie informacją biznesową oraz procesami wymiany informacji w ramach sektora ubezpieczeniowego, ze szczególnym uwzględnieniem procesów obsługi świadczeń, przeciwdziałania przestępczości ubezpieczeniowej, marketingu i zarządzania sprzedażą. Na seminarium dyskutowane były również zagadnienia związane z zarządzaniem jakością i bezpieczeństwem informacji w systemach informatycznych w kontekście przepisów o ochronie danych osobowych, prawnymi podstawami wymagań odnoszących się do jakości i bezpieczeństwa danych, analizą ryzyka w związku z tworzeniem odpowiedniej polityki bezpieczeństwa danych, zarządzaniem bezpieczeństwem w skali całej instytucji, w zakresie systemów informatycznych, bądź danego systemu informatycznego. Omówiona też została instrukcja zarządzania systemem informatycznym.

3. Konwent Przewodniczących i Radców Prawnych Okręgowych Izb Lekarskich (Mierzęcin, 9 maja 2008 r.).

Wiodącym tematem Konwentu był zakres i sposób udostępniania danych osobowych z rejestrów izb lekarskich. Dyskutowano m.in. kiedy, komu i w jakim zakresie izba lekarska ma obowiązek przekazywać dane osobowe z prowadzonych rejestrów

oraz kiedy wymagana jest dodatkowa zgoda osoby, której dane dotyczą, na jakich zasadach można udostępniać dane rejestrowe podmiotom do celów komercyjnych oraz w jakich sytuacjach można odmówić przekazywania danych osobowych. Zajęto się również kwestią tworzenia rejestrów z danymi medycznymi w gabinetach lekarskich, zasad ich zabezpieczania, przechowywania oraz uprawnień Generalnego Inspektora Ochrony Danych Osobowych w zakresie kontroli tych rejestrów. Generalny Inspektor zaproponował współpracę z izbami lekarskimi nad przygotowaniem procedur i zasad związanych z tworzeniem rejestrów medycznych i sposobami udostępniania z nich danych osobowych. Omówiono także wymaganą przepisami dokumentację oraz zalecane procedury wymagane przy przetwarzaniu danych na poziomie okręgowych izb lekarskich.

4. Warsztaty w ramach programu TAIEX „Przewidywane zmiany w prawodawstwie Unii Europejskiej w kontekście wdrażania *acquis communautaire* (dorobek prawny wspólnot europejskich i UE) w obszarze ochrony danych osobowych” (Warszawa, 15-16 maja 2008 r.)

Warsztaty organizowane przez Generalnego Inspektora Ochrony Danych Osobowych i Komisję Europejską w ramach programu TAIEX adresowane były w szczególności do przedstawicieli środowisk sędziów i prokuratorów. Prowadzone były przez polskich i unijnych ekspertów zajmujących się problematyką ochrony danych.

Program spotkań koncentrował się na następujących zagadnieniach:

- a) podstawy prawne ochrony danych osobowych w Unii Europejskiej,
- b) podstawowe zasady ochrony danych w kontekście prawa UE,
- c) przewidywane zmiany w prawie unijnym,
- d) ochrona danych osobowych w orzecznictwie Europejskiego Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka,
- e) organy wymiaru sprawiedliwości i ochrona danych - rola sędziów i prokuratorów, ochrona danych osobowych w orzecznictwie sądów administracyjnych, doświadczenia na poziomie krajowym,
- f) ochrona danych osobowych w praktyce organów wymiaru sprawiedliwości w świetle postępowań i kontroli prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych.

5. IX Konferencja Okrągłego Stołu „Polska w drodze do społeczeństwa informacyjnego; Człowiek wobec wyzwań powstającego Społeczeństwa Informacyjnego” zorganizowana przez Stowarzyszenie Elektryków Polskich, objęta honorowym patronatem Marszałka Sejmu Bronisława Komorowskiego (Warszawa, 16 maja 2008 r.).

Organizowane w Polsce co roku, w maju, obchody Światowego Dnia Telekomunikacji ustanowione na mocy rezolucji Zgromadzenia Ogólnego ONZ z 2006 r. poświęcone były szeroko rozumianej tematyce telekomunikacji i jej wpływu na rozwój i życie codzienne społeczeństw na całym świecie.

6. Konferencja „Biznes a Ochrona Danych Osobowych” zorganizowana przez Wyższą Szkołę Biznesu National-Louis University w Nowym Sączu (Nowy Sącz, 20 maja 2008 r.).

Podczas konferencji Generalny Inspektor Ochrony Danych Osobowych i Jego Magnificencja Rektor Wyższej Szkoły Biznesu National-Louis University podpisali porozumienie i umowę o współpracy w zakresie ochrony prywatności i danych osobowych.

7. Konferencja szkoleniowa „Ochrona Danych Osobowych” zorganizowana przez Krajową Radę Radców Prawnych (Warszawa, 5 czerwca 2008 r.).

8. XXII Kongres Związku Adwokatów Europejskich pt. „Prawo prywatności: ochrona praw jednostki a globalna ekonomia” (Warszawa, 6 czerwca 2008 r.).

Generalny Inspektor Ochrony Danych Osobowych w swoim wystąpieniu podkreślił rolę organów ochrony danych osobowych we współczesnym świecie, zwrócił uwagę na aktualne zagrożenia dla prywatności jednostek oraz zaapelował do zgromadzonych adwokatów o działania wspierające i chroniące prywatność i dane osobowe w ich codziennej pracy.

9. Konferencja „Holistyczne zarządzanie danymi osobowymi II” zorganizowana przez Global Information Security Sp. z o.o. (Mikołajki, 6 czerwca 2008 r.). Na spotkaniu przedstawiona została prezentacja dotycząca sposobu korzystania z platformy e-GIODO, a także planowanych w najbliższym czasie zmian w zakresie umożliwienia wysyłki wniosków rejestracyjnych bez konieczności ich elektronicznego podpisywania oraz planowanych zmian wzoru formularza rejestrowego.

10. Konferencja „Bezpieczeństwo w sieciach handlowych” zorganizowana przez Grupę KONSALNET, Puls Biznesu oraz Polską Organizację Handlu i Dystrybucji (Warszawa, 26 września 2008 r.).

Celem konferencji było omówienie formalnoprawnych aspektów współpracy i wymiany danych oraz informacji pomiędzy sieciami handlowymi, celem zapewnienia bezpieczeństwa biznesu na terenie galerii i parków handlowych w zakresie eliminacji nadużyć, wykroczeń i przestępstw.

11. XII konferencja „SECURE 2008 – bezpieczeństwo teleinformatyczne” zorganizowana przez NASK, CERT Polska oraz ENISA (Warszawa, 2 października 2008 r.).

SECURE to cykliczna konferencja poświęcona bezpieczeństwu sieci i systemów ICT. Podczas konferencji SECURE podejmowane są aktualne kwestie związane z zagrożeniami bezpieczeństwa teleinformatycznego. Na XII konferencji SECURE 2008 Generalny Inspektor Ochrony Danych Osobowych odniósł się do kwestii zagrożeń prywatności i kradzieży tożsamości w kontekście funkcjonowania portali społecznościowych.

12. Seminarium „Jakość danych w systemach informatycznych zakładów ubezpieczeń” zorganizowane przez Polską Izbę Ubezpieczeń (Warszawa, 2 października 2008 r.).

Zaproszenia do udziału w seminarium zostały skierowane do ściśle określonej grupy osób, głównie pracowników zakładów ubezpieczeń, odpowiedzialnych za zarządzanie informacją biznesową oraz procesami wymiany informacji w ramach sektora ubezpieczeniowego, ze szczególnym uwzględnieniem procesów: likwidacji szkód i obsługi świadczeń, przeciwdziałania przestępczości ubezpieczeniowej, marketingu i zarządzania sprzedażą.

13. Konferencja poświęcona „Portalowi informacyjno - szkoleniowemu eduGIODO” zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych w Centrum Partnerstwa Społecznego e-Dialog (Warszawa, 22 października 2008 r.).

Program konferencji obejmował sesję poświęconą zagadnieniom ochrony prywatności we współczesnym świecie oraz prezentację portalu informacyjno - szkoleniowego „eduGIODO”. W konferencji udział wzięło ok. 150 osób reprezentujących różne środowiska i branże.

13. Konferencja promująca „Portal informacyjno - szkoleniowy eduGIODO” zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych (Gdańsk, 31 października 2008 r.)

W konferencji, której program objął zagadnienia poruszone podczas konferencji warszawskiej, uczestniczyło ponad 80 osób.

14. V Forum ADO/ABI „Nowe zjawiska i problemy wykonania ustawowych obowiązków ochrony danych osobowych” zorganizowane przez Centrum Promocji Informatyki Sp. z o.o. (Warszawa, 6 listopada 2008 r.)

Na ww. forum prezentowane były zagadnienia dotyczące zgłoszonych projektów zmian zarówno ustawy o ochronie danych osobowych, jak i rozporządzenia wprowadzającego nowy wzór formularza zgłoszenia zbioru danych osobowych do rejestracji, a także inne zagadnienia, jak problem kompetencji w zakresie rozstrzygania spraw dotyczących spamu.

15. Okrągły Stół z Generalnym Inspektorem Ochrony Danych Osobowych i dyrektorami departamentów Biura GODO zorganizowany przez Privacy Laws & Business European Privacy Officers Network⁴¹⁴ (Warszawa, 13 listopada 2008r.).

Okrągły Stół to jedno z wielu działań edukacyjnych podejmowanych przez Generalnego Inspektora Ochrony Danych Osobowych, którego celem była wymiana doświadczeń. Zorganizowany został w ramach utworzonego przez Stewarta Dresnera - European Privacy Officers Network. Dotychczas zorganizowano już takie spotkania z przedstawicielami organów ochrony danych osobowych m.in. z Hiszpanii, Holandii i Belgii.

W czasie obrad Generalny Inspektor Ochrony Danych Osobowych omówił główne kierunki działań polskiego organu, bieżące wydarzenia, najważniejsze problemy wymagające przyjęcia określonej polityki oraz przedstawił działania podjęte w kwestii egzekwowania przestrzegania prawa o ochronie danych. Inne tematy poruszane w trakcie obrad Okrągłego Stołu, to: planowane zmiany ustawy o ochronie danych osobowych i innych aktach wykonawczych do niej, rola samoregulacji w polskim systemie ochrony danych osobowych oraz w praktyce GODO, nowe inicjatywy, przekazywanie danych do państw trzecich, badania kliniczne a ochrona danych osobowych, praktyczne aspekty wdrażania przepisów o ochronie danych osobowych, ochrona danych osobowych a zatrudnienie, stanowiska i praktyka GODO, bezpieczeństwo danych w świetle polskich przepisów o ochronie danych i w praktyce GODO, zasady i praktyczne aspekty rejestracji zbiorów danych osobowych, rejestracja zbiorów danych osobowych za pośrednictwem platformy e-GODO, podział właściwości: GODO / Urząd Komunikacji Elektronicznej (UKE) oraz GODO / Urząd Ochrony Konkurencji i Konsumentów (UOKiK).

16. Konferencja naukowa „Granice ochrony danych osobowych w stosunkach pracy” zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych oraz Katedrę Prawa Prywatnego Kolegium Prawa Akademii Leona Koźmińskiego (Warszawa, 2 grudnia 2008 r.).

Spotkanie było okazją do dyskusji na temat ochrony danych osobowych pracowników, dopuszczalności stosowania przez pracodawców nowoczesnych metod nadzoru w miejscu pracy, w tym takich zabezpieczeń, których wdrażanie wiąże się z koniecznością udostępniania danych szczególnie chronionych. Uczestnicy konferencji szukali odpowiedzi na pytania o zakres danych, jakich pracodawca może żądać od pracowników, o metody i technologie, które mogą mieć zastosowanie w celu pozyskania danych, a które z nich są bezprawne, o instrumenty ochrony pracowników przed nadmierną ingerencją pracodawców w sferę ich prywatności, a także gdzie przebiega granica między prawami pracodawców a prawami pracowników do prywatności.

6.2.6 Internet

W roku 2008 wprowadzone zostały zmiany dotyczące funkcjonowania strony podmiotowej GODO. Kontynuowano prace dostosowujące stronę internetową Biura GODO do uruchomienia Elektronicznej Skrzynki Podawczej [ESP] oraz wykonywano modyfikację systemu ESP w zakresie przyjmowania informacji za pośrednictwem opracowanych formularzy. W szczególności doprowadzono do rozszerzenia istniejącej funkcjonalności o mechanizm informowania o danych osoby podpisującej otrzymane formularze i o wydawcach oraz terminach ważności użytych do weryfikacji podpisu certyfikatów. Dokonano zmian konfiguracji subdomen na serwerze www. W 2008 r. na stronie informacyjnej GODO zmieniono sposób prezentacji menu bocznego oraz sposobu wyświetlania informacji o zamieszczanych dokumentach (metadanych). Te ostatnie przeprowadzono głównie w celu dostosowania serwisu GODO do wymagań określonych w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001, nr 112, poz. 1198). Dokonana również została modyfikacja formularza służącego do dodawania i edycji artykułów w systemie CMS zarządzającym serwisem www.godo.gov.pl. Wykonano modyfikacje elementów kodu PHP odpowiedzialnego

⁴¹⁴ Obrady Okrągłego Stołu poprzedziło spotkanie w dniu 4 sierpnia 2008 r. Generalnego Inspektora Ochrony Danych Osobowych ze Stewartem Dresnerem, Dyrektorem Wykonawczym Privacy Laws & Business z Wielkiej Brytanii oraz Adèle Kendler, menedżerem projektu. Stewart Dresner od lat siedemdziesiątych XX w. zajmuje się różnymi aspektami ochrony danych osobowych. W 1987 r. utworzył magazyn Privacy Laws & Business - obecnie jeden z największych magazynów poświęconych ochronie prywatności i danych osobowych w świecie biznesu.

za wyświetlanie boksów zawierających aktualności i ważne informacje, aby działały w pełni automatycznie na podstawie zdefiniowanych parametrów. Zmodyfikowano też działanie mechanizmu wyszukiwania w serwisie www.giodo.gov.pl. Mianowicie do serwisu www.giodo.gov.pl podpięto statystyki google analytics w celu zebrania danych do szczegółowej analizy oglądalności serwisu. Zebrane dane posłużyły do przeprowadzenia statystycznej analizy zachowań użytkowników odwiedzających serwis informacyjny GIODO. Wyniki analizy statystyk serwisu www.giodo.gov.pl w postaci wydruków przekazywane były do Zespołu Rzecznika Prasowego. Posłużyły one do podjęcia wstępnych decyzji odnośnie sugerowanych zmian w nowej wersji serwisu. W roku 2008 rozpoczęto również prace nad nowym skryptem do obsługi górnego menu w serwisie www.giodo.gov.pl. Przygotowano nową wersję układu strony głównej oraz podstron tego serwisu. Przygotowany projekt przekazany został firmie, której w porozumieniu z Dyrektorem Zespołu Prasowego zlecono kompleksowe opracowanie projektu graficznego nowej strony informacyjnej GIODO.

Elektroniczna Skrzynka Podawcza (ESP)

W minionym roku sprawozdawczym 2007, uruchomiona została Elektroniczna Skrzynka Podawcza, co 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.

Na początku roku 2008 kontynuowano prace dostosowujące stronę internetową Biura GIODO do zadań związanych z uruchomieniem Elektronicznej Skrzynki Podawczej. Wykonywano również modyfikację konfiguracji systemu ESP w zakresie przyjmowania informacji za pośrednictwem opracowanych formularzy. W serwisie informacyjnym zamieszczono szczegółowe instrukcje dotyczące sposobu przygotowania komputera użytkownika do współpracy z oprogramowaniem obsługującym ESP Biura GIODO. W dniu 31 marca 2008 r. na stronie informacyjnej Biura GIODO uruchomiono nową zakładkę z funkcjami Elektronicznej Skrzynki Podawczej. Równoległe z wprowadzeniem ww. funkcjonalności przeprowadzono oczyszczenie bazy danych systemu ESP z korespondencji, która wysyłana była w celach testowych. Prace wdrożeniowe ESP zakończone zostały wdrożeniem opracowanych procedur wykonywania kopii bezpieczeństwa, które uwzględniają dane przetwarzane w systemie ESP.

Rozszerzenie funkcjonalności elektronicznej platformy komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych (platforma e-GIODO)

W roku 2008 wykonano kilka bardzo istotnych z punktu widzenia funkcjonalności, modyfikacji platformy e-GIODO. Najważniejsze z nich to:

1. Wprowadzenie możliwości wysyłania wniosków zgłoszenia zbiorów danych osobowych do rejestracji bez konieczności ich elektronicznego podpisywania – funkcja ta umożliwia wysłanie do GIODO drogą elektroniczną wniosku zgłoszenia zbiorów danych osobowych do rejestracji lub jego aktualizację również wtedy, gdy administrator danych nie ma możliwości opatrzenia go bezpiecznym podpisem elektronicznym. Wniosek taki może zostać rozpatrzony merytorycznie, gdy równoległe dostarczona zostanie do GIODO jego podpisana wersja papierowa.
2. Dodanie funkcji umożliwiającej sprawdzenie zawartości przygotowanego do wysłania pliku danych zawierającego wniosek zgłoszenia zbiorów danych osobowych do rejestracji wraz z ewentualnymi załącznikami - funkcja ta umożliwia podgląd treści przygotowanego do wysłania wniosku oraz załączonych do niego dokumentów, które zapisane zostały w

pliku danych w postaci gotowej do elektronicznej wysyłki. Plik ten zapisany jest w formacie XML, co sprawia, że zawarte w nim informacje nie są wprost czytelne dla użytkownika. Wprowadzona funkcjonalność pozwala na przekształcenie danych zawartych w tym pliku z postaci XML do postaci czytelnej dla użytkownika. Jej użycie powoduje wyświetlenie treści przygotowanego wniosku w postaci formularza, który był używany podczas jego przygotowywania.

3. Zmodyfikowanie funkcji „Użyj do wniosku aktualizacyjnego”. Zmodyfikowana funkcja przenosi do nowego wniosku dodatkowo dane dotyczące numeru referencyjnego pierwotnego zgłoszenia. Przeniesiony numer referencyjny dodany został również na wydruku przygotowanego wniosku, a w przypadku przesłania wniosku drogą elektroniczną, dodatkowo do treści generowanej korespondencji w celu ułatwienia obsługi nadesłanego zgłoszenia.
4. Dodanie funkcji, która umożliwia elektroniczne podpisanie i wysłanie wniosku bez konieczności stosowania zewnętrznej aplikacji do składania podpisu elektronicznego. Funkcja ta usprawnia końcowe operacje wykonywane przez administratora danych w celu złożenia podpisu elektronicznego i wysłania podpisanego wniosku do GIODO.
5. Zmiana umiejscowienia funkcji umożliwiającej zapisanie sporządzonego wniosku wraz z załącznikami do pliku w formacie XML w celu jego późniejszego użycia.
6. Zmiana umiejscowienia funkcji umożliwiającej zapisanie wniosku w postaci pliku w formacie html i/lub jego wydruk w formacie formularza czytelnego dla użytkownika.
7. Zmiana procedur obsługi wniosków nadesłanych z wewnętrznym podpisem elektronicznym w standardach ETSI oraz Xades. Potrzeba wprowadzenia tej zmiany spowodowana została zmianami standardów podpisu elektronicznego przez UNIZETO Technologies. S.A. – jednego z dostawców certyfikatów kwalifikowanych.

Portal informacyjno – szkoleniowy „eduGIODO”

W 2007 r. rozpoczęła się realizacja projektu „Ochrona danych osobowych – moje prawa, moje zadania”, który zakładał wprowadzenie 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.

Rezultatem wspomnianego projektu było uruchomienie w 2008 r. przez Generalnego Inspektora Ochrony Danych Osobowych portalu informacyjno – szkoleniowego „eduGIODO”.

Inicjatywa utworzenia internetowego serwisu edukacyjnego powstała w efekcie ustawicznego dążenia do upowszechniania tematyki ochrony danych osobowych oraz idei zwiększenia dostępu do wiedzy w tym zakresie dla każdego zainteresowanego. Podstawowym zadaniem platformy *e-learningowej* eduGIODO jest przybliżenie zagadnień dotyczących ochrony danych osobowych oraz pomoc w efektywnym stosowaniu przepisów prawa z tego obszaru.

Moduł informacyjny zawiera informacje obejmujące między innymi podstawowe definicje z zakresu ochrony danych osobowych, zasady przetwarzania danych osobowych. Administrowanie danymi oraz ich przetwarzanie w różnych obszarach, jak: komunikacja elektroniczna i społeczeństwo informacyjne, zdrowie publiczne, sprawy pracownicze, sprawy konsumenckie i inne.

Moduł szkoleniowy umożliwia uczestniczenie w 3 specjalistycznych kursach *e-learningowych*:

1. „Twoje prawa” – adresowany do osób fizycznych;
2. „Ogólne zasady przetwarzania danych” – adresowany do administratorów danych osobowych;
3. „Obowiązki administratorów danych” – adresowany do podmiotów przetwarzających dane osobowe.

Na platformie zamieszczony jest również wykaz dokumentów aktów prawa krajowego i unijnego odnoszących się do ochrony danych osobowych, ankieta analizująca profil użytkownika oraz forum dyskusyjne.

W ramach promocji portalu informacyjno – szkoleniowego eduGIODO, Generalny Inspektor Ochrony Danych Osobowych zorganizował dwie konferencje w Warszawie i Gdańsku. Zgłosił go też do V edycji konkursu na najlepsze praktyki dotyczące ochrony danych osobowych w sektorze administracji publicznej, organizowanego przez Madrycką Agencję Ochrony Danych Osobowych.

Udział Generalnego Inspektora Ochrony Danych Osobowych w pracach Komitetu Technicznego nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych

W roku 2008, podobnie jak w latach ubiegłych, GIODO uczestniczył w pracach Komitetu Technicznego nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych przy Polskim Komitecie Normalizacyjnym. Aktywność GIODO zwrócona była szczególnie na prace podejmowane przez Komitet JTC/SC27w ramach grupy roboczej WG 5 - Identity management and privacy Technologies. W roku 2008, w ramach ww. komitetu KT-182 przygotowanych zostało między innymi 5 projektów norm:

1. prPN – ISO/IEC 15946-1 Cryptographic techniques based on elliptic curves – Part 1: General, Techniki kryptograficzne oparte na krzywych eliptycznych – Część 1: Zasady ogólne.
2. prPN – ISO/IEC 19794 -1 Information Technology – Biometric data interchange formats – Part 1: Framework, Technika informatyczna – Format wymiany danych biometrycznych – Część 1: Struktura 1. wydanie – A.
3. prPN – ISO/IEC 19794 - 5 Information Technology – Biometric data interchange formats – Part 5: Face image data, Technika informatyczna – Format wymiany danych biometrycznych – Część 5: Struktura 1. Dane obrazu twarzy 1. wydanie - A.
4. prPN – ISO/IEC 19794 - 5 AMD Information Technology – Biometric data interchange formats – Part 5: Face image data AMENDMENT 1: Conditions for taking photographs for face image data, Technika informatyczna – Format wymiany danych biometrycznych – Część 5: Struktura 1. Dane obrazu twarzy AMD 1: Warunki dla wykonywania zdjęć do danych obrazu twarzy 1. wydanie - A.
5. prPN – ISO/IEC 24762 Information Technology – Security techniques – Guidelines for information and Communications technology disaster recovery services; Technika informatyczna – Techniki zabezpieczeń – Wytyczne do technik informacyjnych i komunikacyjnych dla usług odtwarzania po katastrofie.

6.2.7 Inne informacje

Porozumienie pomiędzy GIODO a Stowarzyszeniem Marketingu Bezpośredniego o wspólnym działaniu na rzecz poprawy poziomu ochrony danych osobowych i prawa do prywatności w działalności marketingowej oraz stosowaniu Kodeksu Dobrych Praktyk (Warszawa, 28 stycznia 2008 r.)

W dniu 28 stycznia 2008 r., podczas konferencji prasowej zorganizowanej w ramach obchodów Dnia Ochrony Danych Osobowych, GIODO i SMB podpisały porozumienie o współpracy na rzecz poprawy poziomu ochrony danych osobowych oraz zapewnienia prawa do prywatności. Podjęta z inicjatywy GIODO współpraca ma pomóc w standaryzacji branży marketingu bezpośredniego, uczulić na zagadnienia dotyczące danych osobowych i poprawić jej jakość i kondycję. Stowarzyszenie Marketingu Bezpośredniego zobowiązało się do podjęcia działań obligujących uczestników rynku do stosowania Kodeksu Dobrych Praktyk w prowadzonej działalności marketingowej. Kodeks ten, stanowiący załącznik do Porozumienia, definiuje najważniejsze pojęcia marketingu bezpośredniego, obowiązki administratorów oraz zasady odnoszące się do zbierania i wykorzystywania danych osobowych w tym sektorze. Strony zdecydowały także, że będą ściśle współpracowały przy nowelizacji ustawy o ochronie danych osobowych i innych procesach legislacyjnych w zakresie odnoszącym się do ochrony danych osobowych.

Wzorem dla podpisanego dokumentu były europejskie regulacje prawne w zakresie ochrony danych osobowych oraz uchwały kodeksu postępowania z danymi osobowymi w marketingu bezpośrednim Europejskiej Federacji Marketingu Bezpośredniego (FEDMA).

Studia Podyplomowe „Ochrona danych osobowych” w Wyższej Szkole Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego w Warszawie (15 marca 2008 r.)

W dniu 15 marca 2008 r. prof. dr hab. Jolanta Jabłońska – Bonca, Prorektor ds. Studiów Prawniczych Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, otworzyła pierwszą edycję studiów podyplomowych "Ochrona Danych Osobowych", organizowanych wspólnie z Generalnym Inspektorem Ochrony Danych Osobowych. Głównym celem studiów podyplomowych jest usystematyzowane zapoznanie słuchaczy z problematyką funkcjonowania systemu ochrony danych osobowych na gruncie prawa polskiego i europejskiego. Zajęcia na studiach prowadzą znani i cenieni przedstawiciele nauki polskiej, sędziowie Sądu Najwyższego, Naczelnego Sądu Administracyjnego, adwokaci, radcy prawni oraz specjaliści pełniący funkcje dyrektorów poszczególnych departamentów Biura Generalnego Inspektora Ochrony Danych Osobowych.

Porozumienie o współpracy między Generalnym Inspektorem Ochrony Danych Osobowych a Wyższą Szkołą Biznesu National-Louis w Nowym Sączu (20 maja 2008 r.)

Podczas konferencji „Biznes a Ochrona Danych Osobowych” zorganizowanej przez Wyższą Szkołę Biznesu National-Louis University w Nowym Sączu (Nowy Sącz, 20 maja 2008 r.). Pan Michał Serzycki Generalny Inspektor Ochrony Danych Osobowych i Jego Magnificencja Pan dr Richard Magner, Rektor Wyższej Szkoły Biznesu National-Louis University podpisali Porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych. Natomiast Pan Andrzej Lewiński - Zastępca Generalnego Inspektora Ochrony Danych Osobowych oraz Pan dr Krzysztof Pawłowski, Prezydent Wyższej Szkoły Biznesu National-Louis University podpisali Umowę w sprawie współpracy w zakresie ochrony prywatności i danych osobowych. Dążąc do podwyższania wiedzy zawodowej i profesjonalnych umiejętności praktycznych oraz doskonalenia mechanizmów działalności w zakresie ochrony prywatności i danych osobowych, obie instytucje postanowiły, że inicjować będą wspólne przedsięwzięcia, takie jak seminaria, konferencje, prace naukowe i badawcze w celu spełnienia założeń Porozumienia i Umowy.

Newsletter „Prywatność w świecie. Przegląd wydarzeń.”

W celu zagwarantowania systematycznego otrzymywania informacji dotyczących ochrony prywatności i danych osobowych za granicą, od września 2008 r. Departament Edukacji Społecznej i Współpracy Międzynarodowej rozpoczął periodyczne rozsyłanie pracownikom Biura GODO Newsletter „Prywatność w świecie. Przegląd wydarzeń.”

Wznowienie współpracy Generalnego Inspektora Ochrony Danych Osobowych z Polską Izłą Ubezpieczeń.

Współpraca ekspercka, podejmowanie wspólnych działań legislacyjnych i edukacyjnych oraz wspólne prowadzenie prac nad Kodeksem Dobrych Praktyk w zakresie przetwarzania danych osobowych - to główne ustalenia ze spotkania Generalnego Inspektora Ochrony Danych Osobowych z przedstawicielami Polskiej Izby Ubezpieczeń, które odbyło się 31 lipca 2008 r. w Warszawie.

Strony uzgodniły, że Zarząd Polskiej Izby Ubezpieczeń [PIU] i GODO będą uczestniczyli w organizowanych cyklicznie co kwartał spotkaniach w celu wymiany doświadczeń. Generalny Inspektor Ochrony Danych zapowiedział wydanie broszury „ABC ochrony danych osobowych w działalności ubezpieczeniowej”.

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

Jednym z zadań Generalnego Inspektora jest uczestnictwo 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 organizowanych w kraju i za granicą, a także różnych formach współpracy z innymi organami ochrony danych osobowych. Do najważniejszych zadań GODO w ramach współpracy międzynarodowej należy:

1. udział w pracach Grupy roboczej art. 29 ds. ochrony danych osobowych,
2. wyznaczenie członków Wspólnego Organu Nadzorczego zajmującego się zagadnieniami ochrony danych osobowych w związku z utworzeniem tzw. Obszaru Schengen (WON Schengen),
3. wybór członków Wspólnego Organu Nadzorczego nad Europolem (WON Europol), ich zastępców oraz kandydatów na członka Komitetu Rewizyjnego oraz jego zastępcę,
4. udział w pracach grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac,
5. uczestniczenie w pracach Komitetu Konsultacyjnego ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych,
6. wyznaczenie członków Wspólnego Organu Nadzorczego właściwego w sprawach ochrony danych osobowych w związku z wykorzystywaniem systemu informacji celnej (WON Cła),
7. udział w pracach Grupy roboczej ds. policji i wymiaru sprawiedliwości,
8. współpraca w ramach Grupy organów ochrony danych osobowych Europy Środkowej i Wschodniej,
9. udział w pracach Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji,
10. udział w Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności, Wiosennej Konferencji Europejskich Organów Ochrony Danych oraz Warsztatach Rozpatrywania Spraw,
11. współpraca z rzecznikami ochrony danych innych krajów,
12. współpraca z Data Protection Review i członkostwo w Radzie Doradczej tego ukazującego się co cztery miesiące periodyku internetowego, publikowanego przez madrycki organ ochrony danych.⁴¹⁵

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

Grupa robocza art. 29

W omawianym roku sprawozdawczym, podobnie 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 przede wszystkim do zagadnień związanych z przetwarzaniem danych osobowych w I i III filarze UE.

Na szczególne podkreślenie zasługuje zwłaszcza współpraca Generalnego Inspektora z w ramach Grupy roboczej art. 29 ds. ochrony danych osobowych, która została ustanowiona na podstawie art. 29 dyrektywy 95/46/WE. 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 roku 2008 Grupa przyjęła Program prac na lata 2008-2009, w którym podkreślono konieczność rozważenia trzech podstawowych kwestii: zwiększenia oddziaływania dyrektywy 95/46/WE oraz roli Grupy roboczej, wpływu nowych technologii na kwestie ochrony danych osobowych oraz uwarunkowania światowe (przekazywanie danych do innych krajów oraz zagadnienia dotyczące ochrony prywatności i jurysdykcji w wymiarze światowym).⁴¹⁶ Efektem prac Grupy w bieżącym okresie sprawozdawczym było przyjęcie opinii i dokumentów roboczych dotyczących ochrony danych osobowych dzieci, ochrony danych związanych z wykorzystywaniem przeglądarek internetowych, wspólnych działań kontrolnych,⁴¹⁷ wiążących reguł korporacyjnych, przeglądu dyrektywy 2002/58/WE o ochronie prywatności w sektorze łączności elektronicznej oraz standardów ochrony danych w Globalnym Kodeksie Antydopingowym. W wyniku działań podjętych przez Generalnego Inspektora Ochrony Danych

⁴¹⁵ Najnowsze wydanie i archiwalne numery periodyka „Data Protection Review” można znaleźć w Internecie pod adresem www.dataprotectionreview.eu

⁴¹⁶ Dokumenty przyjęte przez Grupę dostępne są na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych <http://www.giodo.gov.pl/463/j/pl/> oraz na stronie Komisji Europejskiej http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm

Osobowych, służby tłumaczeniowe Komisji Europejskiej zagwarantowały możliwość wypowiadania się w języku polskim podczas posiedzeń plenarnych Grupy roboczej art. 29.

Generalny Inspektor uczestniczył w spotkaniu podgrupy roboczej art. 29 ds. technologii (Technology Subgroup), które odbyło się 22 kwietnia 2008 r. w Brukseli.

Spotkanie podgrupy miało na celu przygotowanie opinii w sprawie zrewidowania i aktualizacji postanowień dyrektywy ePrivacy, w związku z nowymi środkami przekazu i dostarczania informacji oraz z uwagi na niezbędne z punktu widzenia transparentności działań, informowanie opinii publicznej o każdym naruszeniu bezpieczeństwa danych. W trakcie spotkania wskazano na potrzebę współpracy dostawców usług telekomunikacyjnych z krajowym organem regulującym (NRA) w tej dziedzinie. W przypadku Polski byłby to Urząd Komunikacji Elektronicznej. Wskazywano również na konieczność rozszerzenia działalności samej dyrektywy z abonentów danej usługi na wszystkie osoby. Modyfikacja ta dawałaby możliwość objęcia ochroną również osoby korzystające z usług elektronicznych (np. z połączeń w technologii bluetooth), ale niebędących abonentami dostawcy usług telekomunikacyjnych w tym zakresie. Biorąc powyższe pod uwagę, podgrupa położyła nacisk na konieczność uregulowania kwestii niezamówionej komunikacji za pośrednictwem ww. technologii bluetooth (lub innych podobnych), gdzie osoba posiadająca aktywne urządzenie z taką technologią jest atakowana niechcianymi informacjami z pobliskich słupów reklamowych, wyposażonych w nadajniki. W związku z powyższym podgrupa wskazała na potrzebę rozszerzenia definicji systemów automatycznego dzwonienia o automatyczne systemy komunikacyjne.

Wspólne Organy Nadzorcze

W 2008 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. Podczas prac przyjęte zostały opinie dotyczące, między innymi przepisów mających zastosowanie do plików analitycznych Europolu, projektu przepisów wykonawczych dotyczących stosunków Europolu z jego partnerami, w tym wymiany danych osobowych i informacji tajnych.⁴¹⁸ Generalny Inspektor uczestniczył również w pracach Wspólnego Organu Nadzorczego nad Systemem Schengen oraz Wspólnego Organu Nadzorczego nad Cłami. Ponadto w 2008 r. Komitet rewizyjny rozpatrywał jedną sprawę indywidualną, w której uznał, że decyzja Europolu w sprawie wniosku Pana W. o sprawdzenie, poprawienie i usunięcie danych jest zgodna z art. 19 ust. 3 Konwencji o Europolu.⁴¹⁹

Generalny Inspektor uczestniczył również w pracach Wspólnego Organu Nadzorczego nad Systemem Informacyjnym Schengen (WON Schengen), Wspólnego Organu Nadzorczego nad Cłami oraz Grupy roboczej ds. Policji i Wymiaru sprawiedliwości. W ramach WON Schengen szczególną uwagę należy zwrócić na rozpoczęcie prac mających na celu zgromadzenie informacji na temat procedur stosowanych na poziomie krajowym przy dokonywaniu wpisów do SIS na podstawie art. 97 i 98 Konwencji Wykonawczej do Układu z Schengen. Generalny Inspektor zwrócił się w tej sprawie do Komendanta Głównego Policji.⁴²⁰

W omawianym okresie sprawozdawczym Generalny Inspektor brał również udział w pracach grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac, w ramach których na podstawie wspólnie przygotowanego kwestionariusza przeprowadzono badanie dotyczące sposobu spełnienia obowiązku informacyjnego wobec osób, których dane są zbierane na potrzeby tego systemu oraz oceny wieku osób młodocianych ubiegających się o azyl - nielegalnych imigrantów. Generalny Inspektor zwrócił się

⁴¹⁷ Grupa robocza podjęła decyzję o przeprowadzeniu drugiej skoordynowanej kontroli mającej na celu sprawdzenie poziomu zgodności działań dostawców usług telekomunikacyjnych i Internetu z przepisami prawa w zakresie przechowywania danych transmisyjnych na poziomie krajowym na podstawie art. 6 i 9 dyrektywy 2002/58/WE o prywatności i łączności elektronicznej oraz dyrektywy 2006/24/WE zmieniającej dyrektywę o prywatności i łączności elektronicznej.

⁴¹⁸ Więcej informacji na stronach internetowych Generalnego Inspektora: http://www.giodo.gov.pl/265/id_art/2716/j/pl/ oraz WON: <http://europoljsb.consilium.europa.eu/default.asp?lang=PL>.

⁴¹⁹ Decyzja nr 06/01 z dnia 26 marca 2008 r.

⁴²⁰ DESIWM-074-33/08.

o wypełnienie kwestionariusza do Komendanta Głównego Straży Granicznej, Komendanta Głównego Policji oraz Szefa Urzędu ds. Cudzoziemców.⁴²¹ Na podstawie zebranych informacji zostanie przygotowany całościowy raport obrazujący sytuację w UE.

7.1 Międzynarodowe spotkania i konferencje

Generalny Inspektor Ochrony Danych Osobowych oraz pracownicy jego Biura uczestniczyli także w konferencjach i seminariach o charakterze międzynarodowym w kraju i za granicą. Do najważniejszych z nich należy zaliczyć te wymienione poniżej.

1. 43. Spotkanie Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji (Rzym, 3 - 4 marca 2008 r.)

Głównym tematem tego spotkania były sprawy związane z działalnością portali społecznościowych. W odniesieniu do tego tematu, Generalny Inspektor Ochrony Danych Osobowych przedstawił dwie zasadnicze uwagi do redagowanego przed i w czasie spotkania dokumentu stanowiącego rekomendacje dla twórców i użytkowników portali społecznościowych. Dotyczyły one, po pierwsze - zwrócenia szczególnej uwagi ze strony osób starszych i opiekunów na osoby niepełnoletnie, które korzystają z portali społecznościowych i po drugie – na kwestie związane z używaniem innych zestawów danych służących do uwierzytelniania się w tych portalach, niż zestawy stosowane do uwierzytelniania się w systemach bankowych czy poczcie elektronicznej.

2. Wiosenna Konferencja Europejskich Organów Ochrony Danych i Prywatności (Rzym, 17 – 18 kwietnia 2008 r.)

Motywy przewodnim Konferencji było pytanie o przyszłość dla prywatności i bezpieczeństwa. Podczas sesji „Ochrona prywatności a bezpieczeństwo” Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Ochrona danych w obszarze wolności, bezpieczeństwa i sprawiedliwości w świetle Traktatu z Lizbony”. Konferencja przyjęła również Deklarację stanowiącą podsumowanie jej obrad. W Deklaracji tej wyrażone jest zaniepokojenie Komisji zbyt daleko idącą kontrolą osób wkraczających na obszar Schengen lub opuszczających go, niezależnie od narodowości. Uznano, że choć skuteczne zarządzanie bezpieczeństwem granic jest niezbędne do ochrony Unii przed potencjalnymi zagrożeniami, to nie powinno ono wpływać na ochronę praw i wolności podróżnych, zwłaszcza na ich prawo do prywatności. Monitoring podróżnych musi być dobrze uzasadniony i może być dozwolony wyłącznie w wyjątkowych przypadkach oraz dla konkretnych, uzasadnionych celów. Natomiast wszelki ogólny nadzór powoduje niedopuszczalne zagrożenie dla wolności obywateli. Inna kwestia poruszona w Deklaracji, to leżący u podstaw tych działań brak zaufania do podróżnych, okazywany przez oddzielanie podróżnych „w dobrej wierze” od pozostałych, a nawet uznawanie tych ostatnich za potencjalnych przestępców i dwukrotne prześwietlanie ich zarówno przed, jak i za bramką i automatyczne przetwarzanie szczegółowych danych ich dotyczących.

Rzecznicy ochrony danych zgodni byli co do tego, że biorąc pod uwagę koszty – pośrednie i bezpośrednie, zarówno finansowe jak i dla wolności – tworzenia nowych systemów, takich jak system wejść-wyjść, powinny istnieć niepodważalne dowody, że systemy te stanowią najlepszą odpowiedź na problemy, z którymi mają walczyć. W przeciwnym razie należy przyjąć, że tego rodzaju praktyki są sprzeczne z wartościami uznawanymi przez Unię Europejską.

3. X. Spotkanie Grupy Organów Ochrony Danych Osobowych Europy Środkowej i Wschodniej (Central and Eastern European Data Protection Authorities), Kazimierz Dolny, 1–4 czerwca 2008 r. zorganizowane przez Generalnego Inspektora Ochrony Danych Osobowych.

Ideę corocznych Spotkań Grupy Organów Ochrony Danych Osobowych Europy Środkowej i Wschodniej zainicjował polski organ ochrony danych osobowych w 2001 r. w Warszawie i przez wszystkie lata jego istnienia odgrywał kluczową rolę w jego pracach i podejmowanych wspólnie inicjatywach. Podczas X. spotkania dyskutowano między innymi o prywatności dzieci w środowisku

⁴²¹ DESiWM-072-31/08.

on-line, zadaniach realizowanych przez organy ochrony danych osobowych z państw Europy Środkowej i Wschodniej w kontekście rozszerzanie strefy Schengen, kwalifikacjach, zadaniach i uprawnieniach Administratorów Bezpieczeństwa Informacji, a także podsumowano ostatnie lata działalności forum CEEDPA. Grupa przyjęła również dwie deklaracje końcowe w sprawie dalszej współpracy w ramach Grupy oraz w sprawie równego traktowania języków narodowych wszystkich państw członkowskich Unii Europejskiej. Druga z wymienionych deklaracji została następnie przesłana do Komisji Europejskiej oraz Przewodniczącego Grupy roboczej art. 29.

4. 30. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności pt. „Ochrona prywatności w świecie bez granic” (Strasburg, 15 – 17 października 2008 r.)

W związku z głównym tematem konferencji przyjęta została „Rezolucja dotycząca naglącej potrzeby ochrony prywatności w świecie bez granic oraz w sprawie wypracowania wspólnego stanowiska dotyczącego Międzynarodowych Standardów Ochrony Danych i Prywatności.”

Jednym z najważniejszych tematów omawianych w Strasburgu była ochrona prywatności nieletnich. Przedstawiciele ponad 60 krajów zgodzili się, że najlepszą drogą do wykształcenia u młodych ludzi umiejętności bezpiecznego korzystania z Internetu są programy edukacyjne, wskazujące na rozwiązania przyjazne dla ochrony prywatności i uczące szacunku dla prywatności innych osób. Efektem prac podjętych w czasie konferencji było przyjęcie rezolucji dotyczącej ochrony prywatności dzieci w Internecie. Inne ważne tematy to ochrona prywatności w dobie szybkiego rozwoju portali społecznościowych (przyjęta została rezolucja dotycząca tego zagadnienia) oraz wielokrotnie podkreślana przez przedstawicieli wielu organów ochrony danych, konieczność nawiązania ściślejszej współpracy między organami ochrony danych a światem biznesu. W zglobalizowanym świecie odpowiednie zabezpieczenia przepływu danych potrzebne są bardziej niż kiedykolwiek. Ochrona danych nie powinna być jednak traktowana jako przeszkoda w prowadzeniu interesów, a raczej jako użyteczne narzędzie ochrony klientów, pozwalające na nawiązanie z nimi poprawnych relacji.

Uczestnicy konferencji przyjęli również kilka innych rezolucji traktujących o najważniejszych problemach poruszanych na tym spotkaniu. I tak przyjęto rezolucję dotyczącą ustanowienia Komitetu Sterującego ds. reprezentacji na posiedzeniach organizacji międzynarodowych. Celem tej rezolucji jest doprowadzenie do utworzenia procedury umożliwiającej wnoszenie wspólnego wkładu do pracy organizacji międzynarodowych oraz reprezentowanie organów ochrony danych na posiedzeniach organizacji międzynarodowych, zarówno rządowych, jak i pozarządowych, w celu lepszego propagowania podstawowych powszechnych zasad ochrony danych i prywatności na poziomie międzynarodowym oraz do utworzenia Komitetu Sterującego. Przyjęto również rezolucje dotyczące wprowadzenia Dnia Ochrony Danych i Prywatności oraz rezolucję zaproponowaną przez Grupę Roboczą ds. Strony Internetowej.

5. Warsztaty EPON

W dniach 12 – 13 listopada 2008 r. w Warszawie odbyły się warsztaty zorganizowane przez Generalnego Inspektora Ochrony Danych Osobowych oraz European Privacy Officers Network [EPON]. Głównym celem warsztatów organizowanych cyklicznie przez EPON jest przybliżenie problematyki dotyczącej ochrony danych osobowych i prywatności zainteresowanym podmiotom reprezentującym szeroko rozumiany sektor prywatny oraz nawiązanie odpowiedniego dialogu pomiędzy tymi podmiotami a organami nadzorczymi w celu wypracowania jak najlepszych rozwiązań w omawianej dziedzinie. Podczas tegorocznych warsztatów dyskutowano między innymi następujące kwestie: główne kierunki działań GODO, najważniejsze problemy w dziedzinie ochrony danych, planowane zmiany w ustawie o ochronie danych oraz aktach wykonawczych, bezpieczeństwo danych, przekazywanie danych za granicę, ochrona danych w sektorze zatrudnienia.

6. Seminarium międzynarodowe „Przyspieszenie dochodzenia prawnokarnego i ścigania transgranicznej przestępczości gospodarczej” (Paryż, 17-19 listopada 2008 r.).

Seminarium międzynarodowe było drugim z kolei spotkaniem ekspertów w ramach wspólnego projektu szkoleniowego (wspieranego przez program Komisji Europejskiej „Wymiar sprawiedliwości w sprawach karnych”) Ministerstwa Sprawiedliwości

Niemiec i Francji oraz Krajowego Centrum Szkolenia Kadr Sądów Powszechnych i Prokuratury z Polski. Celem seminarium było rozszerzenie współpracy różnych organów w zakresie ścigania i zapobiegania transgranicznej przestępczości gospodarczej. Generalny Inspektor Ochrony Danych Osobowych wygłosił referat na temat ochrony danych osobowych w związku ze ściganiem przestępstw gospodarczych, uwzględniając sytuację podmiotów gospodarczych, na które nakładane są obowiązki związane z kontrolą i nadzorem aktywności konsumentów oraz przedsiębiorców.

7.1 międzynarodowe seminarium na temat ochrony danych i statusu prawnego jednostki (Madryt, 4 grudnia 2008 r.) zorganizowane na Uniwersytecie Rey Juan Carlos.

Seminarium adresowane było do studentów, nauczycieli, naukowców i wszystkich zainteresowanych problematyką ochrony danych osobowych w kontekście zagwarantowania fundamentalnych praw jednostce w różnych sytuacjach społecznych, w jakich może się ona znaleźć, np. będąc osobą niepełnoletnią, w trakcie edukacji, postępowania przygotowawczego prowadzonego przez organy ścigania czy będąc uczestnikiem handlu elektronicznego. Podczas obrad przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych przedstawił referat na temat ochrony danych osobowych w kontekście innych fundamentalnych praw w polskim systemie legislacyjnym.

7.2 Wizyty robocze

W działalności Generalnego Inspektora tradycyjnie dużą rolę odgrywa współpraca dwustronna, która polega m.in. na wymianie informacji, pomocy przy prowadzeniu postępowań administracyjnych i 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 wykorzystywane były w dalszej jego pracy.

W dniu **24 kwietnia 2008 r.** Generalny Inspektor Ochrony Danych Osobowych gościł delegację Słowackiego Organu Ochrony Danych Osobowych wraz z Panem Gyula Vszelei, jego Prezydentem. W trakcie spotkania omówiona została działalność obu organów, wspólne problemy dotyczące ochrony danych osobowych oraz wymiana doświadczeń związanych z działalnością polskiego i słowackiego organu.

Prezydent Słowackiego Organu Ochrony Danych Osobowych udzielił wywiadu prasowego dla ogólnopolskiego dziennika „Rzeczpospolita”, w którym poruszył między innymi zagadnienia związane z regulacjami słowackiego prawa o ochronie danych osobowych w odniesieniu do danych biometrycznych.

W dniach **6 - 7 sierpnia 2008 r.** Generalny Inspektor Ochrony Danych Osobowych złożył roboczą wizytę w Biurze Rzecznika Ochrony Danych Osobowych w Czechach. Tematem spotkania były zagadnienia dotyczące wzajemnej współpracy na poziomie krajowym i międzynarodowym oraz wymiana doświadczeń.

7.3 Warsztaty Rozpatrywania Spraw

Przedstawiciele Biura Generalnego Inspektora Ochrony Danych Osobowych systematycznie uczestniczą w organizowanych dwa razy w roku warsztatach rozpatrywania spraw, tzw. warsztatach skargowych (case handling workshop). W roku 2008 warsztaty były zorganizowane w dniach 31 marca – 1 kwietnia w Słowenii i 29–30 września w Bratysławie. Podczas warsztatów przedstawiciele organów ochrony danych osobowych z państw członkowskich Unii Europejskiej wraz z Europejskim Inspektorem Ochrony Danych przedyskutowali kwestie dotyczące między innymi: prowadzenia postępowań w związku z wnoszonymi skargami oraz postępowań kontrolnych (również w związku z przystąpieniem nowych państw członkowskich UE do strefy Schengen), ochrony danych w związku z działalnością mass mediów, środków bezpieczeństwa przy przetwarzaniu danych osobowych, ochrony danych w związku z wykorzystywaniem tzw. linii donosicielskich, monitoringu pracowników w miejscu pracy oraz monitoringu video w miejscach publicznych oraz na terenach prywatnych.

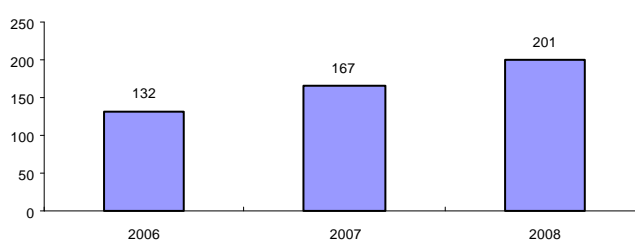
Część III.

Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2008 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 zabranieniem 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.

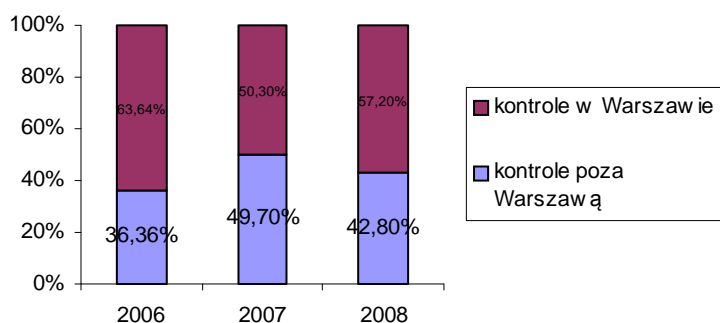
Liczne uchybienia występowały również w procesie przetwarzania danych osobowych przy użyciu **systemów informatycznych**. Trudności z prawidłowym wypełnieniem obowiązków określonych w przepisach rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych,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

W 2008 r. przeprowadzonych zostało 201 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Od 2006 r. liczba kontroli systematycznie wzrasta (zob. Wykres 26).



Wykres 26.
Porównanie liczby kontroli przeprowadzonych w latach 2006–2008.

Z kolei Wykres 27 przedstawia procentowe zastawienie kontroli przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych na terenie Warszawy oraz poza nią.



Wykres 27.
Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2006–2008.

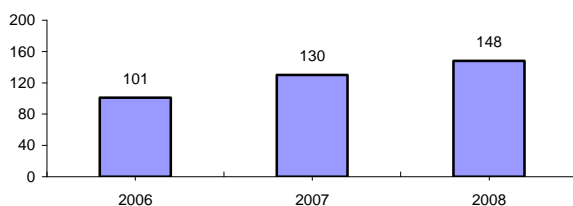
Najwięcej kontroli przeprowadzonych zostało z urzędu (133). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący:

Inicjatywa kontroli	Liczba kontroli
Z urzędu	133
Departament Orzecznictwa, Legislacji i Skarg	30
Departament Rejestracji Zbiorów Danych Osobowych	12
Departament Edukacji Społecznej i Spraw Międzynarodowych	1
Prokuratura	6
Rzecznik Dyscypliny Finansów Publicznych	1
Kancelaria Prezesa Rady Ministrów	1
W związku z inną kontrolą	17

Najczęściej czynnościom kontrolnym poddawane były podmioty z sektorów oświaty, mieszkalnictwa, biur podróży i marketingu. Jednakże 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 w 2008 r. szkoły (24 kontrole), spółdzielnie mieszkaniowe (16 kontroli), biura podróży (20 kontroli) oraz firmy marketingowe (20 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 2008 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 9 kontroli sprawdzających wykonanie decyzji administracyjnych. Wykazały one, że wszystkie skontrolowane ponownie podmioty wykonały wydane wobec nich decyzje. W 2008 r. Generalny Inspektor w związku z przeprowadzonymi kontrolami wydał łącznie 148 decyzji.

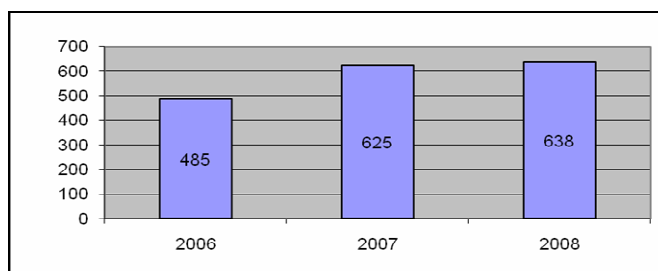


Wykres 28.

Porównanie liczby decyzji wydanych w związku z kontrolami przeprowadzonymi w latach 2006–2008.

W okresie sprawozdawczym, w związku z wejściem Polski do strefy Schengen, przeprowadzone zostały także kontrole podmiotów uprawnionych do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych SIS oraz w celu wglądu do danych SIS, tj. jednostek Policji (8 kontroli), jednostek Straży Granicznej (9 kontroli), izb celnych (4 kontrole) i konsulatów (2 kontrole). W wyniku kontroli ustalono sposób przetwarzania danych osobowych przez te podmioty w związku z realizacją ich uprawnień wynikających z przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej.⁴²²

W 2008 r. skontrolowano 638 systemów informatycznych wykorzystywanych do przetwarzania danych osobowych, co obrazuje Wykres 29:



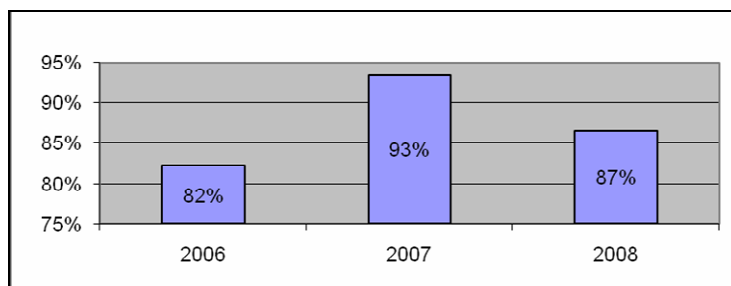
Wykres 29.

Liczba skontrolowanych systemów informatycznych w latach 2006-2008.

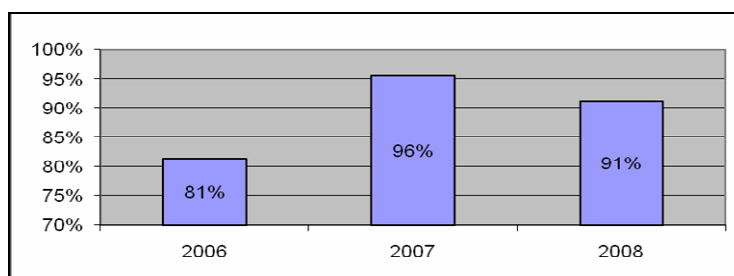
Stopień wypełnienia w poszczególnych latach (od roku 2006 do 2008) wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie o ochronie danych osobowych i rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych, przedstawiony został poniżej w formie wykresów statystycznych. Poszczególne zestawienia obrazują procentowe wyniki kontroli w odniesieniu do ogólnej liczby kontroli w danym roku lub ogólnej liczby kontrolowanych w danym roku systemów informatycznych. W zestawieniach tych przyjęto zasadę, że warunki odnoszące się do wymaganych funkcjonalności systemów informatycznych oceniane były w skali procentowej do liczby kontrolowanych systemów. Pozostałe natomiast, odnoszące się, np. do dokumentacji procesu przetwarzania, czy też do obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, oceniano w skali procentowej w stosunku do liczby kontrolowanych podmiotów.

Co do stopnia wypełnienia wymogów formalnych i organizacyjnych, jednostkę statystyczną stanowił kontrolowany podmiot. Stopień wykonania przez kontrolowane podmioty poszczególnych warunków przedstawiono na poniższych wykresach.

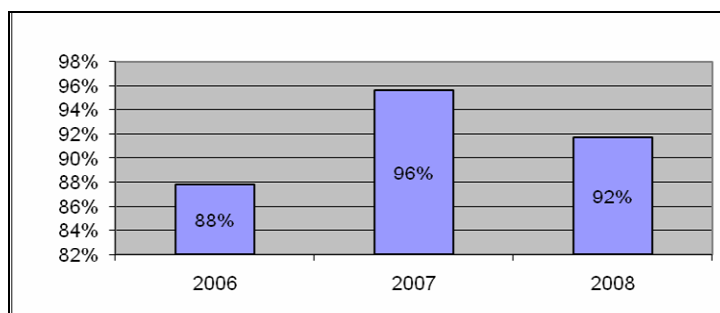
⁴²² Dz. U. Nr 165, poz. 1170.



Wykres 30.
Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych w latach 2006 - 2008.

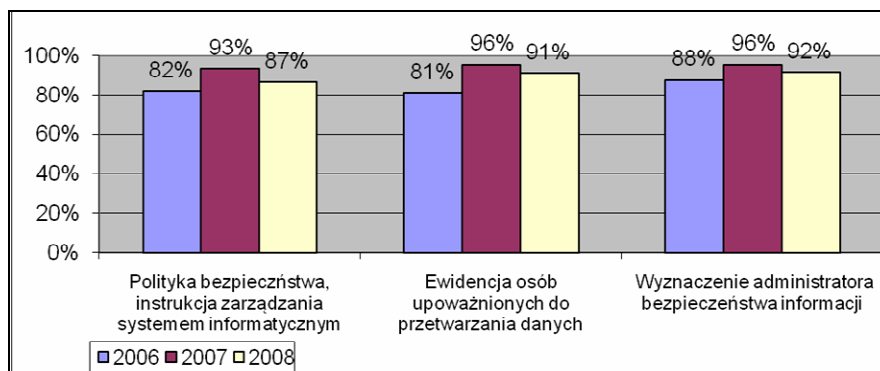


Wykres 31.
Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w latach 2006 - 2008.



Wykres 32.
Stopień realizacji obowiązku wyznaczenia osoby wykonującej zadania administratora bezpieczeństwa informacji w latach 2006 – 2008.

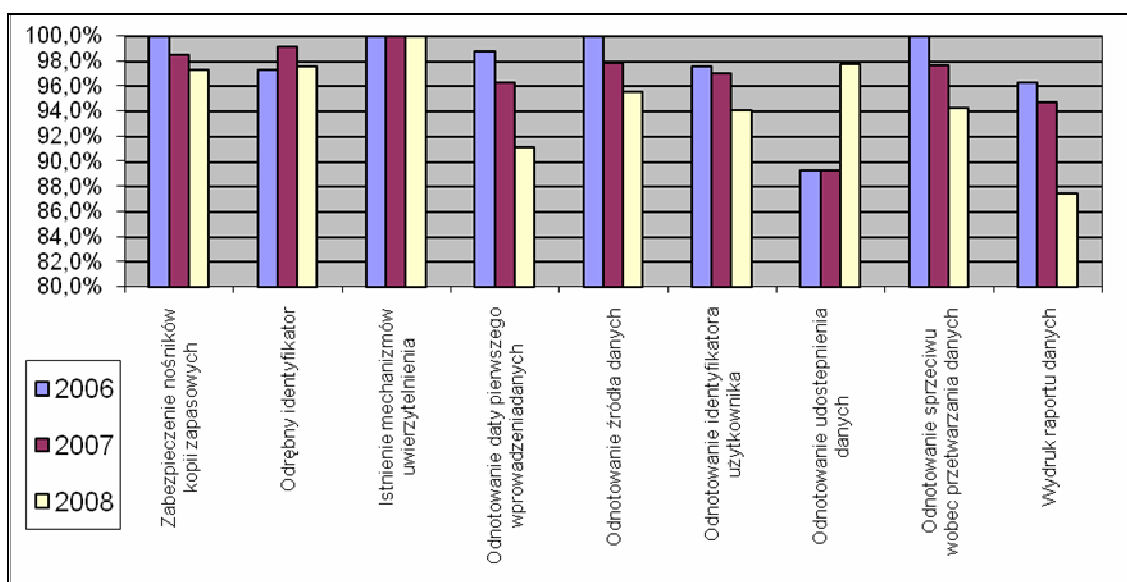
Stopień wypełnienia wymogów formalnych, organizacyjnych i personalnych w zakresie dotyczącym prowadzenia dokumentacji przetwarzania danych osobowych, wdrożenia do stosowania opracowanej dokumentacji oraz wyznaczenia osoby wykonującej zadania administratora bezpieczeństwa informacji [ABI], odnoszących się do warunków, jakim powinny odpowiadać urządzenia i systemy informatyczne używane do przetwarzania danych osobowych, zestawiono na poniższym wykresie:



Wykres 33.

Stopień realizacji obowiązku prowadzenia dokumentacji stanowiącej politykę bezpieczeństwa, instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych, oraz wypełnienie obowiązku wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji w latach 2006 – 2008.

Jednostkę statystyczną w zestawieniach odnoszących się do stopnia realizacji technicznych warunków przetwarzania danych stanowił kontrolowany system informatyczny. Przewidziane warunki uznawano dla kontrolowanego systemu 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 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 osobowych.



Wykres 34.

Stopień realizacji wymogów technicznych w latach 2006 – 2008.

Kontrola dużej liczby różnorodnych systemów informatycznych spowodowała, że działania kontrolne obejmowały szeroki zakres rozwiązań technologicznych, od najbardziej rozbudowanych opartych o zaawansowane mechanizmy bazodanowe, po najprostsze, gdzie zbiory danych osobowych przetwarzane były z wykorzystaniem powszechnie dostępnych aplikacji biurowych (edytorów tekstu, arkuszy kalkulacyjnych). W przypadku rozbudowanych systemów informatycznych zaobserwowano, że podmioty kontrolowane stosowały najczęściej kompleksowe podejście do zagadnień bezpieczeństwa. Większość z takich podmiotów

przetwarzała dane osobowe w sposób zgodny z ustawą o ochronie danych osobowych. W żadnym z kontrolowanych w 2008 r. podmiotów inspektorzy nie natrafili na systemy informatyczne służące do przetwarzania danych, które zostały dopuszczone przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

Oceniając wyniki przeprowadzonych kontroli stwierdzić należy, że duża część kontrolowanych jednostek miała problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Około 13% kontrolowanych podmiotów miało również problem z prawidłowym opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych. Ponadto wiele zastrzeżeń budziły także stosowane środki techniczne i organizacyjne mające zapewnić ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń i kategorii danych objętych ochroną, tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Porównanie stopnia realizacji poszczególnych wymogów ustawy i rozporządzenia w latach 2006 - 2008 wskazuje tendencję spadkową zarówno w odniesieniu do wymagań formalno-organizacyjnych, jak i wymagań o charakterze technicznym. Sposób realizacji w 2008 r. obowiązku prowadzenia dokumentacji stanowiącej politykę bezpieczeństwa, instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych, jak również sposób realizacji obowiązku wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji kształtował się średnio na poziomie 90%, co w porównaniu z rokiem ubiegłym stanowi około 5% spadek. Należy również zauważyć, że porównanie stopnia realizacji poszczególnych wymogów ustawy w latach 2006 – 2008 wskazuje widoczny spadek w obszarze dotyczącym technicznych warunków przetwarzania danych osobowych, a zwłaszcza w obszarze wymagań dotyczących funkcjonalności systemów informatycznych. W odniesieniu do 2007 r. największy spadek w zakresie stopnia realizacji wymogów o charakterze technicznym, stanowi brak zapewnienia przez systemy informatyczne odnotowania informacji o dacie pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane do systemu, sprzeciwu wobec przetwarzania danych, jak również brak możliwości sporządzenia i wydrukowania przez system informatyczny raportu zawierającego w powszechnie zrozumiałej formie informacji, o których mowa w § 7 ust. 1 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 osobowych. W porównaniu z latami ubiegłymi, na wzrost stwierdzonych nieprawidłowości w 2008 r. wpłynął głównie niski stopień realizacji przepisów o ochronie danych osobowych w spółdzielniach mieszkaniowych, firmach marketingowych oraz jednostkach oświatowych. Nieprawidłowości ustalone w ww. grupach były znacznie większe niż średnia nieprawidłowości dla wszystkich kontrolowanych jednostek.

W obszarze dotyczącym funkcjonalności systemów informatycznych zaobserwować można wyraźną (ponad ośmioprocentową) poprawę realizacji wymogu zapewnienia przez systemy informatyczne odnotowania informacji komu, kiedy i w jakim zakresie dane zostały udostępnione. Na przełomie lat 2006 - 2008 można zaobserwować tendencję wzrostową w zakresie dotyczącym stopnia implementacji mechanizmów uwierzytelnienia. Najczęściej stosowanym mechanizmem zabezpieczającym dostęp do danych wykorzystywanym przez systemy informatyczne był standardowy proces logowania, polegający na wprowadzaniu przy użyciu klawiatury komputera w systemowe okno logowania identyfikatora użytkownika oraz hasła. Odmienne sposoby uwierzytelnienia użytkowników stosowane do kontroli dostępu do danych odnotowano jedynie w jednostkach Policji, gdzie zastosowano osobiste identyfikatory cyfrowe (tzw. kluczyki) oraz karty mikroprocesorowe. Wraz z kluczykiem i/lub kartą mikroprocesorową użytkownik otrzymywał czteroznakowy PIN (sekret). W celu wzmocnienia bezpieczeństwa w procesie uwierzytelniania zastosowano więc metodę uwierzytelniania bazującą na weryfikacji posiadanej rzeczy oraz znanego tylko upoważnionemu użytkownikowi sekretu. W procesie uwierzytelniania do poprawnej weryfikacji niezbędne było użycie właściwego kluczyka bądź karty mikroprocesorowej i wprowadzenie kodu PIN.

Należy jednak zaznaczyć, że mimo iż w kontrolowanych systemach informatycznych zastosowane były wspomniane mechanizmy uwierzytelnienia, to w niektórych podmiotach był on niewłaściwie stosowany. Najczęściej spotykanymi

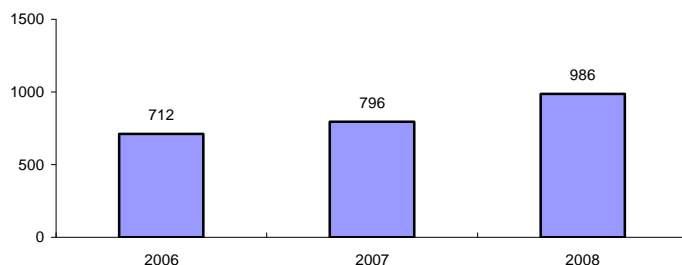
nieprawidłowościami było wykorzystywanie jednego identyfikatora logowania przez więcej niż jedną osobę, wykorzystywanie wspólnego hasła logowania, nieodpowiednia konstrukcja hasła (zazwyczaj zbyt krótkie) oraz częstotliwość jego zmiany (rzadziej niż raz na 30 dni). W 2008 r. zaobserwowano ponadto większą liczbę uchybień dotyczących należytego zabezpieczenia nośników zawierających zapasowe kopie danych. W dobie elektronizacji danych proces ich zabezpieczania za pomocą kopii zapasowych powinien być jednym z priorytetowych. Spadek stopnia realizacji powyższego wymogu, choć nieznaczny, budzi więc zaniepokojenie.

Obowiązki określone w przepisach o ochronie danych osobowych nie były wykonywane przez jednostki kontrolowane najczęściej z powodu błędnej interpretacji tych przepisów oraz ich niekonsekwentnego stosowania. Często przyczyną, w szczególności w przypadku szkół oraz spółdzielni mieszkaniowych, był również brak odpowiednich środków finansowych niezbędnych do pokrycia kosztów związanych z wdrożeniem rozwiązań zapewniających prawidłowe spełnienie wymogów. W niektórych przypadkach przyczyny powyższego stanu rzeczy wynikały jednak nie tylko z braku odpowiednich środków finansowych, ale także z niewłaściwego podejścia osób odpowiedzialnych za przetwarzanie danych osobowych do problematyki ochrony danych, a nawet z lekceważenia tych przepisów. Świadczy o tym w szczególności niewykonywanie 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 trakcie kontroli uchybienia były usuwane przez jednostki kontrolowane w toku postępowania. Natomiast do nielicznych należały sytuacje składania przez te jednostki wniosków o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora oraz zaskarżania decyzji GODO do Wojewódzkiego Sądu Administracyjnego w Warszawie lub Naczelnego Sądu Administracyjnego.

W roku 2008 do Wojewódzkiego Sądu Administracyjnego oraz Naczelnego Sądu Administracyjnego skierowanych zostało **8 skarg** w związku z przeprowadzonymi kontrolami.

Na podstawie ustaleń z kontroli przeprowadzonych w 2008 r. należy stwierdzić, że w porównaniu z latami ubiegłymi osoby odpowiedzialne za przetwarzanie danych osobowych wykazały większą świadomość zagrożeń związanych z ochroną danych osobowych, a tym samym świadomość konieczności zapewnienia odpowiednich środków organizacyjnych i technicznych. Konsekwencją było większe wyczulenie na prawidłowe dopełnienie obowiązków wynikających z przepisów o ochronie danych osobowych, co oczywiście nie oznacza, że obowiązki te zostały wykonane w sposób właściwy. Niestety, powyższe spostrzeżenia nie dotyczą wszystkich podmiotów, w których przeprowadzono kontrole. Zdarzały się bowiem kontrole, które wykazywały, że jednostki kontrolowane nie wykonywały większości obowiązków wynikających z przepisów o ochronie danych osobowych.

W porównaniu z poprzednimi latami, w 2008 r. daje się zauważyć wzrost liczby **skarg**, które wpłynęły do Biura GODO.



Wykres 35.
Zestawienie porównawcze liczby skarg, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2006 - 2008.

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.

Z treści rozpatrywanych w 2008 r. skarg można było wskazać na nowe zagadnienie - pozyskiwanie przez pracodawców od związków zawodowych imiennych list ich członków. W ocenie organu, żądanie takich informacji w odniesieniu do wszystkich pracowników korzystających z ochrony danego związku zawodowego w sytuacji, gdy nie są oni objęci zamiarem pracodawcy rozwiązania z nimi umów o pracę, jest bezpodstawne. Przepisy bowiem art. 30 ust. 2¹ ustawy o związkach zawodowych oraz art. 23² Kodeksu pracy, nie upoważniają pracodawcy do pozyskiwania od związku zawodowego za pomocą imiennej listy pracowników, danych osobowych wszystkich pracowników korzystających z ochrony tego związku. Zwłaszcza w sytuacji, gdy nie wszystkim tym osobom pracodawca zamierza wypowiedzieć czy też rozwiązać bez wypowiedzenia umowy o pracę. W jednej ze spraw pracodawca zakwestionował takie stanowisko i skierował do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na decyzję Generalnego Inspektora Ochrony Danych Osobowych. Jednak nie zapadło jeszcze w tej materii orzeczenie sądu administracyjnego.

Kolejny problem dotyczący przetwarzania danych osobowych przez pracodawców był ściśle związany z rozwojem nowych technologii. Podmioty z tego sektora przejawiały tendencję pozyskiwania danych w szerszym zakresie niż zezwalają na to przepisy prawa pracy. Chodzi tu, na przykład, o dane biometryczne typu odcisk palca. Tymczasem wielu pracowników przejawia negatywny stosunek do tego typu rozwiązań proponowanych przez pracodawcę.

Na uwagę zasługuje również rozstrzygnięta przez Wojewódzki Sąd Administracyjny w Warszawie sprawa przetwarzania danych osobowych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczyły, dla celów stosowania metod statystycznych przez Biuro Informacji Kredytowej S.A. W ocenie sądu art. 105a ust. 4 Prawa bankowego stanowi samodzielną podstawę takiego przetwarzania. Konsekwencją powyższego orzeczenia było uznanie Biura Informacji Kredytowej S.A. za administratora danych przez nie przetwarzanych. Przed wydaniem wspomnianego wyroku zagadnienie to budziło wiele wątpliwości.

Wojewódzki Sąd Administracyjny w Warszawie rozpatrzył również sprawę udostępniania przez operatora telekomunikacyjnego numerów telefonów abonentów prywatnych dobieranych pod kątem potrzeb nabywcy, np. według kryterium geograficznego. Przede wszystkim sąd stwierdził, że taki zestaw informacji stanowi dane osobowe w rozumieniu ustawy. Natomiast zgoda na umieszczenie danych w powszechnie dostępnych spisach abonentów nie może być utożsamiana ze zgodą na udostępnienie danych w celach marketingowych innym podmiotom. Stanowisko to zostało podzielone również przez Naczelny Sąd Administracyjny.

W znacznej liczbie skarg sygnalizowany był problem nielegalnego upubliczniania danych osobowych przez podmioty z sektora publicznego na stronach internetowych Biuletynu Informacji Publicznej. Realizując ustawowe obowiązki wynikające z ujawniania informacji publicznych, podmioty te często publikowały informacje zawierające dane osobowe w zbyt szerokim zakresie, tj. w zakresie niewymagany przepisami prawa. Wspomniane przypadki dotyczyły np. ujawniania oświadczeń majątkowych funkcjonariuszy publicznych wraz z zawartymi w nich informacjami o adresie zamieszkania, ewentualnie adresach nieruchomości stanowiących własność osoby, której oświadczenie dotyczyło.

Nierzadko Generalny Inspektor Ochrony Danych Osobowych był również informowany o ujawnianiu w sposób sprzeczny z ustawą o ochronie danych osobowych treści uchwał podejmowanych przez rady gminy. Chodziło o przypadki publikowania na stronach internetowych urzędów gmin informacji zawierających dane osobowe wnioskodawców (imię i nazwisko oraz adres zamieszkania). Generalny Inspektor Ochrony Danych Osobowych kwestionował w tych przypadkach zakres ujawnionych danych twierdząc, że dla spełnienia obowiązku informacyjnego wynikającego z ustawy o dostępie do informacji publicznej zbędne jest udostępnianie danych pozwalających na pełną identyfikację osób, których dotyczy uchwała, tj. imienia i nazwiska (w pewnych sytuacjach adresu zamieszkania), jako godzących w ich prawo do prywatności oraz nieadekwatnych do celu, jakemu służy upublicznienie uchwały. Wojewódzki Sąd Administracyjny w Warszawie potwierdził słuszność stanowiska Generalnego Inspektora Ochrony Danych Osobowych stwierdzając, iż usunięcie personaliów osób prywatnych czy też ich zanonimizowanie w ogłoszonej w Biuletynie Informacji Publicznej uchwale organu gminnego, nie wpływa na czytelność dokonanego w ten sposób przekazu, ponieważ akt taki nie traci waloru informacyjnego.

Dodać należy, że podmioty publiczne (najczęściej organy samorządowe) nadal wskazują przepisy ustawy o ochronie danych osobowych jako podstawę odmowy udzielania petentom wielu informacji o charakterze publicznym. Tego typu sytuacje są

wskazaniem dla GODO do przeprowadzenia działań edukacyjnych z udziałem pracowników tych podmiotów. Z drugiej strony, zwiększyła się bowiem również liczba przypadków upubliczniania przez wspomniane podmioty danych osobowych bez podstawy prawnej w imię błędnie postrzeganej transparentności życia publicznego, w tym działalności organów publicznych.

W analizowanym roku 2008 wzrosła także liczba skarg dotyczących odmowy udostępnienia przez wydawców gazet danych osobowych dziennikarzy niezbędnych do wystąpienia przez wnioskodawcę z powództwem cywilnym przeciwko tym osobom w związku z naruszeniem dóbr osobistych publikacją prasową. W większości tego typu wniosków, po analizie okoliczności faktycznych i prawnych, Generalny Inspektor Ochrony Danych Osobowych nakazywał udostępnienie danych pod warunkiem, że wniosek o udostępnienie danych wypełniał dyspozycję art. 29 ust. 2 i art. 30 ustawy o ochronie danych osobowych oraz nie zachodziły negatywne przesłanki zastosowania tych przepisów. Trzeba podkreślić, iż możliwość dochodzenia praw przed sądem nie jest wartością mniejszą niż prawo do ochrony danych osobowych.

Na niezmienionym w stosunku do lat ubiegłych poziomie pod względem liczby skarg utrzymał się problem niewłaściwego zabezpieczenia danych osobowych zarówno przez podmioty z sektora publicznego, jak i prywatnego. W większości przypadków, podobnie jak w poprzednich okresach sprawozdawczych, przyczyną naruszeń przepisów w tym zakresie było nie tylko niedostateczne techniczne zabezpieczenie przetwarzania danych, ale ignorowanie bądź błędne interpretowanie przepisów dotyczących ochrony danych osobowych przez pracowników zatrudnionych bezpośrednio przy ich przetwarzaniu. Skutkiem tego rodzaju działań było najczęściej ujawnianie danych osobowych osobie nieuprawnionej. W takich przypadkach organ korzystał ze swojej ustawowej kompetencji występowania do administratorów danych z wnioskami o wszczęcie postępowań dyscyplinarnych wobec osób odpowiedzialnych za sprzeczne z przepisami prawa przetwarzanie danych osobowych oraz występował z sygnalizacjami, których celem było zapewnienie lepszego poziomu ich ochrony przez administratora.

Odnotować należy również, że na skutek rozstrzygnięć zapadłych przed sądami administracyjnymi zmalała liczba skarg dotyczących udostępnienia danych podmiotom trzecim w związku z dochodzeniem roszczeń pieniężnych (na podstawie cesji wierzytelności lub zlecenia prowadzenia postępowania windykacyjnego). Jednakże nadal pojawiał się problem utożsamiania powierzenia przetwarzania danych na podstawie art. 31 ustawy z nielegalnym udostępnieniem danych.

W dalszym ciągu Generalny Inspektor Ochrony Danych Osobowych był adresatem skarg dotyczących niespełnienia, albo spełnienia w ograniczonym zakresie, bądź po upływie ustawowego 30-dniowego terminu, obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych. Analiza tych skarg doprowadziła do wniosku, że podobnie jak w latach ubiegłych administratorzy danych ignorowali (nie wypełniali) wspomnianego obowiązku informacyjnego bądź realizowali go w sposób niedbały, świadczący o dużym stopniu lekceważenia ustawowych regulacji dotyczących analizowanej problematyki. W takich sprawach Generalny Inspektor Ochrony Danych Osobowych konsekwentnie wydawał decyzje nakazujące spełnienie obowiązku informacyjnego. Odnosząc się do kwestii spełnienia obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych nie sposób pominąć orzeczenia (nieprawomocnego) Wojewódzkiego Sądu Administracyjnego w Warszawie rozstrzygającego w sprawie uzależnienia realizacji tego uprawnienia kontrolnego od uiszczenia stosowanej opłaty na pokrycie kosztów związanych z dostępem do danych osobowych (chodzi o koszty przesyłki). Sąd, oddalając skargę na decyzję Generalnego Inspektora Ochrony Danych Osobowych stwierdził, iż administrator danych nie ma prawa do pobierania takiej opłaty, chyba że osoba uprawniona zwraca się z wnioskiem o udzielenie informacji częściej niż co 6 miesięcy.

W podsumowaniu należy stwierdzić, że przyczyn wzrostu liczby skarg, które wpłynęły do GODO w analizowanym okresie 2008 r. należy upatrywać przede wszystkim we wzroście świadomości społeczeństwa co do zasad ochrony danych osobowych i jego aktywności w dochodzeniu przysługujących mu praw.

W odniesieniu do **zawiadomień o podejrzeniu popełnienia przestępstwa** kierowanych przez GODO 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 powołując art. 17 § 1 pkt. 2 i 3 Kodeksu postępowania karnego. W uzasadnieniu wskazywano, 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 jak w latach poprzednich, organy ścigania wykazywały się nieznajomością przepisów o ochronie danych osobowych oraz bezzasadną oceną przypadków złamania tej ustawy, jako

czynów o znikomej społecznej szkodliwości. Jednocześnie trzeba zaznaczyć, iż pojawiła się nowa przyczyna umarzania postępowań przez organy ścigania – przedawnienie karalności (art. 17 § 1 pkt 6 Kodeksu postępowania karnego). W kontekście powyższego jednym z priorytetów Generalnego Inspektora Ochrony Danych Osobowych, obok prowadzenia działalności edukacyjnej oraz propagującej zasady ochrony danych osobowych nie tylko wśród „zwykłych” obywateli, ale również wśród podmiotów te dane przetwarzających, było spowodowanie poprzez wystąpienia do Ministra Sprawiedliwości Prokuratora Generalnego, zmiany postrzegania przez podległych mu prokuratorów, spraw z zakresu ochrony danych osobowych jako spraw błahych i mało ważnych. Zadanie to jest o tyle ważne, że coraz powszechniejsze jest zjawisko niekontrolowanego handlu na masową skalę bazami danych osobowych zgromadzonych i przetwarzanych w sposób sprzeczny z ustawą o ochronie danych osobowych.

Z kolei analiza **projektów aktów normatywnych** przesyłanych w 2008 r. do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych 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.

Podsumowując uchybienia dostrzeżone w projektach aktów prawnych przesyłanych Generalnemu Inspektorowi do zaopiniowania należy wskazać, że większość z nich dotyczyła 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. Niemniej należy w tym miejscu bezwzględnie podkreślić istnienie zauważalnej tendencji 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.

Na arenie międzynarodowej należy odnotować wciąż aktywny udział Generalnego Inspektora w procesie utrwalania 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 [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 Generalnego Inspektora w 2008 roku było zorganizowanie w Polsce 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.

W 2008 r. do Generalnego Inspektora wpłynęło 28 wniosków o **udzielenie zgody na przekazanie danych osobowych do państwa trzeciego**. Generalny Inspektor jest uprawniony do udzielenia zgody na przekazanie danych osobowych do państwa trzeciego, pod warunkiem zapewnienia przez administratora danych odpowiedniego zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. Można to osiągnąć przede wszystkim poprzez przyjęcie odpowiednich zobowiązań umownych, do których należy zaliczyć między innymi standardowe klauzule umowne przyjęte przez

Komisję Europejską⁴²³ oraz wiążące reguły korporacyjne.⁴²⁴ Trzeba jednak podkreślić, że znaczna liczba międzynarodowych transferów danych odbywa się w ramach Europejskiego Obszaru Gospodarczego i nie ma wtedy konieczności stosowania przepisów rozdziału 7 ustawy o ochronie danych osobowych, które regulują przekazywanie danych do państwa trzeciego. Ponadto administratorzy danych mogą również skorzystać z możliwości zastosowania innych przesłanek upoważniających ich 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.

W omawianym okresie sprawozdawczym do Generalnego Inspektora Ochrony Danych Osobowych wpływały jedynie wnioski, w których administratorzy danych powoływali się na zastosowanie wspomnianych standardowych klauzul umownych, ustanowionych przez Komisję Europejską. Rozwiązanie to jest preferowane przez większość organów ochrony danych osobowych w Europie. Administratorzy danych nie korzystali natomiast z innych rozwiązań umownych. Należy zauważyć, że choć Generalny Inspektor uczestniczył w kilku procedurach koordynacyjnych mających na celu wypracowanie przez międzynarodowe korporacje wiążących reguł korporacyjnych, to nie stały się one jeszcze podstawą formalnych wniosków o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego. 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 badał również okoliczności planowanych transferów danych, w tym również przyjęte przez odbiorcę danych organizacyjne i techniczne środki zabezpieczeń. Podkreślenia wymaga, że do najczęstszych braków wskazywanych w toku postępowania wyjaśniającego należały kwestie dotyczące spełnienia wymogów bezpieczeństwa danych osobowych. Należy również zauważyć przypadki, w których w toku postępowania o wyrażenie zgody na przekazanie danych do państwa trzeciego pojawiały się poważne wątpliwości, co do spełnienia przez wnioskodawcę wymogów ustawy o ochronie danych osobowych w odniesieniu do przetwarzania danych osobowych na terytorium RP.

Warta odnotowania jest również coraz częstsza praktyka przygotowywania wniosków o wyrażenie zgody przez Generalnego Inspektora w imieniu administratorów danych mających siedzibę na terytorium RP przez zagraniczne spółki matki, co niekiedy wiązało się z niedopełnieniem wymogów formalnych we wnioskach, spowodowane brakiem wiedzy o polskim systemie prawa.

W roku sprawozdawczym 2008, GODO wydał 12 decyzji w sprawach o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego (załącznik 7).

W 2008 roku wśród **zgłoszeń do rejestracji** pochodzących od podmiotów publicznych dominowały zgłoszenia zbiorów danych osobowych prowadzonych w związku z przyznawaniem świadczeń alimentacyjnych. Było to spowodowane tym, że w dniu 1 października 2008 r. weszły w życie przepisy ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów,⁴²⁵ które wprowadziły zmiany zasad przyznawania świadczeń alimentacyjnych. Zmiana stanu prawnego znalazła zatem przełożenie na obowiązki administratorów danych. Administratorzy danych często zadawali pytania, co powinni zrobić ze zbiorami danych

⁴²³ 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. U. 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.

⁴²⁴ 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.

prowadzonych na podstawie przepisów ustawy z dnia 22 kwietnia 2005 roku o postępowaniu wobec dłużników alimentacyjnych oraz zaliczce alimentacyjnej.⁴²⁶ Niektórzy administratorzy występowali nawet z wnioskiem o wykreślenie tych zbiorów danych z rejestru.⁴²⁷

Należy zwrócić uwagę, iż zgodnie z przepisami ustawy o pomocy osobom uprawnionym do alimentów, utrata mocy obowiązującej przepisów ustawy o postępowaniu wobec dłużników alimentacyjnych oraz zaliczce alimentacyjnej nie jest równoznaczna z zakończeniem zadań dotyczących zaliczek alimentacyjnych. Zgodnie z postanowieniami ustawy o pomocy osobom uprawnionym do alimentów, sprawy o zaliczki alimentacyjne podlegają rozpatrzeniu na zasadach i w trybie określonym w przepisach dotychczasowych.⁴²⁸

Przepisy ustawy o postępowaniu wobec dłużników alimentacyjnych oraz zaliczce alimentacyjnej znajdują więc w niektórych przypadkach zastosowanie również po wejściu w życie ustawy o pomocy osobom uprawnionym do alimentów. Oznacza to, iż zbiory danych osobowych prowadzone dotychczas na podstawie ustawy o postępowaniu wobec dłużników alimentacyjnych oraz zaliczce alimentacyjnej będą w dalszym ciągu wykorzystywane, a dane osobowe zgromadzone w tych zbiorach będą nadal przetwarzane dla potrzeb prowadzonych postępowań. Natomiast dane pozyskiwane w celu realizacji ustawy o pomocy osobom uprawnionym do alimentów mogą być przetwarzane w prowadzonym dotychczas zbiorze albo w zbiorze odrębnie utworzonym. O utworzeniu nowego zbioru bądź o zmianie struktury dotychczasowego zbioru decyduje administrator danych biorąc pod uwagę stan faktyczny i prawny.

Zatem w zależności od przyjętego rozwiązania dopuszczalne są dwa alternatywne zgłoszenia. Administrator danych może, w trybie art. 41 ust. 2 ustawy, zaktualizować zbiór danych prowadzony na podstawie ustawy o postępowaniu wobec dłużników alimentacyjnych oraz zaliczce alimentacyjnej, informując o dokonanych zmianach (m.in. w zakresie podstawy prawnej upoważniającej do prowadzenia zbioru), lub zgłosić nowy zbiór danych prowadzony na podstawie ustawy o pomocy osobom uprawnionym do alimentów.

Jak wspomniano powyżej, w 2008 r. wśród wniosków o rejestrację pochodzących od podmiotów prywatnych dominowały zgłoszenia od przedsiębiorców, którzy przetwarzając dane osobowe, wykorzystują sieć Internet. Prowadzenie przez administratorów danych zbiorów przy użyciu narzędzi internetowych powoduje, iż ci właśnie administratorzy w sposób szczególny zobowiązani są do zapewnienia ochrony przetwarzanych przez nich danych osobowych. Specyfika sieci Internet powoduje bowiem, iż dane osobowe przetwarzane przy jej użyciu narażone są na wiele szkodliwych działań (np. udostępnienie osobom nieupoważnionym, uszkodzenie, zmianę, a nawet utratę). W okresie sprawozdawczym najwięcej zgłoszeń zbiorów danych osobowych do rejestracji, których prowadzenie było związane z funkcjonowaniem sieci Internet, dotyczyło:

- serwisów związanych z pośrednictwem w zatrudnieniu,
- serwisów randkowych,
- sklepów internetowych.

Podobnie jak w latach wcześniejszych, również w 2008 r. do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były zbiory danych dotyczących tzw. newsletterów. Przy ich pomocy wiele firm - administratorów danych - powiadamiało klientów o nowościach w swojej ofercie.

W roku 2008 Generalny Inspektor Ochrony Danych Osobowych opracował **projekt nowego wzoru zgłoszenia zbioru danych osobowych do rejestracji** będący załącznikiem do rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych,⁴²⁹ wydawanego

⁴²⁵ Dz. U. Nr 192, poz. 1378 z późn. zm.

⁴²⁶ Dz. U. Nr 86, poz. 732 z późn. zm.

⁴²⁷ R 004224/06.

⁴²⁸ Rozdział 7 ustawy o pomocy osobom uprawnionym do alimentów.

⁴²⁹ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (D.U. Nr 229, poz. 1536).

na podstawie art. 46a ustawy o ochronie danych osobowych. Akt ten wszedł w życie w dniu 10 lutego 2009 r. zastępując dotychczas obowiązujące rozporządzenie MSWiA z dnia 29 kwietnia 2004 roku.⁴³⁰

Potrzeba wprowadzenia nowego wzoru wynikała z oceny kilkuletniej praktyki stosowania dotychczasowego formularza zgłoszenia. W ocenie GODO, prawidłowe zgłoszenie zbioru do rejestracji sprawiało administratorom danych wiele trudności. Wnioskodawcy mieli najwięcej problemów z prawidłowym wypełnieniem części E zgłoszenia dotyczącej informacji o środkach technicznych i organizacyjnych zastosowanych w celu zabezpieczenia danych. Dotychczasowa część E wzoru zgłoszenia składała się z siedmiu punktów o charakterze opisowym, w których administratorzy podawali informacje o poszczególnych rodzajach zastosowanych środków zabezpieczających dane zgromadzone w zbiorze. Administratorzy danych, wypełniając tę część zgłoszenia, podawali często wiele informacji związanych z zabezpieczeniem zbiorów nie zawsze istotnych z punktu widzenia spełnienia wymogów ustawowych. Nie podawali natomiast informacji o zabezpieczeniach wymaganych wprost przepisami ustawy. Należy podkreślić, że stwierdzenie powyższych nieprawidłowości w zgłoszeniu niejednokrotnie obligowało Generalnego Inspektora Ochrony Danych Osobowych do wydawania decyzji o odmowie rejestracji zbioru danych. Wraz z odmową rejestracji Generalny Inspektor mógł również nakazać ograniczenie przetwarzania danych lub ich usunięcie ze zbioru. Skutki błędnego wypełnienia formularza zgłoszenia mogły więc mieć negatywny wpływ na całą działalność wnioskodawcy, często wręcz uniemożliwiając jej kontynuowanie.

W nowym wzorze zgłoszenia opisowe punkty zostały zastąpione polami wyboru, poprzez zaznaczenie których wnioskodawca będzie składał oświadczenie o spełnieniu konkretnych wymogów ustawowych w zakresie zabezpieczeń. Ponadto w tej części zgłoszenia został dodany jeden punkt o charakterze opisowym, w którym wnioskodawca będzie miał możliwość podania informacji o innych środkach zabezpieczeń, niewynikających wprost z ustawy, zastosowanych w celu zabezpieczenia danych. Zatem w części E wnioskodawca będzie zobligowany do podania informacji o zabezpieczeniach wprost wynikających z ustawy o ochronie danych osobowych, ale także będzie miał możliwość podania innych, istotnych, jego zdaniem, informacji charakteryzujących system zabezpieczeń.

Głównym celem modyfikacji wzoru zgłoszenia było zatem uporządkowanie i zwiększenie transparentności części E formularza zgłoszenia dotyczącej informacji o środkach technicznych i organizacyjnych zastosowanych w celu zabezpieczenia danych. Zasadniczym celem tych zmian było uproszczenie procedury zgłoszenia i wyeksponowanie zasadniczych obowiązków administratora danych w zakresie ich zabezpieczenia.

Ponadto w stosunku do obowiązującego wzoru zgłoszenia dokonano zmiany w części D wzoru - sposób zbierania oraz udostępnianie danych - poprzez ograniczenie w pkt 11 zgłoszenia sposobu zbierania danych do wskazania, czy dane będą pozyskiwane od osób, których dotyczą, czy też z innych źródeł. Natomiast w punkcie 12 ograniczono krąg podmiotów, którym dane ze zbioru będą udostępniane do podmiotów innych niż uprawnione na podstawie przepisów prawa.

Wprowadzenie nowego wzoru zgłoszenia niewątpliwie pomoże administratorom danych, szczególnie drobnym przedsiębiorcom niedysponującym profesjonalną obsługą prawną, w prawidłowym wypełnieniu ustawowego obowiązku. Zastosowanie nowego wzoru zgłoszenia powinno spowodować zmniejszenie liczby nieprawidłowo wypełnionych zgłoszeń, skutkujących koniecznością przeprowadzenia postępowania wyjaśniającego, co przedłuża proces rejestracji zbioru. Jest to szczególnie istotne obecnie, gdy - w związku z prowadzoną przez Generalnego Inspektora Ochrony Danych Osobowych zintensyfikowaną działalnością edukacyjną i informacyjną - wzrasta świadomość przedsiębiorców w kwestii zasad ochrony danych osobowych i obowiązków związanych z ich realizacją. W szczególności zaś obowiązku rejestracji prowadzonych zbiorów danych, co przekłada się na zwiększenie liczby wpływających zgłoszeń.

Aby ułatwić prawidłowe zgłaszanie zbiorów danych do rejestracji, w 2008 r. dokonano również modyfikacji programu komputerowego służącego do wypełnienia zgłoszenia, udostępnionego na stronie internetowej GODO. Program ten, wraz z internetową wersją rejestru zbiorów danych osobowych, funkcjonuje w ramach systemu „Elektroniczna platforma komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych”, tzw. e-GODO. Został on opracowany w celu minimalizacji błędów

⁴³⁰ Dz. U. Nr 100, poz. 1025.

popelnianych przez wnioskodawców przy wypełnianiu formularza zgłoszenia. Modyfikacja programu wspomagającego wypełnienie formularza zgłoszenia polegała m.in. na tym, iż wnioskodawca może wysłać drogą elektroniczną zgłoszenie do rejestracji również wtedy, gdy nie dysponuje bezpiecznym podpisem elektronicznym. W takim przypadku należy opatrzyć wydruk zgłoszenia przesyłanego elektronicznie podpisem i pieczętą wnioskodawcy, a następnie przesłać pocztą lub złożyć w siedzibie GODO. Powyższa modyfikacja, oprócz ułatwienia dla administratorów danych, usprawni także proces rozpatrywania zgłoszeń. W roku 2008 Generalny Inspektor Ochrony Danych Osobowych wydał **420 decyzji administracyjnych** (w tym głównie decyzje o odmowie rejestracji zbioru danych oraz decyzje związane z uaktualnieniem rejestru zbiorów, tj. o wykreśleniu zbioru z rejestru z powodu zaprzestania przetwarzania danych). Zastosowane rozwiązania legislacyjne i techniczne powinny doprowadzić do zmniejszenia się liczby decyzji o odmowie rejestracji.

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. Przed Generalnym Inspektorem Ochrony Danych Osobowych w dalszym ciągu stoi zadanie aktywizowania administratorów danych, by dopełnili obowiązku rejestracyjnego.

Część IV.

Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych

Do ustawowego obowiązku Generalnego Inspektora Ochrony Danych Osobowych należy przedłożenie Sejmowi sprawozdania ze swej działalności. Przedstawiona w niniejszym Sprawozdaniu analiza skarg dotyczących naruszeń ochrony danych, wyników kontroli przeprowadzanych u administratorów danych, wydawanych opinii prawnych, przedsięwzięć legislacyjnych, orzecznictwa sądów administracyjnych, a także inne działania podjęte przez GODO w 2008 r. stanowią podstawę do sformułowania wniosków wynikających ze stanu przestrzegania przepisów o ochronie danych osobowych i określenia zadań na przyszłość.

Generalny Inspektor rozpoczął konsultacje dotyczące przepisów szczególnych względem ustawy o ochronie danych osobowych. Przykładowo w związku z niedostosowaniem obowiązujących przepisów prawa pracy do potrzeb pracodawców i pracowników w kontekście ochrony danych osobowych i prywatności, GODO zainicjował publiczną debatę na ten temat. W jej ramach Generalny Inspektor wraz z Kolegium Prawa Akademii Leona Koźmińskiego wspólnie zorganizowali w dniu 2 grudnia 2008 r. konferencję naukową pt. „Granice ochrony danych osobowych w stosunkach pracy”. Kolejnym krokiem było zwrócenie się w 2009 r. do organizacji pracodawców i pracowników, instytucji zajmujących się ochroną praw człowieka, a także reprezentantów świata nauki, z prośbą o opinie dotyczące kierunków koniecznych zmian obowiązujących w tym zakresie przepisów Kodeksu Pracy.

Istotnym elementem wpływającym na stan ochrony danych osobowych w Polsce jest proces legislacyjny na poziomie UE. W pierwszej kolejności należy zwrócić uwagę na konsekwencje wejścia w życie Traktatu z Lizbony na ochronę danych osobowych w Europie, do których należy zaliczyć m.in. rezygnację z podziału na filary UE, zwiększenie udziału Parlamentu Europejskiego w procesie ustawodawczym, czy wprowadzenie wyraźnych gwarancji ochrony danych osobowych.⁴³¹ Warto także odnotować przyjęcie w dniu 27 listopada 2008 r. decyzji ramowej Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.⁴³² Na stan ochrony danych osobowych mają

⁴³¹ Tematyka ta była przedmiotem referatu Generalnego Inspektora pt. „Ochrona danych w obszarze wolności, bezpieczeństwa i sprawiedliwości w świetle Traktatu z Lizbony”, wygłoszonego w trakcie Wiosennej Konferencji Europejskich Organów Ochrony Danych i Prywatności, która miała miejsce dniach 17-18 kwietnia 2008 r. w Rzymie. Tekst referatu jest dostępny na stronie internetowej: http://www.giodo.gov.pl/489/id_art/2116/j/pl/

⁴³² Dz. Urz. UE L 350/60 z 30. 12.2008 r. Decyzja będzie wymagała wdrożenia w polskim porządku prawnym do dnia 27 listopada 2010 r.

i będą miały wpływ w przyszłości prace nad europejskimi systemami wymiany informacji, do których należy np. System Informacyjny Schengen drugiej generacji. Wreszcie w najbliższych latach duże znaczenie będzie miał - zainicjowany przez Komisję Europejską - proces oceny przepisów dyrektywy 95/46/WE.

Generalny Inspektor w takim samym stopniu jak obecnie będzie uczestniczył w pracach nad projektami aktów prawnych Unii Europejskiej oraz aktów prawa krajowego. Na podkreślenie zasługuje również to, że biorąc udział w konsultacjach międzyresortowych dotyczących przygotowania stanowisk rządu RP w sprawie projektów aktów UE mających wpływ na ochronę danych osobowych, w sposób bezpośredni kształtuje jakość prawa dotyczącego ochrony danych.

Generalny Inspektor w ramach działalności międzynarodowej uczestniczy w różnych formach współpracy zarówno w I jak i III filarze Unii Europejskiej, biorąc udział w przygotowaniu wielu istotnych dla ochrony danych osobowych dokumentów dotyczących m.in. wyszukiwarek internetowych czy ochrony danych osobowych dzieci. Przeprowadza również inspekcje oraz inne czynności wyjaśniające w ramach skoordynowanych działań kontrolnych.

Priorytetowe znaczenie w działalności Generalnego Inspektora ma współpraca dwustronna oraz wielostronna z organami ochrony danych osobowych z państw Europy Środkowej i Wschodniej, czemu w szczególności służy zainicjowana przez GODO w 2001 r. współpraca w ramach Grupy Państw Europy Środkowej i Wschodniej. Na tym forum m.in. wytycza się kierunki przyszłych rozwiązań problemów dotyczących ochrony danych osobowych ze szczególnym uwzględnieniem specyfiki tego regionu oraz wymienia doświadczeniami dotyczącymi interpretacji i stosowania przepisów o ochronie danych osobowych.

Po dziesięciu latach obowiązywania ustawy o ochronie danych osobowych znajomość norm prawnych w tym obszarze jest w świadomości społecznej coraz powszechniejsza. Według wyników badań Eurobarometru⁴³³ opublikowanych na początku 2008 r. Rzeczpospolita Polska znalazła się na pierwszym miejscu wśród krajów Unii Europejskiej ze względu na deklarowaną przez 43% obywateli świadomość praw związanych z ochroną danych osobowych. 45% Polaków stwierdziło, że ich dane osobowe są należycie chronione.

Przynajmniej w części jest to efekt działań edukacyjnych prowadzonych przez Generalnego Inspektora. Analizując wyniki badań opinii publicznej należy pamiętać, że ustawa o ochronie danych osobowych powstawała w czasie, kiedy nie było jeszcze bankowości elektronicznej, podpisu elektronicznego, tworzenia profili behawioralnych czy znaczników identyfikacji radiowej RFID. Każde z tych rozwiązań technologicznych generuje nowe obszary zagrożeń dla prawa do prywatności i ochrony danych osobowych, wymuszając nie tylko konieczność opracowania odpowiednich uregulowań w celu zagwarantowania bezpieczeństwa dla tych praw, ale także działania na rzecz edukacji obywateli. Tymczasem – jak wynika z przeprowadzonych badań – świadomość Polaków co do zagrożeń dla ochrony danych osobowych nie idzie w parze ze stosowaniem przez nich odpowiednich zabezpieczeń. Tak więc o ochronę naszych danych osobowych powinny dbać w równym stopniu instytucje, którym je powierzamy, jak i sami obywatele. Dlatego przed organem ds. ochrony danych osobowych stoi bardzo ważne i wciąż aktualne wyzwanie – wykształcenie aktywnego, dobrze poinformowanego o zasadach ochrony danych społeczeństwa obywatelskiego. Chodzi tu nie tylko o dotarcie z informacją o zagrożeniach do szerokiego kręgu odbiorców, ale także skuteczne ich zaktywizowanie. Brak bowiem **osobistego zaangażowania obywateli** w ochronę ich własnych praw stanowi największe zagrożenie dla ochrony ich prywatności i danych osobowych.

Dlatego od 2007 r. adresatem działań edukacyjnych podejmowanych przez GODO byli zarówno najmłodsi obywatele – uczniowie szkół podstawowych, dla których zorganizował dwie edycje konkursu plastycznego (II edycja zorganizowana w 2008 r. miała tytuł „Ochrona danych osobowych w świecie bez granic – Schengen”) - jak i słuchacze szkół wyższych. Dzięki jego inicjatywie w Akademii Leona Koźmińskiego w Warszawie powstało w 2008 r. dwusemestralne podyplomowe studium z zakresu ochrony danych osobowych. Od dwóch lat promuje prace magisterskie, licencjackie i inne opracowania o tematyce związanej z danymi osobowymi. Rozpoczął II edycję broszur z cyklu ABC ochrony danych osobowych, odnoszących się do takich zagadnień, jak przetwarzanie danych osobowych w sektorze bankowym, medycznym, ubezpieczeniowym, telekomunikacyjnym

⁴³³ Sondaże Eurobarometru, ośrodka badań opinii publicznej prowadzonych na zlecenie Komisji Europejskiej, przeprowadzane są regularnie we wszystkich państwach Unii Europejskiej, krajach kandydujących, a także na terytorium Cypru Północnego. Ich wyniki publikowane są w postaci ogólnodostępnych raportów.

i marketingowym, a także bezpieczeństwa danych osobowych w sieci. Należy nadmienić, że ze względu na brak wystarczających środków finansowych działania wydawnicze prowadzone są we współpracy z podmiotami spoza administracji publicznej. GODO kontynuuje organizację cyklicznych szkoleń dla przedstawicieli kluczowych jednostek administracji publicznej, izb i samorządów zawodowych wszystkich sektorów, a także pracowników wymiaru sprawiedliwości. Zamierzeniem organu ds. ochrony danych osobowych jest bowiem zaktywizowanie danego środowiska do samodzielnego podejmowania działań na rzecz ochrony danych. Przykładem może być porozumienie zawarte w 2008 r. pomiędzy GODO a Stowarzyszeniem Marketingu Bezpośredniego ***o wspólnym działaniu na rzecz poprawy poziomu ochrony danych osobowych i prawa do prywatności w działalności marketingowej oraz stosowaniu Kodeksu Dobrych Praktyk***. Rezultatem szeroko zakrojonej działalności edukacyjnej było też wznowienie współpracy Generalnego Inspektora Ochrony Danych Osobowych z Polską Izbą Ubezpieczeń w obszarze wspólnych działań legislacyjnych i edukacyjnych, w tym nad wypracowaniem Kodeksu Dobrych Praktyk w zakresie przetwarzania danych osobowych w tym sektorze.

W tym miejscu należy też wspomnieć o uruchomionym w 2008 r. nowym źródle informacji o ochronie danych osobowych, jakim jest portal edukacyjno – informacyjny eduGODO.

Przedstawioną w Sprawozdaniu aktywność GODO na forum krajowym i międzynarodowym należy wiązać z postępującym procesem globalizacji gospodarki światowej i rozwojem nowych technologii. Wymusza to na organie ds. ochrony danych konieczność przeprowadzania analiz tych procesów i związanych z nimi nowych rozwiązań technologicznych, ponieważ mają one ogromny wpływ na stosowanie ustawy o ochronie danych osobowych (np. numer IP). Pamiętać bowiem należy, że w świetle nowatorskich rozwiązań technologicznych coraz więcej informacji, które do tej pory nie miały charakteru danych osobowych, dzięki tym technologiom i w powiązaniu z innymi informacjami stają się danymi osobowymi w rozumieniu ustawy.

Dlatego istotą propagowania idei ochrony danych osobowych jest zapobieganie powstawaniu zagrożeń płynących z rozwoju nowoczesnych technologii, które należy traktować instrumentalnie, jako środki, a nie cel sam w sobie. Mają one służyć człowiekowi i wspomagać jego działanie, a nie – być użyte przeciwko niemu. W centrum wysiłków podejmowanych dla ochrony prywatności i danych osobowych zawsze musi być człowiek, z jego podstawowymi prawami i godnością. Wobec tego równolegle z poszerzaniem działalności edukacyjnej organu w tym obszarze, powinno iść w parze budowanie odpowiednich relacji między obywatelami a instytucjami publicznymi w kwestii praw i obowiązków wynikających ze stosowania ustawy o ochronie danych osobowych. Zadania te – obok innych, wskazanych przez ustawodawcę w art. 12 - wymagają szeregu długofalowych przedsięwzięć i związanych z ich realizacją nakładów finansowych.

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych
w roku 2008 o charakterze generalnym do centralnych organów państwa
i do innych podmiotów z sektora publicznego**

L.p.	Nazwa podmiotu	Data wystąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	Pan Sylwester Chruszcz Poseł do PE	8.01.2008 r. DOLiS-035-47/07/330/08	Wystąpienie dotyczące wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych pozyskiwanych za pomocą formularza amieszczonego na stronie internetowej www.chruszcz.pl
2.	Prezes Urzędu Komunikacji Elektronicznej	23.01.2008 r. DOLiS-035-23/08/1724/08	Wskazanie, że zgoda osoby, której dane dotyczą, jest oświadczeniem woli składającego oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
3.	Minister Sprawiedliwości	29.02.2008 r. GI-DS-430/335/06/5416/08/DOLiS	Zasygnalizowanie wątpliwości odnośnie sposobu prowadzenia przez podległe Ministrowi Sprawiedliwości jednostki prokuratury, niektórych postępowań w sprawach z zakresu ochrony danych osobowych.
4.	Wójt Gminy Lipowa	11.03.2008 r. DOLiS-440-32/08/6424	Wystąpienie w sprawie wyeliminowania praktyki ujawniania na stronie internetowej Biuletynu Informacji Publicznej oświadczeń majątkowych przewodniczącego Rady Gminy Lipowa i Wójta Gminy Lipowa oraz oświadczeń majątkowych kierowników jednostek organizacyjnych oraz radnych Gminy Lipowa w całości.
5.	Wójt Gminy Lipnica	28.03.2008 r. DOLiS-035-331/08/7955/08	Wystąpienie o zmianę praktyki ujawniania w Biuletynie Informacji Publicznej oraz na tablicach ogłoszeń w siedzibie Urzędu Gminy, szerszego niż wynikający z przepisów prawa zakresu danych osobowych osób, które wygrały przetarg na zakup nieruchomości.
6.	Minister Sprawiedliwości	28.03.2008 r. DOLiS-035-475/08/7906/08	Wystąpienie z prośbą o dokonanie oceny praktyki kancelarii komorniczych, polegającej na wysyłaniu do pracodawców informacji o zajęciu wynagrodzenia za pracę dłużników, bez wstępnego sprawdzenia, czy dana osoba rzeczywiście jest zatrudniona u pracodawcy, do którego zajęcie zostało skierowane.
7.	Przewodniczący Rady Miasta Szczecina	14.04.2008 r. DOLiS-035-163/08/9561	Poinformowanie, iż zamieszczanie w uchwałach Rady Miasta Szczecina informacji o adresie zamieszkania osób, których uchwały dotyczą, pozostaje w sprzeczności z ustawą o ochronie danych osobowych.
8.	Prezydent Bydgoszczy	18.04.2008 r. DOLiS-035-468/08/10045	Wystąpienie o realizację obowiązku informacyjnego z art. 24 ust. 1 ustawy o ochronie danych osobowych, przy prowadzeniu rejestracji dzieci do przedszkoli za pośrednictwem strony internetowej.
9.	Dyrektor Izby Celnej w Katowicach	29.04.2008 r. DOLiS-440-245/08/11096	Wystąpienie o zmianę praktyki pozyskiwania w treści „protokołu przesłuchania jako osoby podejrzanej o popełnienie wykroczenia”, danych o karalności oraz o stanie zdrowia psychicznego.
10.	Dyrektor Zespołu Szkół nr 2 z Oddziałami Integracyjnymi w Brzegu	30.04.2008 r. DOLiS-440-109/08/11307	Wystąpienie o nieudostępnianie Poradni Neurologicznej NZOZ, danych osobowych ucznia szkoły, bez zgody jego przedstawiciela ustawowego.

11.	Wojewoda Warmińsko-Mazurski	19.05.2008 r. GI-DS- 430/344/05/12581/08/DOLiS	Wystąpienie o podjęcie działań w celu wyeliminowania praktyki udostępniania Dyrektorowi Zakładu Obsługi Szkół, przez Rzecznika Dyscyplinarnego dla Nauczycieli przy Wojewodzie Warmińsko-Mazurskim, informacji o ukaraniu dyscyplinarnym nauczyciela bez podstawy prawnej.
12.	Przewodniczący Rady Miejskiej w Goleniowie	28.05.2008 r. DOLiS-035-570/08/13372	Wystąpienie o zmianę uchwały Rady Miejskiej jako naruszającej ustawę o ochronie danych osobowych oraz o zapewnienie zgodności z jej przepisami, konstruowanego w przyszłości przez Radę Miejską w Goleniowie prawa miejscowego.
13.	Minister Sprawiedliwości	5.06.2008 r. DOLiS-440-208/08/14114	Wystąpienie o spowodowanie zmian w praktyce stosowanej przez prokuratury, polegającej na wpisywaniu na stronie adresowej kopert, informacji o treści pisma (postanowienia, zawiadomienia), jako niezgodnej z przepisami ustawy o ochronie danych osobowych.
14.	Komendant Główny Policji	11.06.2008 r. DOLiS-035-748/08/14747	Wystąpienie o zaprzestanie upubliczniania na stronie internetowej www.policja.pl , wizerunku roznieglizowanych osób, jako że działanie to narusza sferę prywatności tych osób.
15.	Mazowiecki Kurator Oświaty w Warszawie	17.06.2008 r. DIS-K-421/47/08	Podjęcie działań mających na celu wyeliminowanie nieprawidłowości związanych z prowadzeniem przez Gimnazjum nr 1 im. Powstańców Warszawy w Piasecznie, dokumentacji dotyczącej przebiegu nauczania.
16.	Minister Sprawiedliwości	24.07.2008 r. DOLiS-035-916/08/18982	Wystąpienie z informacją, iż w obowiązującym stanie prawnym, brak jest podstaw do wdrożenia w sądach powszechnych wokand internetowych.
17.	Minister Spraw Wewnętrznych i Administracji	30.07.2008 r. GI-DS.-430/16/06/19451/08/DOLiS	Wystąpienie o rozważenie zasadności podjęcia działań legislacyjnych mających na celu nowelizację ustawy o ochronie danych osobowych.
18.	Komendant Wojewódzkiej Policji w Szczecinie	4.08.2008 r. DOLiS-440-429/08/19950	Wystąpienie o niezwłoczne wyeliminowanie praktyki udostępniania informacji o stanie zdrowia, podległych Komendantowi Wojewódzkiemu funkcjonariuszy Policji, innym podległym funkcjonariuszom bądź pracownikom Policji oraz innym osobom i podmiotom trzecim.
19.	Dyrektor Miejskiego Ośrodka Pomocy Rodzinie w Kielcach	4.08.2008 r. DOLiS-035-920/08/19952/08	Wystąpienie w sprawie podjęcia działań w celu zabezpieczenia danych osobowych przetwarzanych przez pracowników MOPR w trakcie obsługi interesantów.
20.	Komendant Miejskiej Policji w Krakowie	7.08.2008 r. DOLiS-440-366/08/20354	Wystąpienie o zmianę praktyki doręczania pism przeznaczonych dla uczestników postępowania, poprzez pozostawianie ich w drzwiach mieszkań osób, do których są kierowane.
21.	Główny Inspektor Pracy	11.08.2008 r. DOLiS-440-121/08/20776	Wystąpienie o zmianę praktyki pozyskiwania danych osobowych podległych GIP inspektorów pracy, w związku z podejmowaniem przez nich dodatkowych zajęć zarobkowych.
22.	Minister Zdrowia	13.08.2008 r. DOLiS-035-500/08/21090	Wystąpienie z prośbą o podjęcie działań legislacyjnych mających na celu zmianę brzmienia art. 20 ust. 2 pkt 3 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, jako sprzecznego z ustawą o ochronie danych osobowych.
23.	Prokurator Okręgowy w Szczecinie	14.08.2008 r. DOLiS-440-73/08/21182	Wystąpienie w sprawie wyeliminowania praktyki udostępniania danych osobowych utrwalonych w aktach postępowań, w sytuacji braku podstaw prawnych.

24.	Dyrektor Powiatowego Urzędu Pracy w Białymstoku	25.08.2008 r. DOLiS-035-1051/08/21975	Wystąpienie o zaprzestanie praktyki zatrzymywania dowodu tożsamości, w sytuacji pobierania klucza do toalety przez klientów tego urzędu.
25.	Minister Edukacji Narodowej	08.09.2008 r. DIS-K-421/47/08	Podjęcie działań mających na celu dostosowanie systemu informatycznego, o którym mowa w art. 5 ustawy z dnia 19 lutego 2004 r. o systemie informacji oświatowej (Dz. U. Nr 49, poz. 463 z późn. zm.) oraz systemu informatycznego wykorzystywanego przez szkoły w celu określonym w § 41 ust. 1 pkt 1 i § 63 ust. 8 rozporządzenia Ministra Edukacji Narodowej z dnia 30 kwietnia 2007 r. w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów i słuchaczy oraz przeprowadzania sprawdzianów i egzaminów w szkołach publicznych (Dz. U. Nr 83, poz. 562 z późn. zm.), do wymogów określonych w przepisach o ochronie danych osobowych.
26.	Burmistrz Rogoźna	24.09.2008 r. DOLiS-440-495/08/25095	Wystąpienie w sprawie odstąpienia od praktyki publikowania na stronie internetowej Urzędu Miejskiego w Rogoźnie danych Osobowych, bez podstawy prawnej wynikającej z ustawy o ochronie danych osobowych.
27.	Prezydent Miasta Torunia	25.09.2008 r. DOLiS-440-483/08/25317	Wystąpienie o niezamieszczanie w treści pism, danych osobowych innych stron postępowania toczącego się o ustalenie opłaty rocznej z tytułu użytkowania wieczystego gruntu Gminy Miasta Toruń.
28.	Wiceminister Gospodarki	2.10.2008 r. DOLiS-440-502/08/26001	Wystąpienie o rozważenie możliwości wprowadzenia zmian w obowiązujących przepisach prawa, które usunęłyby wątpliwości w ustalaniu obowiązków osób składających do właściwych organów administracji „Wniosków o ustalenie warunków zabudowy lub lokalizacji inwestycji celu publicznego.”
29.	Burmistrz Wielunia	2.10.2008 r. DOLiS-440-502/08/26006	Wystąpienie o zmianę formularza „Wniosku o ustalenie warunków zabudowy lub lokalizacji inwestycji celu publicznego”, z uwzględnieniem wskazówek wynikających z zasad ochrony danych osobowych.
30.	Przewodniczący Sejmowej Komisji Nadzwyczajnej „Przyjazne Państwo” do spraw związanych z ograniczeniem biurokracji	2.10.2008 r. DOLiS-440-502/08/26003	Wystąpienie o rozważenie możliwości wprowadzenia zmian w obowiązujących przepisach prawa, które usunęłyby wątpliwości w ustalaniu obowiązków osób składających do właściwych organów administracji „Wnioski o ustalenie warunków zabudowy lub lokalizacji inwestycji celu publicznego.”
31.	Dowódca Jednostki Wojskowej nr 3271 w Elblągu	3.11.2008 r. DOLiS-440-383/08/29652	Wystąpienie o zmianę praktyki dotyczącej realizacji obowiązku informacyjnego z art. 33 ust. 1 ustawy o ochronie danych osobowych.
32.	Prezydent Białegostoku	12.11.2008 r. DOLiS-035-919/08/30538	Wezwanie do zaprzestania praktyki potwierdzania przez pracowników urzędu, danych osobowych „gapowicza” za każdym razem, gdy osoba dokonująca kontroli dokumentów przewozu, z taką prośbą wystąpi.
33.	Minister Sprawiedliwości	18.11.2008 r. DOLiS-440-318/02/31463/08/DOLiS	Zasygnalizowanie wątpliwości, co do sposobu prowadzenia przez podległą prokuraturę postępowania przygotowawczego, zakończonego postanowieniem o umorzeniu śledztwa.

34.	Prezes Zarządu Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych	25.11.2008 r. DOLiS-440-627/08/32348	Wystąpienie o zmianę formularza dot. przyznania pomocy w ramach programu „Pegaz 2003”, pod kątem jego zgodności z ustawą o ochronie danych osobowych.
35.	Komendant Główny Policji	10.12.2008 r. DOLiS-035-1542/08/34121/08	Wystąpienie o zapewnienie respektowania przepisów ustawy o ochronie danych osobowych przy przetwarzaniu danych osób zwracających się do Policji z prośbą o pomoc i nieujawnianiu ich danych osobom trzecim.
36.	Wójt Gminy Siedlisko	19.12.2008 r. DOLiS-035-1672/08/35375	Wystąpienie o zaprzestanie praktyki publikowania na stronach Biuletynu Informacji Publicznej, szerszego niż wynikający z przepisów prawa zakresu danych osobowych osób, które sprawują mandat radnego gminy.
37.	Minister Spraw Wewnętrznych i Administracji	23.12.2008 r. DOLiS-035-1673/08/35769	Wystąpienie o podjęcie działań legislacyjnych mających na celu stworzenie podstawy prawnej dla zgodnego z ustawą o ochronie danych osobowych, gromadzenia danych osób nieletnich przez funkcjonariuszy Policji w celu założenia tzw. Karty Nieletniego.

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych
w roku 2008 do podmiotów prywatnych**

L.p.	Nazwa podmiotu, do którego skierowano wystąpienie	Data wstąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	Spółdzielnia Mieszkaniowa "Podleśna" w Warszawie	14.01.2008 r. DOLiS-440-110/07/672/08	Wystąpienie dotyczące zaprzestania praktyki, ujawniania danych osobowych w miejscach powszechnie dostępnych.
2.	Przedsiębiorstwo Instalacyjno Usługowe INTECH w Białobrzegach	23.01.2008 r. DOLiS-440-190/07/1645/08	Wystąpienie o podjęcie działań mających na celu zabezpieczenie procesu przetwarzania danych osobowych, podczas przesyłania do adresatów korespondencji zawierającej dane osobowe.
3.	Spółdzielnia Mieszkaniowa "Przyczółek Grochowski" w Warszawie	28.01.2008 r. DOLiS-440-133/07/2068/08	Wystąpienie dotyczące zaprzestania praktyki rozsyłania do członków Spółdzielni Mieszkaniowej korespondencji, przez osoby nieupoważnione oraz w sposób umożliwiający zapoznanie się z jej treścią przez osoby trzecie.
4.	Znak Centrum Komputerowe Sp. z o.o.	19.02.2008 r. GI-DOLiS-035-207/08/4212	Wystąpienie o zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających właściwą ochronę danych Osobowych, pozyskiwanych za pomocą formularza zamieszczonego na stronie internetowej www.znak.pl .
5.	Leader's Digest Sp. z o.o.	29.02.2008 r. DOLiS-440-126/07/5398/08	Wystąpienie dotyczące zmiany treści klauzuli zgody, zamieszczonej na kuponach konkursowych.
6.	Rada Lubelskiej Okręgowej Izby Inżynierów Budownictwa	20.03.2008 r. DOLiS-035-15/08/7386	Wystąpienie o rozważenie zmiany praktyki, polegającej na udostępnianiu w treści zaświadczenia o przynależności do Izby (wydawanego na potrzeby postępowania poprzedzającego rozpoczęcie robót budowlanych), adresu zamieszkania jej członka.
7.	Zarząd Wspólnoty Mieszkaniowej Steyera 1 w Gdyni	1.04.2008 r. DOLiS-440-236/07/8262/08	Wystąpienie o zmianę praktyki umieszczania na tablicach ogłoszeń, kierowanych do członków Wspólnoty, treści zawierających dane osobowe stron, w związku z toczącym się postępowaniem sądowym wytoczonym Wspólnocie.
8.	Polskie Towarzystwo Psychologiczne	14.04.2008 r. DOLiS-035-491/08/9530/08	Wystąpienie o respektowanie zasad wynikających z ustawy o ochronie danych osobowych przy przetwarzaniu danych Osobowych, uczestników zjazdów naukowych PTS.
9.	KOLDWind Buk Sp. z o.o.	28.04.2008 r. DOLiS-440-10/08/10956	Wystąpienie o podjęcie działań w celu przestrzegania przepisów ustawy o ochronie danych osobowych przy przetwarzaniu przez Spółkę, danych osobowych właścicieli gruntów rolnych.
10.	AVENIR we Wrocławiu	14.05.2008 r. DOLiS-035-586/08/12316	Wystąpienie w sprawie dostosowania procesu przetwarzania danych osobowych gromadzonych za pośrednictwem formularza zamieszczonego na stronie internetowej www.korepetycje.twoje.pl , do wymogów wynikających z ustawy o ochronie danych osobowych.
11.	PKP Intercity S.A.	28.05.2008 r. DOLiS-035-258/08/13340/08 GI-DOLiS-430/6/07	Wystąpienie o wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych podróźnych, korzystających z systemu internetowej sprzedaży biletów, gromadzonych za pomocą formularza rejestracyjnego umieszczonego na stronie internetowej www.bilety.intercity.pl

12.	Spółdzielnia Mieszkaniowa „PAX” w Warszawie	30.05.2008 r. DOLiS-440-202/08/13598	Wystąpienie o zmianę praktyki upubliczniania danych osobowych, w treści ogłoszeń o zaskarżeniu przez członka Spółdzielni uchwały Zarządu Spółdzielni.
13.	Centralwings Nowy Przewoźnik Sp. z o.o.	6.06.2008 r. DOLiS-035-577/08/14199	Wystąpienie o dostosowanie przetwarzania danych na stronie internetowej www.centralwings.com poprzez zastosowanie środków kryptograficznej ochrony danych oraz prawidłowego sformułowania klauzuli informacyjnej.
14.	Wspólnota Mieszkaniowa w Jaworze	6.06.2008 r. DOLiS-440-218/08/14216	Wystąpienie o zmianę praktyki umieszczania danych osobowych, w treści ogłoszeń o zebraniu właścicieli nieruchomości.
15.	Związek Rzemiosła Polskiego	17.06.2008 r. DOLiS-035-221/08/15230/08	Wystąpienie o podjęcie działań mających na celu upowszechnienie wśród organizacji samorządu gospodarczego rzemiosła, znajomości przepisów ustawy o ochronie danych osobowych.
16.	ESC Computers	24.06.2008 r. DOLiS-035-634/08/15809/08	Wystąpienie o spełnienie obowiązku informacyjnego z art. 24 ust. 1 ustawy o ochronie danych osobowych.
17.	Telekomunikacja Polska S.A.	16.07.2008 r. DOLiS-35-892/08/18052/08	Wystąpienie o zastosowanie dodatkowych środków technicznych i organizacyjnych zapewniających właściwą ochronę przetwarzanych danych osobowych na stronie www.tp.pl .
18.	Bank Handlowy S.A. w Warszawie	30.07.2008 r. DOLiS-035-971/08/19458	Wystąpienie o zaprzestanie praktyki przysyłania do klientów banku korespondencji w niezaklejonych lub niedokładnie zaklejonych kopertach.
19.	Polska Wytwórnia Papierów Wartościowych S.A.	7.08.2008 r. DOLiS-440-579/08/20429	Wystąpienie o zmianę treści klauzuli zgody na kuponie rabatowym.
20.	Wspólnota Mieszkaniowa Siennicka 34 w Warszawie	7.08.2008 r. DOLiS-440-477/08/20275	Wystąpienie o zmianę praktyki upubliczniania w treści ogłoszeń danych osobowych członka Wspólnoty Mieszkaniowej.
21.	Telekomunikacja Polska S.A.	29.08.2008 r. DOLiS-035-950/08/22461/08	Wystąpienie o zmianę treści formularza oświadczenia o wyrażeniu zgody przez abonenta na zamieszczenie identyfikujących go danych w spisach abonentów prowadzonych przez TP S.A.
22.	BP Polska Sp. z o.o.	22.09.2008 r. DOLiS-440-715/08/24727	Wystąpienie o dostosowanie procesu przetwarzania danych osobowych gromadzonych za pośrednictwem formularza zamieszczonego na stronie internetowej www.bppartnerclub.pl do wymogów ustawy o ochronie danych osobowych.
23.	Sygma Banque Societe Anonyme S.A.	24.09.2008 r. DOLiS-440-503/08/25085	Wystąpienie o zaprzestanie przetwarzania danych osobowych w celach marketingowych, mimo zgłoszonego sprzeciwu.
24.	Skarbnica Narodowa Sp. z o.o.	25.09.2008 r. DOLiS-440-278/08/25208	Wystąpienie o respektowanie w działalności Spółki zasad wynikających z przepisów o ochronie danych osobowych, poprzez odstąpienie od działań polegających na uwzględnianiu ze zwłoką sprzeciwu wobec przetwarzania danych w celach marketingowych.
25.	DOZ S.A.	20.10.2008 r. DOLiS-035-1327/08/28003	Wystąpienie o dostosowanie procesu przetwarzania danych gromadzonych za pośrednictwem formularza zamieszczonego na stronie internetowej www.doz.pl do wymogów ustawy o ochronie danych osobowych.
26.	PH JUREX	21.10.2008 r. DOLiS-035-1262/28157	Wystąpienie o zmodyfikowanie treści klauzuli zgody na przetwarzanie danych, umieszczonej na stronie internetowej www.e-ticket.pl oraz dopełnienie obowiązku informacyjnego.
27.	Stołeczne Przedsiębiorstwo Energetyki Ciepłej S.A.	21.10.2008 r. DOLiS-440-628/08/28148	Wystąpienie o zmianę praktyki występowania do osób fizycznych, będących stronami umów na dostarczanie energii ciepłej, o wyrażenie zgody na przetwarzanie ich danych osobowych w celu realizacji tych umów.

28.	Spółdzielnia Mieszkaniowa im. Władysława Jagiełły w Łodzi	24.10.2008 r. DOLiS-035-1368/28697	Wystąpienie dotyczące prowadzenia przez Spółdzielnię video - nadzoru na jej terenie, wobec możliwości postawienia zarzutu naruszenia przez nią konstytucyjnie gwarantowanego prawa do prywatności.
29.	Commercial Union PTE BPH CU WBK S.A.	27.10.2008 r. DOLiS-035-1175/28911	Wystąpienie o dostosowanie procesu przetwarzania danych do wymogów ustawy o ochronie danych osobowych poprzez ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym.
30.	Bank Polska Kasa Opieki S.A.	30.10.2008 r. GI-DS-43052/06/29267/08/DOLiS	Wezwanie do wyeliminowania w przyszłości praktyki udostępniania bez podstawy prawnej, danych osobowych klienta Banku, Naczelnikowi Urzędu Skarbowego.
31.	Państwo Grażyna i Wiesław Grabarek	4.11.2008 r. DOLiS-440-258/08/29893	Wystąpienie ze wskazaniem, że rejestrowanie obrazu z sąsiedniej posesji za pomocą monitoringu, może prowadzić do postawienia zarzutu naruszenia konstytucyjnie gwarantowanego prawa do prywatności.
32.	Proboszcz Parafii Rzymskokatolickiej w Pławnie	12.12.2008 r. DOLiS-440-654/08/34568	Wystąpienie o uwzględnianie przepisów ustawy o ochronie danych osobowych i nieudostępnianie danych osobom nieupoważnionym.
33.	Polska Telefonia Cyfrowa Sp. z o.o.	15.12.2008 r. DOLiS-440-499/08/34679	Wystąpienie o przestrzeganie przepisów ustawy o ochronie danych osobowych podczas wykorzystywania danych abonentów Spółki, w celu marketingu produktów lub usług innego podmiotu.
34.	Polska Telefonia Komórkowa Centertel Sp. z o.o.	29.12.2008 r. DOLiS-035-1585/08/35948	Wystąpienie o dostosowanie procesu przetwarzania danych osobowych gromadzonych przy pomocy elektronicznego formularza, umożliwiającego zadanie pytania konsultantowi sieci Orange co do wymogów określonych w ustawie o ochronie danych osobowych.

Wykaz kontroli przeprowadzonych w 2008 r.

L.p.	Data / Sygnatura kontroli	Nazwa i miejsce podmiotu kontrolowanego	Inicjatywa kontroli	Rozstrzygnięcie oraz/lub data i sygnatura decyzji.
1.	09-11.01.2008r. DISK-421/108	I.D. Marketing Sp. z o.o. Warszawa, ul. Ryżowa 49	z urzędu	03.04.2008 r. decyzja DIS/DEC-213/8452/08
2.	16-18.01.2008r. DISK-421/208	IQ Marketing (Poland) Sp. z o.o. Warszawa, ul. W. Wiedeńskiej 17	z urzędu	13.06.2008 r. decyzja DIS/DEC-357/14952/08
3.	17-18.01.2008r. DISK-421/308	Tequila Polska Sp. z o.o. Poznań, ul. Wielka 20	z urzędu	materiał dowodowy dołączony do kontroli DIS-K-421/23/08
4.	16-18.01.2008r. DISK-421/408	Instytut Gruźlicy i Chorób Płuc Warszawa, ul. Płocka 26	z urzędu	przywrócono stan zgodny z prawem
5.	21-25.01.2008r. DISK-421/508	Nasza Klasa Sp. z o.o. Wrocław, ul. Dembowskiego 57/5	Departament Rejestracji Zbiorów Danych Osobowych	15.04.2008 r. decyzja DIS/DEC-242/9762/08
6.	21-25.01.2008r. DISK-421/608	Zespół Szkół Samorządowych Opoczno, ul. Armii Krajowej 1	Departament Orzecznictwa, Legislacji i Skarg	12.05.2008 r. decyzja DIS/DEC-290/12012/08
7.	23-25.01.2008r. DISK-421/708	Niezależny Związek Zawodowy Pracowników Ministerstwa Finansów, Warszawa, ul. Świętokrzyska 12	Departament Orzecznictwa, Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
8.	28-29.01.2008r. DISK-421/808	Prezes Urzędu Ochrony Konkurencji i Konsumentów, Warszawa, Pl. Powstańców Warszawy 1	w związku z kontrolą GDISK-411/11307	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
9.	29-31.01.2008r. DISK-421/908	Direct Communication Sp. z o.o. Warszawa, ul. Świętojerska 5/7	z urzędu	09.05.2008 r. decyzja DIS/DEC-288/11881/08
10.	30.01-01.02.2008 DISK-421/1008	Instytut Psychologii Zdrowia Polskiego Towarzystwa Psychologicznego, Warszawa, ul. Gęślarska 3	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
11.	31.01-01 i 04.02.2008r. DISK-421/1108	Bank Handlowy w Warszawie S.A. Warszawa, ul. Senatorska 16	Departament Orzecznictwa, Legislacji i Skarg	21.05.2008 r. decyzja DIS/DEC-306/12915/08
12.	04-07.02.2008r. DISK-421/1208	Polski Związek Żeglarski, Warszawa, ul. Chocimska 14	Departament Rejestracji Zbiorów Danych Osobowych	10.06.2008 r. decyzja DIS/DEC-349/14489/08
13.	05-07.02.2008r. DISK-421/1308	EM LAB Sp. z o.o. Warszawa, ul. Olimpijska 37	z urzędu	03.04.2008 r. decyzja DIS/DEC-214/8453/08
14.	11-15.02.2008r. DISK-421/1408	Krystyna Zawidniak prowadząca działalność gospodarczą pod nazwą „www.osmo.pl”, Bytom, ul. Karola Miarki 3/1	Prokuratura Rejonowa w Bytomiu	przywrócono stan zgodny z prawem
15.	11-12.02.2008r. DISK-421/1508	Tomczuk sp. j. Warszawa, ul. Leszczyńska 14	Departament Orzecznictwa, Legislacji i Skarg	12.05.2008 r. decyzja DIS/DEC-291/12020/08
16.	12-13.02.2008r. DISK-421/1608	Biblioteka Narodowa, Warszawa, Al. Niepodległości 213	z urzędu	28.03.2008 r. decyzja DIS/DEC-206/8000/08
17.	18-22.02.2008r. DISK-421/1708	Amitech Poland Sp. z o.o. Gdańsk, ul. Nowy Świat 20a	Departament Orzecznictwa, Legislacji i Skarg	przywrócono stan zgodny z prawem
18.	19-21.02.2008r. DISK-421/1808	PMI Combera Sp. z o.o., Warszawa, ul. Filomatów 27	z urzędu	09.05.2008 r. decyzja DIS/DEC-287/11880/08

19.	19-20.02.2008r. DISK-421/1908	Polski Związek Piłki Nożnej, Warszawa, ul. Miodowa 1	z urzędu	13.06.2008 r. decyzja DIS/DEC-358/14971/08
20.	25-27.02.2008r. DISK-421/2008	Renata Łącka prowadząca działalność gospodarczą pod nazwą „MarketShare”, Warszawa, ul. Owalna 7	z urzędu	nie stwierdzono uchybień
21.	26-29.02.2008r. DISK-421/2108	Focus Media Group Sp. z o.o. Warszawa, ul. Dąbrowskiego 46 lok. 1	z urzędu	24.04.2008 r. decyzja DIS/DEC-253/10611/08
22.	25-29.02.2008r. DISK-421/2208	Data Solutions Sp. z o.o. Poznań, ul. Wielka 20	z urzędu	08.10.2008 r. decyzja DISDEC- 634/26744,26747,26751,26757,26761/08
23.	25-29.02.2008r. DISK-421/2308	Tequila Polska Sp. z o.o. Poznań, ul. Wielka 20	w związku z kontrolą DISK-421/308	08.10.2008 r. decyzja DIS/DEC-632/26727,26728/08
24.	25-27.02.2008r. DISK-421/2408	ARC Worldwide Polska Sp. z o.o. Warszawa, ul. Wołoska 9	z urzędu	10.06.2008 r. decyzja DIS/DEC-351/14497/08
25.	25-26.02.2008r. DISK-421/2508	Partner ASM A. Stańczak, Sz. Pikula, M. Skrzypiec sp. j. Warszawa, ul. Świętokrzyska 18	z urzędu	17.06.2008 r. decyzja DIS/DEC-364/15210/08
26.	25-28.02.2008r. DISK-421/2608	Less Sp. z o.o. Ruda Śląska, ul. Kokotek 4	w związku z kontrolą DISK-421/1908	19.06.2008 r. decyzja DIS/DEC-370/15450,15510/08
27.	05-07.03.2008r. DISK-421/2708	Sławomir Giemza prowadzący działalność gospodarczą pod nazwą „PPGI Pierwsza Polska Grupa Inseminacyjna”, Warszawa, ul. Odkryta 48E lok. 411	Departament Orzecznictwa, Legislacji i Skarg	21.05.2008 r. decyzja DIS/DEC-307/12921/08
28.	26-28.03.2008r. DISK-421/2808	Momentum Worldwide Sp. z o.o. Warszawa, ul. Cybernetyki 19	z urzędu	nie stwierdzono uchybień
29.	05-07.03.2008r. 10-11.03.2008r. DISK-421/2908	Polymus Sp. z o.o. Warszawa, ul. Bobrowiecka 1A	z urzędu	19.08.2008 r. decyzja DIS/DEC-486/21461,21465/08
30.	10-14.03.2008r. DISK-421/3008	Arkadiusz Binek, Radosław Mazurek – wspólnicy CASA A. Binek R. Mazurek s.c. Gdańsk, ul. Hynka 73G	z urzędu	05.11.2008 r. decyzja DIS/DEC-717/30132/08
31.	10-14.03.2008r. DISK-421/3108	Radosław Mazurek, Bogdan Lipecki – wspólnicy Bono R. Mazurek sp.j. Gdynia, ul. Zielona 28	z urzędu	24.10.2008 r. decyzja DIS/DEC-689/28676/08
32.	10-12.03.2008r. DISK-421/3208	Stowarzyszenie Wikimedia Polska, Łódź, ul. Mazowiecka 59	Departament Orzecznictwa, Legislacji i Skarg	09.05.2008 r. decyzja DIS/DEC-289/11882/08
33.	12-14.03.2008r. DISK-421/3308	Wodne Ochotnicze Pogotowie Ratunkowe, Warszawa, ul. Pyłtasińskiego 17	Departament Orzecznictwa, Legislacji i Skarg	16.09.2008 r. decyzja DIS/DEC-540/24201/08
34.	12-14.03.2008r. DISK-421/3408	Arkadiusz Obłuski prowadzący działalność gospodarczą pod nazwą „Notar”, Legionowo, ul. Moniuszki 41	w związku z kontrolą DIS-K-421/144/07	nie stwierdzono uchybień
35.	17-19.03.2008r. DISK-421/3508	Juliusz Sarat prowadzący działalność gospodarczą pod nazwą „Przedsiębiorstwo Instalacyjno – Usługowe Intech”, Białobrzegi, ul. Osiedle Wojskowe 89/22	z urzędu	19.09.2008 r. decyzja DIS/DEC-567/24580/08
36.	17-19.03.2008r. DISK-421/3608	BBDO Warszawa Sp. z o.o. Warszawa, ul. Burakowska 5/7	z urzędu	nie stwierdzono uchybień

37.	17-19.03.2008r. DISK-421/3708	Elavon Financial Services LTD (Sp. z o.o.) Oddział w Polsce, Poznań, Al. Solidarności 46	w związku z kontrolą DIS-K-421/142/07	06.11.2008 r. decyzja DIS/DEC-720/30316/08
38.	17-19.03.2008r. DISK-421/3808	CardPoint S.A., Poznań, Al. Solidarności 46	w związku z kontrolą DIS-K-421/142/07	nie stwierdzono uchybień
39.	19-21.03.2008r. DISK-421/3908	Doug Faber Family Sp. z o.o. Warszawa, ul. Łowicka 35	z urzędu	19.06.2008 r. decyzja DIS/DEC-372/15461/08
40.	26-28.03.2008r. DISK-421/4008	Albedo Marketing Sp. z o.o. Poznań, ul. Żegockiego 10	z urzędu	15.07.2008 r. decyzja DIS/DEC-434/17869/08
41.	26.03.2008r. DISK-421/4108	Wodne Ochotnicze Pogotowie Ratunkowe, Warszawa, ul. Pyłtasińskiego 17	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
42.	26-28.03.2008r. DISK-421/4208	VA Strategic Communications Sp. z o.o. Warszawa, ul. Karwińska 21	z urzędu	19.06.2008 r. decyzja DIS/DEC-371/15458/08
43.	26-28.03.2008r. DISK-421/4308	Arteria S.A. Warszawa, ul. Rosoła 10	z urzędu	11.08.2008 r. decyzja DIS/DEC-472/20698,20700/08
44.	01-04.04.2008r. DISK-421/4408	Agencja Reklamowa Fresh Sp. z o.o. Poznań, ul. Chlebowa 4/8	z urzędu	26.05.2008 r. decyzja DIS/DEC-310/12973/08
45.	03-04.04.2008r. 08-09.04.2008r. DISK-421/4508	Urząd Miasta Łodzi, Łódź, ul. Piotrkowska 104	z urzędu	14.07.2008 r. decyzja DIS/DEC-433/17679/08
46.	08-11.04.2008r. 14.04.2008r. DISK-421/4608	Komenda Rejonowa Policji Warszawa, ul. Żeromskiego 7	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji
47.	07-09.04.2008r. DISK-421/4708	Gimnazjum nr 1 im. Powstańców Warszawy, Piaseczno, ul. Gen. Sikorskiego 20	z urzędu	17.06.2008 r. - wystąpienie do Mazowieckiego Kuratora Oświaty, 2008-09-08 r. - wystąpienie do Ministra Edukacji Narodowej, 13.10.2008 r. decyzja DIS/DEC-646/27140/08
48.	08-10.04.2008r. DISK-421/4808	Zespół Szkół nr 67 Gimnazjum nr 34 z Oddziałami Dwujęzycznymi, Warszawa, ul. Klonowa 16	z urzędu	24.10.2008 r. decyzja DIS/DEC-688/28673/08
49.	09-11.04.2008r. DISK-421/4908	Prywatna Szkoła Podstawowa nr 41, Warszawa, ul. Świętojerska 24	z urzędu	15.10.2008 r. decyzja DIS/DEC-655/27563/08
50.	14-16.04.2008r. DISK-421/5008	Komenda Rejonowa Policji Warszawa VI, Warszawa, ul. Cyryla i Metodego 4	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji
51.	14-16.04.2008r. DISK-421/5108	Zespół Szkół nr 68 – Gimnazjum nr 39, Warszawa, ul. Hoża 11/15	z urzędu	15.10.2008 r. decyzja DIS/DEC-657/27574/08
52.	15-18.04.2008r. DISK-421/5208	Urząd Miasta Inowrocławia, Inowrocław, ul. Roosevelta 36	Prokuratura Rejonowa w Inowrocławiu	ustalenia przekazano do Prokuratury Rejonowej w Inowrocławiu
53.	14-16.04.2008r. DISK-421/5308	Szkoła Podstawowa nr 12 im. Powstańców Śląskich, Warszawa, ul. Górnośląska 45	z urzędu	04.11.2008 r. decyzja DIS/DEC-714/29907/08
54.	15-18.04.2008r. DISK-421/5408	Wyższa Szkoła Menadżerska, Warszawa, ul. Kawęczyńska 36	z urzędu	11.08.2008 r. decyzja DIS/DEC-473/20705/08

55.	21-22.04.2008r. DISK-421/5508	Środowiskowe Warszawskie Wodne Ochotnicze Pogotowie Ratunkowe, Warszawa, ul. Jagiellońska 7	w związku z kontrolami DIS-K-421/33/08 i DIS-K-421/41/08	25.09.2008 r. decyzja DIS/DEC-581/25209/08
56.	22-25.04.2008r. DISK-421/5608	Piotr Nowak prowadzący działalność gospodarczą pod nazwą „NetArt Piotr Nowak”, Zabawa 118	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
57.	23-25.04.2008r. DISK-421/5708	Zespół Szkół nr 7 im. Sz.Bońkowskiego – CXXV Liceum Ogólnokształcące im. W. Milewicza, Warszawa, ul.Chłodna 36/46	z urzędu	24.10.2008 r. decyzja DIS/DEC-686/28669/08
58.	28-30.04.2008r. DISK-421/5808	Publiczna Szkoła Podstawowa nr 258 im. gen. Jasińskiego, Warszawa, ul. Brechta 8	z urzędu	03.11.2008 r. decyzja DIS/DEC-713/29667/08
59.	28-30.04.2008r. DISK-421/5908	Szkoła Podstawowa nr 187 im. Mickiewicza, Warszawa, ul. Staffa 21	z urzędu	15.10.2008 r. decyzja DIS/DEC-658/27587/08
60.	06-09.05.2008r. DISK-421/6008	Zbigniew Tyborski prowadzący działalność gospodarczą pod nazwą „RESAM-net”, Gdańsk, ul. Bora Komorowskiego 85A/6	w związku z kontrolami DIS-K-421/30/08, DIS-K-421/31/08 i DIS-K-421/141/07	15.10.2008 r. decyzja DIS/DEC-659/27642/08
61.	06-09.05.2008r. DISK-421/6108	Komenda Wojewódzka Policji w Bydgoszczy, Bydgoszcz, Al. Powstańców Wielkopolskich 7	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji
62.	07-09.05.2008r. i 12.05.2008r. DISK-421/6208	Grono.net S.A. Warszawa, ul. Szturmowa 2A	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
63.	07-09.05.2008r. DISK-421/6308	Admin s.c. Małgorzata Moczorodyńska, Barbara Hubl, Józefosław, ul. Montrealska 20	z urzędu	04.08.2008 r. decyzja DIS/DEC-464/20055/08
64.	12-16.05.2008r. DISK-421/6408	Komenda Wojewódzka Policji w Katowicach, Katowice, ul. Lompy 19	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji
65.	12-14.05.2008r. DISK-421/6508	Szkoła Podstawowa nr 29 im. Garibaldiiego, Warszawa, ul. Fabryczna 19	z urzędu	10.12.2008 r. decyzja DIS/DEC-803/34153/08
66.	12-15.05.2008r. DISK-421/6608	Spoleczna Szkoła Podstawowa nr 24 Społecznego Towarzystwa Oświatowego, Warszawa, ul. Powstańców Śląskich 67A	z urzędu	17.10.2008 r. decyzja DIS/DEC-666/27826/08
67.	14-16.05.2008r. DISK-421/6708	Gimnazjum nr 1, Radzymin, ul. 11-go Listopada 2	z urzędu	24.10.2008 r. decyzja DIS/DEC-687/28670/08
68.	13-14.05.2008r. DISK-421/6808	Komenda Główna Policji (Jednostka Narodowa Europolu), Warszawa, ul. Puławska 148/150	z urzędu	ustalenia przekazano do Sekretarza Wspólnych Organów Nadzorczych
69.	19-21.05.2008r. DISK-421/6908	Spoleczna Szkoła Podstawowa nr 16 Społecznego Towarzystwa Oświatowego, Warszawa, Al. Solidarności 113c	z urzędu	17.10.2008 r. decyzja DIS/DEC-665/27823/08
70.	27-30.05.2008r. DISK-421/7008	Zespół Szkół – Gimnazjum im. ks. Fedorowicza, Izabelin, ul. 3-go Maja 49	z urzędu	03.11.2008 r. decyzja DIS/DEC-712/29665/08
71.	26-30.05.2008r. DISK-421/7108	Komenda Miejska Policji w Gdyni, Gdynia, ul. Portowa 15	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji
72.	26-30.05.2008r. DISK-421/7208	Komenda Wojewódzka Policji w Łodzi, Łódź, ul. Lutomierska 108/112	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji

73.	26-30.05.2008r. DISK-421/7308	Zakład Gospodarki Mieszkaniowej w Końskich, Końskie, ul. Partyzantów 3	Prokuratura Rejonowa w Końskich	11.08.2008 r. decyzja DIS/DEC-471/20697/08
74.	28-30.05.2008r. DISK-421/7408	Zespół Szkół Publicznych – Gimnazjum, Leszno, ul. Leśna 13	z urzędu	21.10.2008 r. decyzja DIS/DEC-671/28142/08
75.	28-30.05.2008r. DISK-421/7508	Cinema City Poland Sp. z o.o. Warszawa, ul. Fosa 37	z urzędu	25.09.2008 r. decyzja DIS/DEC-582/25214/08
76.	28.05.2008r. DISK-421/7608	Stowarzyszenie „Mieszkańcy Osiedla Grabina”, Michałów – Grabina, ul. Grabowa 7	z urzędu	30.09.2008 r. decyzja DIS/DEC-601/25783/08
77.	03-06.06.2008r. DISK-421/7708	Zespół Szkół Ogólnokształcących Liceum Ogólnokształcące im. Prusa, Skierniewice, ul. Sienkiewicza 10	z urzędu	06.10.2008 r. decyzja DIS/DEC-624/26430/08
78.	09-12.06.2008r. DISK-421/7808	Fundacja „Dorośli Dzieciom”, Starachowice, ul. Staszica 10	Departament Orzecznictwa, Legislacji i Skarg	05.09.2008 r. decyzja DIS/DEC-524/23182/08
79.	09-12.06.2008r. DISK-421/7908	Zespół Szkół Licealnych i Technicznych nr 2 CXIX Liceum Ogólnokształcące, Warszawa, ul. Złota 58	z urzędu	22.10.2008 r. decyzja DIS/DEC-674/28348/08
80.	09-13.06.2008r. DISK-421/8008	Komenda Wojewódzka Policji w Białymstoku, Białystok, ul. Sienkiewicza 65	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji
81.	05-06.06.2008r. DISK-421/8108	Grono.net S.A. Warszawa, ul. Szturmowa 2A	z urzędu	nie stwierdzono uchybień
82.	10-12.06.2008r. DISK-421/8208	IX Liceum Ogólnokształcące im. Hofmanowej, Warszawa, ul. Emilii Plater 29	z urzędu	08.10.2008 r. decyzja DIS/DEC-631/26695/08
83.	16-20.06.2008r. DISK-421/8308	Miejskie Przedsiębiorstwo Oczyszczania w m.st. Warszawie Sp. z o.o. Warszawa, ul. Obozowa 43	Departament Orzecznictwa, Legislacji i Skarg	01.12.2008 r. decyzja DIS/DEC-776/33112/08
84.	17-20.06.2008r. DISK-421/8408	XXI Liceum Ogólnokształcące im. Prusa, Łódź, ul. Kopernika 2	z urzędu	22.10.2008 r. decyzja DIS/DEC-675/28358/08
85.	17-20.06.2008r. DISK-421/8508	III Liceum Ogólnokształcące im. Słowackiego, Piotrków Tryb., Al. Armii Krajowej 17	z urzędu	16.12.2008 r. decyzja DIS/DEC-818/34989/08
86.	16-18.06.2008r. DISK-421/8608	Amgen Sp. z o.o. Warszawa, ul. Złota 59	Departament Rejestracji Zbiorów Danych Osobowych	10.12.2008 r. decyzja DIS/DEC-802/34148/08
87.	16-18.06.2008r. DISK-421/8708	Gimnazjum nr 36 im. Kieślowskiego, Warszawa, ul. Polna 7	z urzędu	17.10.2008 r. decyzja DIS/DEC-667/27832/08
88.	25-27.06.2008r. DISK-421/8808	Szkoła Podstawowa nr 1 im. Morcinka, Warszawa, ul. Wilcza 53	z urzędu	24.10.2008 r. decyzja DIS/DEC-690/28681/08
89.	23-26.06.2008r. DISK-421/8908	Zespół Szkół nr 51 – CXXII Liceum Ogólnokształcące im. Domeyki, Warszawa, ul. Staffa 3/5	z urzędu	19.11.2008 r. decyzja DIS/DEC-746/31697/08
90.	23-27.06.2008r. DISK-421/9008	Komenda Wojewódzka Policji w Olsztynie, Olsztyn, ul. Partyzantów 6/8	z urzędu	29.07.2008 r. wystąpienie do Komendanta Głównego Policji
91.	23-27.06.2008r. DISK-421/9108	XXVIII Liceum Ogólnokształcące im. Bednarskiego, Kraków, ul. Czackiego 11	z urzędu	16.12.2008 r. decyzja DIS/DEC-819/34993/08
92.	25-27.06.2008r. DISK-421/9308	Ministerstwo Finansów, Warszawa, ul. Świętokrzyska 12	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
93.	07-10.07.2008r. DISK-421/9408	Spółdzielnia Mieszkaniowa „DOM”, Toruń, ul. Antczaka 21	z urzędu	26.11.2008 r. decyzja DIS/DEC-758/32570/08

94.	07-11.07.2008r. DISK-421/9508	Fundacja Ośrodka „Karta”, Warszawa, ul. Narbutta 29	Departament Rejestracji Zbiorów Danych Osobowych	15.10.2008 r. decyzja DIS/DEC-656/27568/08
95.	07-11.07.2008r. DISK-421/9608	Kujawska Spółdzielnia Mieszkaniowa, Inowrocław, Al. Kopernika 7	z urzędu	22.12.2008 r. decyzja DIS/DEC-863/35613/08
96.	08-10.07.2008r. DISK-421/9708	Spółdzielnia Mieszkaniowa „Aleje Jerozolimskie”, Warszawa, Al. Jerozolimskie 89/25	z urzędu	17.11.2008 r. decyzja DIS/DEC-738/31251/08
97.	14-18.07.2008r. DISK-421/9808	Białostocka Spółdzielnia Mieszkaniowa, Białystok, ul. Św. Rocha 11/1	z urzędu	06.10.2008 r. decyzja DIS/DEC-625/26431/08
98.	14-18.07.2008r. DISK-421/9908	Zachodniopomorska Agencja Rozwoju Regionalnego S.A. Szczecin, ul. Stożkowa 2	Departament Orzecznictwa, Legislacji i Skarg	08.09.2008 r. decyzja DIS/DEC-525/23309/08
99.	15-18.07.2008r. DISK-421/1008	Spółdzielnia Budowlano – Mieszkaniowa „BOWIG”, Warszawa, ul. Filtrowa 61	z urzędu	19.11.2008 r. decyzja DIS/DEC-747/31708/08
100.	15-18.07.2008r. DISK-421/10108	Spółdzielnia Mieszkaniowa „Górczewska”, Warszawa, ul. Doroszewskiego 4	z urzędu	01.12.2008 r. decyzja DIS/DEC-775/33105/08
101.	14-18.07.2008r. DISK-421/10208	Bank PEKAO S.A. Warszawa, ul. Grzybowska 53/57	z urzędu	03.09.2008 r. decyzja DIS/DEC-514/22844/08
102.	21-25.07.2008r. DISK-421/10308	Żabka Polska S.A. Poznań, ul. Ogrodowa 12	Departament Rejestracji Zbiorów Danych Osobowych	24.11.2008 r. decyzja DIS/DEC-751/32097/08
103.	22-23.07.2008r. DISK-421/10408	home.pl sp. j. Szczecin, Pl. Rodła 9	w związku z kontrolą DIS-K-421/102/08	ustalenia wykorzystane w postępowaniu DIS-K-421/102/08
104.	21-23.07.2008r. DISK-421/10508	„Possum Grzegorz Albrecht”, Warszawa, Al. Waszyngtona 2c/20	w związku z kontrolą DIS-K-421/102/08	ustalenia wykorzystane w postępowaniu DIS-K-421/102/08
105.	21-23.07.2008r. DISK-421/10608	GTS Polska Sp. z o.o. Warszawa, Al. Niepodległości 69	w związku z kontrolą DIS-K-421/102/08	ustalenia wykorzystane w postępowaniu DIS-K-421/102/08
106.	28.07-01.08.2008r. DISK-421/10708	Spółdzielnia Mieszkaniowa „Młyniec”, Gdańsk, ul. Pilotów 3	z urzędu	17.12.2008 r. decyzja DIS/DEC-844/35144/08
107.	28.07-01.08.2008 DISK-421/10808	Piotr Nowak prowadzący działalność gospodarczą pod nazwą „NetArt Piotr Nowak”, Zabawa 118	Departament Orzecznictwa, Legislacji i Skarg	13.10.2008 r. decyzja DIS/DEC-647/27157/08
108.	28-31.07.2008r. DISK-421/10908	Urząd Miasta Łodzi, Łódź, ul. Piotrkowska 104	Departament Rejestracji Zbiorów Danych Osobowych	15.12.2008 r. decyzja DIS/DEC-808/34629/08
109.	28-31.07.2008r. DISK-421/11008	Spółdzielnia Mieszkaniowa „3 Maja”, Warszawa, ul. 3-go Maja 5/4	z urzędu	19.11.2008 r. decyzja DIS/DEC-748/31712/08
110.	25.07.2008r. DISK-421/11108	Jarosław Gadziński prowadzący działalność gospodarczą „Equatile Jarosław Gadziński”, Warszawa, ul. Zamiejska 7/40	w związku z kontrolą DIS-K-421/102/08	ustalenia wykorzystane w postępowaniu DIS-K-421/102/08
111.	25.07.2008r. DISK-421/11208	Mateusz Dołęga prowadzący działalność gospodarczą pod nazwą „MDX Solution Mateusz Dołęga”, Łuków, ul. Kiernickich 4/19	w związku z kontrolą DIS-K-421/102/08	ustalenia wykorzystane w postępowaniu DIS-K-421/102/08
112.	04-07.08.2008r. DISK-421/11308	Spółdzielnia Budowlano – Mieszkaniowa „Batory”, Warszawa, ul. Bruna 32	z urzędu	19.12.2008 r. decyzja DIS/DEC-858/35334/08
113.	04-07.08.2008r. DISK-421/11408	Spółdzielnia Mieszkaniowa „Osiedle Młodych”, Warszawa, ul. Grenadierów 21	z urzędu	07.11.2008 r. decyzja DIS/DEC-723/30482/08

114.	04-08-2008r. DISK-421/11508	Spółdzielnia Mieszkaniowa „Arka”, Wrocław, ul. Kościuszki 125A	z urzędu	01.12.2008 r. decyzja DIS/DEC-774/33108/08
115.	11-14-08-2008r. DISK-421/11608	Komenda Nadwiślańskiego Oddziału Straży Granicznej, Warszawa, ul. 17-go Stycznia 23	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
116.	11-14-08-2008r. DISK-421/11708	Komenda Podlaskiego Oddziału Straży Granicznej, Białystok, ul. Bema 100	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
117.	12-14-08-2008r. DISK-421/11808	Kancelaria Prawnicza OBIG Sp. z o.o. Warszawa, ul. Filtrowa 69/32	Departament Orzecznictwa, Legislacji i Skarg	w toku
118.	18-20-08-2008r. DISK-421/11908	Logistep Polska Krzysztof Gajewski Nestor Nalewajko s.c. Ożarów Maz., ul. Poznańska 215	z urzędu	materiał dowodowy dołączono do sprawy DIS-K-421/118/09
119.	18-21-08-2008r. DISK-421/12008	Piotr Iskra prowadzący działalność gospodarczą pod nazwą „Wydawnictwo Rondo Piotr Iskra”, Kraków, ul. Limanowskiego 58	Departament Orzecznictwa, Legislacji i Skarg	31.10.2008 r. decyzja DIS/DEC-709/29526/08
120.	18-22-08-2008r. DISK-421/12108	Komenda Morskiego Oddziału Straży Granicznej, Gdańsk, ul. Oliwska 35	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
121.	18-22-08-2008r. DISK-421/12208	Bank Zachodni WBK S.A. Wrocław, ul. Rynek 9/11	z urzędu	nie stwierdzono uchybień
122.	18-22-08-2008r. DISK-421/12308	Spółdzielnia Budowlano – Mieszkaniowa „Choiny”, Lublin, ul. Gorczańska 2	z urzędu	17.11.2008 r. decyzja DIS/DEC-737/31249/08
123.	25-29-08-2008r. DISK-421/12408	Komenda Nadbużańskiego Oddziału Straży Granicznej, Chełm, ul. Tubakowska 2	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
124.	26-29-08-2008r. DISK-421/12508	Spółdzielnia Mieszkaniowa „Międzynarodowa”, Warszawa, ul. Międzynarodowa 44	z urzędu	14.11.2008 r. decyzja DIS/DEC-734/31101/08
125.	08-12-09-2008r. DISK-421/12608	Placówka Straży Granicznej w Bobrownikach	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
126.	08-12-09-2008r. DISK-421/12708	Placówka Straży Granicznej Warszawa – Okęcie, Warszawa, ul. Żwirki i Wigury 1	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
127.	08-12-09-2008r. DISK-421/12808	Regionalna Izba Obrachunkowa, Rzeszów, ul. Mickiewicza 10	Rzecznik Dyscypliny Finansów Publicznych w Rzeszowie	27.11.2008 r. decyzja DIS/DEC-763/32783/08
128.	08-12-09-2008r. DISK-421/12908	WiW Polska Sp. z o.o. Poznań, ul. Palacza 91A	Departament Orzecznictwa, Legislacji i Skarg	06.01.2009 r. decyzja DIS/DEC-5/175/09
129.	10-09-2008r. DISK-421/13008	McDonald's Polska Sp. z o.o. Warszawa, ul. Postępu 18A	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
130.	15-19-09-2008r. DISK-421/13108	Spółdzielnia Mieszkaniowa „Domator”, Kielce, ul. Massalskiego 4	z urzędu	17.12.2008 r. decyzja DIS/DEC-845/35145/08
131.	15-19-09-2008r. DISK-421/13208	Urząd Miasta Olsztyn, Olsztyn, Pl. Jana Pawła II 1	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
132.	22-26-09-2008r. DISK-421/13408	Placówka Straży Granicznej w Dorohusku	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
133.	22-26-09-2008r. DISK-421/13508	Spółdzielnia Mieszkaniowa „Słoneczny Stok”, Białystok, ul. Armii Krajowej 7	z urzędu	22.12.2008 r. decyzja DIS/DEC-862/35530/08

134.	22-26.09.2008r. DISK-421/136/08	PKO BP S.A. I Oddział w Bielsku – Białej, Bielsko – Biala, ul. 11-go Listopada 15	Prokuratura Rejonowa w Bielsku – Białej	DIS/DEC-1276015/09 – nakazująca DIS/DEC -310/13794/09 – uchylająco-utrzymująca w mocy
135.	24-25.09.2008r. DISK-421/137/08	Włoska Izba Handlowo – Przemysłowa w Polsce CCIIP, Warszawa, ul. Kredytowa 8/26	z urzędu	06.01.2009 r. decyzja DIS/DEC-4/174/09
136.	29.09-03.10.2008 DISK-421/138/08	Spółdzielnia Mieszkaniowa „Górna”, Łódź, ul. Ogniskowa 13	z urzędu	29.12.2008 r. decyzja DIS/DEC-910/35985/08
137.	29.09-03.10.2008 DISK-421/139/08	SPZOZ Państwowy Szpital dla Nerwowo i Psychicznie Chorych, Rybnik, ul. Gliwicka 33	Departament Orzecznictwa, Legislacji i Skarg	nie stwierdzono uchybień
138.	06-10.10.2008r. DISK-421/140/08	Placówka Straży Granicznej w Gdańsku Rębiechowie	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej
139.	01-03.10.2008r. DISK-421/141/08	Kredyt Bank S.A. Warszawa, ul. Kasprzaka 2/8	Departament Orzecznictwa, Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
140.	13-14.10.2008r. DISK-421/142/08	Komenda Główna Policji, Warszawa, ul. Puławska 148/150	Departament Orzecznictwa, Legislacji i Skarg	zakończona sygnalizacją
141.	06-08.10.2008r. DISK-421/143/08	XDATA s.c. N. Pikor, A. Pikor, Lublin, ul. Okopowa 6	Departament Orzecznictwa, Legislacji i Skarg	09.01.2009 r. decyzja DIS/DEC-14/609/09
142.	06-08.10.2008r. DISK-421/144/08	Ministerstwo Gospodarki, Warszawa, Pl. Trzech Krzyży 3/5	Departament Rejestracji Zbiorów Danych Osobowych	w toku
143.	08-10.10.2008r. DISK-421/145/08	Commercial Union Polska Sp. z o.o. Oddział w Łodzi, Łódź, Pl. Wolności 12	z urzędu	nie stwierdzono uchybień
144.	13-17.10.2008r. DISK-421/146/08	Rzeszowskie Przedsiębiorstwo Komunalne Sp. z o.o. Rzeszów, ul. Trembeckiego 3	Departament Orzecznictwa, Legislacji i Skarg	09.01.2009 r. decyzja DIS/DEC-15/615/09
145.	13-17.10.2008r. DISK-421/147/08	Izba Celna w Warszawie, Warszawa, ul. Ciołka 14A	z urzędu	13.01.2009 r. pismo do Szefa Służby Celnej
146.	20-24.10.2008r. DISK-421/149/08	Konsulat Generalny RP we Lwowie, Lwów, ul. Iwana Franki 110	z urzędu	zakończona wystąpieniem do MSZ
147.	15-17.10.2008r. DISK-421/150/08	Wezys Holiday Service Sp. z o.o. Warszawa, ul. Tamka 38	z urzędu	31.12.2008 r. decyzja DIS/DEC-917/36254/08
148.	20-22.10.2008r. DISK-421/151/08	DDB Warszawa Sp. z o.o. Warszawa, ul. Wybrzeże Gdyńskie 6c	w związku z kontrolą DIS-K-421/130/08	nie stwierdzono uchybień
149.	20-23.10.2008r. DISK-421/152/08	Anna Rybak – Kwiecińska prowadząca działalność gospodarczą pod nazwą „Biuro Podróży Anna Travel”, Warszawa, Al. Niepodległości 214/3	z urzędu	11.05.2009 r. DIS/DEC-356/16752/09 decyzja umarzająca
150.	20-24.10.2008r. DISK-421/153/08	Wojewódzki Ośrodek Lecznictwa Psychiatrycznego, Toruń, ul. Curie-Skłodowskiej 27/29	Kancelaria Prezesa Rady Ministrów	30.01.2009 r. DIS/DEC-71/3055/09 decyzja nakazująco-umorzająca
151.	20-24.10.2008r. DISK-421/154/08	Izba Celna w Białymstoku, Białystok, ul. Octowa 2	z urzędu	13.01.2009 r. pismo do Szefa Służby Celnej
152.	20-24.10.2008r. DISK-421/155/08	TUI Poland Sp. z o.o. Warszawa, ul. Wołoska 7	z urzędu	17.03.2009 r. DIS/DEC-206/9231/09
153.	28-31.10.2008r. DISK-421/156/08	Interhome Polska Sp. z o.o.	z urzędu	10.02.2009 r. DIS/DEC-89/4318/09

154.	27-30.10.2008r. DISK-421/15708	Holiday Travel S.A. Warszawa, ul. Nowowiejska 10	z urzędu	22.01.2009 DIS/DEC-54/2026/09
155.	27-31.10.2008r. DISK-421/15808	Biuro Podróży „ARS TOUR”, Gdynia, ul. Krasickiego 12/16	z urzędu	przywrócono stan zgodny z prawem
156.	28-31.10.2008r. DISK-421/15908	Adriatyk Sp. z o.o. Warszawa, ul. Puławska 182	z urzędu	16.04.2009 r. DIS/DEC-306/13534/09 decyzja umarzająca
157.	29-31.10.2008r. DISK-421/16008	ING Towarzystwo Funduszy Inwestycyjnych S.A. Warszawa, Pl. Trzech Krzyży 10/14	Prokuratura Rejonowa Warszawa Mokotów	przywrócono stan zgodny z prawem
158.	04-07.11.2008r. DISK-421/16108	Krajowe Przedsiębiorstwo Turystyczno– Wypoczynkowe „Natura Tour” Sp. z o.o. Gdańsk, ul. Dyrekcyjna 2-4 (miejsce kontroli: Warszawa, ul. Chmielna 73A)	z urzędu	11.03.2009 r. DIS/DEC-181/8527/09
159.	04-07.11.2008 DISK-421/16208	Ultimo Sp. z o.o. Wrocław, ul. Braniborska 58-68	Departament Orzecznictwa, Legislacji i Skarg	w toku
160.	12-14.11.2008r. DISK-421/16308	PolGuard Consulting Sp. z o.o. Warszawa, ul. Ogórkowa 45A/10	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
161.	04-07.11.2008r. 18-19.11.2008r. DISK-421/16408	Jobs.pl S.A. Warszawa Al. KEN 36A lok. 93	Departament Edukacji Społecznej i Współpracy Międzynarodowej	DIS/DEC-584/23650/09 decyzja nakazująco-umarzająca
162.	04-05.11.2008r. DISK-421/16508	Instytut Gruźlicy i Chorób Płuc, Warszawa, ul. Płocka 26	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
163.	04-07.11.2008r. DISK-421/16608	Commercial Union Polska Sp. z o.o. Warszawa, ul. Prosta 70	w związku z kontrolą DIS-K-421/145/08	12.03.2009 r. pismo informujące do Commercial Union Polska S.A. - nie stwierdzono uchybień
164.	05.11.2008r. DISK-421/16708	Twenty Four Seven PR Sp. z o.o. Warszawa ul. Cząstkowska 32	w związku z kontrolą DIS-K-421/130/08	19.12.2008 r. decyzja DIS/DEC-857/35333/08
165.	06-07.11.2008r. DISK-421/16808	Obsługa Funduszy Inwestycyjnych Sp. z o.o. Warszawa, ul. Cybernetyki 21	Prokuratura Rejonowa Warszawa Mokotów	ustalenia przekazano do Prokuratury Rejonowej Warszawa Mokotów
166.	12-14.11.2008r. DISK-421/16908	Dominet Bank S.A. Lublin, ul. Księcia Ludwika I 3	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
167.	17-21.11.2008r. DISK-421/17008	Komunikacja Miejska Sp. z o.o. Głogów, ul. Rudnowska 30	Departament Orzecznictwa, Legislacji i Skarg	12.05.2009 r. DIS/DEC-316/14290/09 decyzja nakazująco-umarzająca
168.	17-20.11.2008r. DISK-421/17108	Kontynenty Sp. z o.o. Warszawa, ul. Widok 18	z urzędu	29.01.2009 r. DIS/DEC- 68/2867/09
169.	17-20.11.2008r. DISK-421/17208	Przedsiębiorstwo Energetyki Ciepłej w Dąbrowie Górniczej S.A. Dąbrowa Górnicza, Al. Piłsudskiego 2	Departament Orzecznictwa, Legislacji i Skarg	10.02.2009 r. DIS/DEC-90/4327/09
170.	17-21.11.2008r. DISK-421/17308	Intourist Polska Sp. z o.o. Warszawa, ul. Nowogrodzka 10	z urzędu	23.02.2009 r. DIS/DEC-125/6007/09
171.	18-21.11.2008r. DISK-421/17508	Ecco Holiday Sp. z o.o. Biuro w Warszawie Al. Jerozolimskie 109	z urzędu	23.02.2009 r. DIS/DEC-124/6005/09
172.	17-20.11.2008r. DISK-421/17608	Państwowe Przedsiębiorstwo Użyteczności Publicznej „Poczta Polska” - Centrum Poczty Oddział Regionalny w Poznaniu ul. Kościuszki 77	z urzędu	nie stwierdzono uchybień
173.	17-18.11.2008r. DISK-421/17708	Państwowe Przedsiębiorstwo Użyteczności Publicznej „Poczta Polska”, Warszawa, ul. Rakowiecka 26	z urzędu	nie stwierdzono uchybień

174.	25.28.11.2008r. DISK-421/178/08	Geovita Sp. z o.o. Warszawa, ul. Krucza 6/14	z urzędu	06.04.2009 r. DIS/DEC-272/12136/09
175.	24.28.11.2008r. DISK-421/179/08	Izba Celna w Poznaniu, Poznań, ul. Krańcowa 28	z urzędu	13.01.2009 r. pismo do Szefa Służby Celnej
176.	20.21.11.2008r. DISK-421/180/08	Wspólnoty Mieszkaniowe, Warszawa, ul. Wielicka 36,38,40,42	Departament Orzecznictwa, Legislacji i Skarg	zakończona pismo z dnia 16.01.2009 r.
177.	25.28.11.2008r. DISK-421/181/08	Urząd Miasta i Gminy Radzymin, Radzymin, Pl. Kościuszki 2	w związku z kontrolą DIS-K-421/67/08	przywrócono stan zgodny z prawem
178.	25.27.11.2008r. DISK-421/182/08	P.P.U.P. „Poczta Polska” Centralny Ośrodek Rozliczeniowy w Bydgoszczy, ul. Bernardyńska 15	z urzędu	nie stwierdzono uchybień
179.	25.27.11.2008r. DISK-421/183/08	Rainbow Tours S.A. Oddział w Warszawie ul. Wilcza 51A	z urzędu	13.05.2009 r. DIS/DEC-390/17359/09 decyzja nakazująco-umarzająca
180.	24.27.11.2008r. DISK-421/184/08	Sigma Travel Sp. z o.o. Warszawa ul. Marszałkowska 140	z urzędu	09.02.2009 r. DIS/DEC-80/4028/09
181.	24.25.11.2008r. DISK-421/185/08	P.P.U.P. „Poczta Polska” Warszawa, ul. Rakowiecka 26	z urzędu	nie stwierdzono uchybień
182.	27.11.2008r. DISK-421/186/08	Państwowe Przedsiębiorstwo Użyteczności Publicznej „Poczta Polska” – Centrum Poczty Węzeł Ekspedycyjno – Rozdzielczy w Łodzi, Al. Włókniarzy 227	z urzędu	nie stwierdzono uchybień
183.	02.05.12.2008r. DISK-421/187/08	Happy Holiday Travel Duo Sp. z o.o. Warszawa, ul. Czackiego 3/5	z urzędu	28.04.2009 r. DIS/DEC-336/15131/09 DIS/DEC-336/15135/09 decyzja umarzająca
184.	04.05.12.2008r. DISK-421/188/08	Samodzielny Zespół Publicznych Zakładów Opieki Zdrowotnej dla Szkół Wyższych – Oddział Szpitalny dla Szkół Wyższych, Warszawa, ul. Mochnickiego 10	z urzędu	wykonano decyzję DIS-DEC-51/1641/08
185.	08.09.12.2008r. DISK-421/189/08	Biblioteka Narodowa, Warszawa, Al. Niepodległości 213	z urzędu	wykonano decyzję DIS/DEC-206/8000/08
186.	04.05.12.2008r. DISK-421/190/08	ARC Worldwide Polska Sp. z o.o. Warszawa, ul. Wołoska 9	z urzędu	wykonano decyzję DIS/DEC-51/14497/08
187.	04.05.12.2008r. DISK-421/191/08	Samodzielny Publiczny Zespół Z.O.Z. Solec Szpital na Solcu, Warszawa, ul. Solec 93	z urzędu	wykonano decyzję DIS/DEC-27/1161/08
188.	10.11.12.2008r. DISK-421/192/08	Samodzielny Publiczny Szpital Kliniczny im. prof. Witolda Orłowskiego – Centrum Medycznego Kształcenia Podyplomowego, Warszawa ul. Czerniakowska 231	z urzędu	nakazy decyzji GİODO wykonano w części DIS/DEC-129/42107/07
189.	08.12.12.2008r. DISK-421/193/08	Wydział Konsularny Ambasady RP w Federacji Rosyjskiej, Moskwa, ul. Klimaszkińska 4	z urzędu	zakończona wystąpieniem do MSZ
190.	08.10.12.2008r. DISK-421/194/08	Komendant Główny Straży Granicznej, Warszawa, Al. Niepodległości 100	z urzędu	14.01.2009 r. pismo do Komendanta Głównego Straży Granicznej

191.	08.10.122008r. DISK-421/19508	Szef Służby Celnej, Warszawa, ul. Świętokrzyska 12	z urzędu	13.01.2009 r. pismo do Szefa Służby Celnej
192.	09.11.122008r. DISK-421/19608	SLG Thomas International Poland Sp. z o.o. Warszawa, ul. Nowy Świat 64	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
193.	10.12.2008r. DISK-421/19708	Animex Sp. z o.o. Warszawa, ul. Chałubińskiego 8	z urzędu	wykonano decyzję DIS/DEC-486/21461,21465/08
194.	15.18.122008r. DISK-421/19808	Exim Tours Sp. z o.o. Warszawa, ul. Piękna 45	z urzędu	23.02.2009 r. DIS/DEC-126/6011/09
195.	15.17.122008r. DISK-421/19908	Ewa Ajdukiewicz prowadząca działalność gospodarczą pod nazwą „Biuro Podróży Ochota”, Warszawa, ul. Grochowska 120	z urzędu	25.02.2009 r. DIS/DEC-135/6327/09
196.	16.19.122008r. DISK-421/20008	Damis Travel Bogdan Marek Tomaszewski, Warszawa, ul. Kłopotowskiego 11	z urzędu	29.04.2009 r. DIS/DEC-348/15553/09 decyzja umarzająca
197.	15.12.2008r. DISK-421/20108	Tomczuk sp. j. Warszawa, ul. Leszcynowa 14	z urzędu	zaprzeszono powierzania przetwarzania danych osobowych
198.	15.18.122008r. DISK-421/20208	GTI Travel Poland Sp. z o.o. Warszawa, ul. Wilcza 66/68	z urzędu	10.04.2009 r. DIS/DEC-288/13016/09 decyzja umarzająca
199.	17.12.2008r. DISK-421/20308	Change Communications Sp. z o.o. Warszawa, ul. Łowiecka 35	z urzędu	nakazy decyzji bezprzedmiotowe
200.	16.19.122008r. 22-23.122008r. DISK-421/20408	Ogólnokrajowa Spółdzielnia Turystyczna „Gromada” Biuro w Warszawie Pl. Powstańców Warszawy 2	z urzędu	DIS/DEC-547/22490/09 decyzja umarzająca
201.	29.12.2008r. DISK-421/20508	Niepubliczny Zakład Opieki Zdrowotnej BOPOL, Warszawa, Al. Jerozolimskie 123A	z urzędu	DIS/DEC-43/1524/08 wykonano decyzję

**Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie
i Naczelnego Sądu Administracyjnego
wydanych w 2008 r. w sprawach prowadzonych
przez Generalnego Inspektora Ochrony Danych Osobowych**

L.p	Data/ Sygnatura orzeczenia WSA w Warszawie lub NSA	Sygnatura rozstrzygnięcia GODO	Przedmiot sprawy	Rozstrzygnięcie WSA w Warszawie lub NSA
1.	2012008r. II SAWa 1717/07	GHDS-430867/054195DOLIS	Skarga na postanowienie GODO w przedmiocie odmowy przywrócenia terminu	stwierdzenie nieważności zaskarżonego postanowienia
2.	17.01.2008r. II SAWa 1551/07	GHDEC-DIS-4607/340	Brak zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, zbioru danych osobowych klientów; brak opracowania polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym oraz zapewnienia, aby systemy informatyczne służące do przetwarzania danych zapewniały odnotowanie, sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie informatycznym, raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze użytkownika wprowadzającego te dane.	uchylenie zaskarżonej decyzji
3.	23.01.2008r. IOZ 1308	GHDEC-DS-30906841,842,843	Przetwarzanie danych osobowych przez operatora telekomunikacyjnego	oddalenie zażalenia na postanowienie WSA w Warszawie o odrzuceniu skargi na decyzję GODO
4.	28.01.2008r. IOSK 136506	GHDEC-DIS-22605/757,758	Udostępnianie danych osobom nieupoważnionym; brak zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych; brak kontroli nad tym, kto, kiedy i jakie dane wprowadził do zbioru oraz komu są przekazywane; brak ewidencji osób upoważnionych do przetwarzania danych osobowych; brak zgłoszenia prowadzonych zbiorów do rejestracji; brak opracowania polityki bezpieczeństwa; brak wszystkich wymaganych elementów w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych; brak odnotowania daty pierwszego wprowadzenia danych do systemu informatycznego; brak identyfikatora użytkownika wprowadzającego te dane oraz informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia; brak zabezpieczenia dostępu do systemu informatycznego, aby był możliwy wyłącznie po wprowadzeniu identyfikatora i podaniu hasła.	oddalenie skargi kasacyjnej
5.	31.01.2008r. II SAWa 1958/07	GHDEC-DOLIS-20107/5346,5347,5348	Przetwarzanie danych osobowych	oddalenie skargi
6.	5.02.2008r. IOSK 3707	GHDEC-DS-705/24,25	Wniosek o nakazanie udostępnienia danych osobowych	uchylenie zaskarżonego wyroku WSA w Warszawie
7.	5.02.2008r. IOSK 1107	GHDEC-DS-106/1,2	Przetwarzanie danych osobowych	oddalenie skargi kasacyjnej

8.	5.02.2008r. IOSK/3707	GHDEC-DS-705/24,25	Wniosek o nakazanie udostępnienia danych osobowych	uchylenie wyroku WSA w Warszawie
9.	5.02.2008r. II SAWa 14508	GHDEC-DOLIS-26107/6727,6728,6729	Wniosek o nakazanie udostępnienia adresów zamieszkania	odrzućcie skargi
10.	5.02.2008r. II SAWa 14508	GHDEC-DOLIS-26107/6727,6728,6729	Wniosek o nakazanie udostępnienia danych osobowych	odrzućcie skargi
11.	6.02.2008r. II SAWa 83006	GHDEC-DS-33505/957,958,959	Przetwarzanie danych osobowych przez Gminę Goleniów	uchylenie zaskarżonej decyzji GİODO
12.	6.02.2008r. II SAWa 115007	GHDEC-DOLIS-9807/2672,2673,2674	Udostępnienie danych osobowych przez ZUS podmiotowi nieuprawnionemu	uchylenie zaskarżonej decyzji
13.	7.02.2008r. II SABWa 708	GHDEC-DOLIS-24707/6439,6440	Przetwarzanie danych osobowych przez Pocztę Polską	odrzućcie skargi na bezczynność GİODO
14.	12.02.2008r. II SAWa 199406	GHDEC-DS-30406/828	Przetwarzanie danych osobowych	odrzućcie zażalenia na postanowienie WSA w Warszawie odrzućcie skargę kasacyjną
15.	14.02.2008r. II SAWa 174507	GH-DOLIS-430131/07/4446	Przetwarzanie danych osobowych przez Gminną Komisję Profilaktyki i Rozwiązywania Problemów Alkoholowych	uchylenie postanowienia GİODO w przedmiocie zwrotu skargi
16.	15.02.2008r. II SAWa 197907	GHDEC-DOLIS-19907/5336,5337,5338	Wniosek o usunięcie danych osobowych	uchylenie zaskarżonej decyzji GİODO
17.	18.02.2008r. II SAWa 174007	GHDEC-DOLIS-11407/2927,2928,2929,2930	Przetwarzanie danych osobowych	odrzućcie skargi kasacyjnej na postanowienie WSA w Warszawie
18.	19.02.2008r. IOZ 6908	GHDEC-DOLIS-14807/3926	Przetwarzanie danych osobowych	oddalenie zażalenia na postanowienie WSA w Warszawie przywracające termin
19.	27.02.2008r. IOSK/29707	GHDEC-DS-3806/117,118	Udostępnienie danych osobowych podmiotowi nieuprawnionemu	uchylenie wyroku WSA w Warszawie
20.	27.02.2008r. IOSK/22107	GHDEC-DIS-14704/315	Zaprzestanie zbierania danych osobowych potencjalnych klientów w zakresie szerszym niż jest to niezbędne dla celów przetwarzania danych (przedstawienia telefonicznej oferty ubezpieczeniowej); zaprzestanie zbierania danych osobowych klientów (w wyniku fotografowania dowodu osobistego i prawa jazdy) w szerszym zakresie niż jest niezbędne dla realizacji celu przetwarzania danych (wystawienia polisy, oceny ryzyka ubezpieczeniowego, wyliczenia składki i realizacji umowy ubezpieczenia); usunięcie danych osobowych osób, z którymi nie zawarto umowy ubezpieczenia; uzupełnienie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych	umorzenie postępowania w sprawie przed NSA
21.	13.03.2008r. II SAWa 14308	GHDEC-DIS-119421/07/847	Brak zgłoszenia do rejestracji Generalnemu Inspektorowi, zbioru danych osobowych klientów oraz faktu usunięcia danych.	oddalenie skargi
22.	18.03.2008r. IOSK/45407	GHDEC-DS-17806/512,513,514	Wniosek o nakazanie przetwarzania danych osobowych	oddalenie skargi kasacyjnej
23.	20.03.2008r. II SAWa 128007	GHDS-4306406/298607/DOLIS	Przetwarzanie danych osobowych	uchylenie postanowienia GİODO w przedmiocie uchylenia terminu do wniesienia wniosku o ponowne rozpoznanie sprawy
24.	28.03.2008r. II SAWa 207807	GHDS-43018506/5638, 563907/DOLIS	Przetwarzanie danych osobowych	odrzućcie skargi kasacyjnej

25.	4.04.2008r.	GHDEC-DOLIS-26807/6944	Przetwarzanie danych osobowych	odrzućcie skargi
26.	17.04.2008r. II SA/Wa 274/08	GHDEC-DS-11705/330,331,332	Udostępnienie danych osobowych podmiotowi nieuprawnionemu	odrzućcie skargi
27.	17.04.2008r. II SA/Wa 1692/06	GHDEC-DS-22506/13,614	Wniosek o nakazanie udostępnienia danych osobowych	stwierdzenie nieważności decyzji
28.	18.04.2008r. I OSK 616/07	GHDEC-DS-7406/241,242,243	Przetwarzanie danych osobowych	uchylenie wyroku WSA w Warszawie
29.	18.04.2008r. I OZ 270/08	GHDEC-DS-30406/828	Przetwarzanie danych osobowych	oddalenie zażalenia na postanowienie WSA w Warszawie
30.	23.04.2008r. I OZ 283/08	GHDEC-DOLIS-11407/2927,2928,2930	Przetwarzanie danych osobowych	oddalenie zażalenia na postanowienie WSA w Warszawie o odrzuceniu skargi kasacyjnej
31.	25.04.2008r. II SA/Wa 2078/07	GHDS-4301/0506	Przetwarzanie danych osobowych	odrzućcie zażalenia na postanowienie WSA w Warszawie
32.	28.04.2008r. II SAB/Wa 250/8	DOLIS-440/607	Przetwarzanie danych osobowych	odrzućcie skargi
33.	28.04.2008r. II SAB/Wa 250/8	DOLIS-440/607	Przetwarzanie danych osobowych	odrzućcie skargi na bezzeczność GODO
34.	6.05.2008r. II SA/Wa 60/08	GHDEC-DOLIS-23307/6154,6155,6156	Wniosek o wydanie nakazu zaprzestania przetwarzania danych osobowych	oddalenie skargi
35.	7.05.2008r. I OSK 998/07	GHDEC-DS-15106/455,456	Brak odpowiedniego zabezpieczenia danych osobowych	oddalenie skargi kasacyjnej
36.	7.05.2008r. I OSK 761/07	GHDEC-DS-8706/275,276,277	Wniosek o nakazanie usunięcia danych osobowych	oddalenie skargi kasacyjnej
37.	7.05.2008r. I OSK 983/07	GHDEC-DIS-34906/953	Brak zgłoszenia do rejestracji Generalnemu Inspektorowi, zbioru danych osobowych zawartych w raportach ze zdarzeń	uchylenie zaskarżonego wyroku i przekazanie sprawy WSA w Warszawie do ponownego rozpatrzenia
38.	9.05.2008r. II SA/Wa 2102/07	GHDEC-DOLIS-20607/5496	Brak odpowiedniego zabezpieczenia danych osobowych	oddalenie skargi kasacyjnej
39.	12.05.2008r. II SA/Wa 326/08	GHDEC-DOLIS-27307/7227,7228,7229	Przetwarzanie danych osobowych	oddalenie skargi
40.	13.05.2008r. II SA/Wa 262/08	GH-DOLIS-430250/07/6979,6970	Przetwarzanie danych osobowych	oddalenie skargi
41.	13.06.2008r. II SA/Wa 241/08	GHDS-430551/066877,6978/07/ DOLIS	Przetwarzanie danych osobowych	uchylenie postanowienia GODO w przedmiocie zawieszenia postanowienia
42.	13.06.2008r. II SA/Wa 241/08	GHDS-430551/066977, 6978/07/DOLIS	Przetwarzanie danych osobowych	uchylenie postanowienia GODO
43.	19.06.2008r. II SAB/Wa 130/07	GHDS-43087/06	Przetwarzanie danych osobowych	odrzućcie skargi na bezzeczność GODO
44.	25.06.2008r. II SA/Wa 2078/07	GHDS-43018506/5638,5639	Przetwarzanie danych osobowych	odrzućcie zażalenia
45.	27.06.2008r. II SA/Wa 800/08	GH-DOLIS-430254/07	Przetwarzanie danych osobowych	odrzućcie skargi

46.	2.07.2008r. II SAWa 2007/07	GHDEC-DOLIS- 20207/5359,5360,5361,5362	Przetwarzanie danych osobowych	oddalenie skargi
47.	10.07.2008r. II SAWa 564/08	DOLISDEC- 12608/4281,4282,4284,4285	Udostępnianie danych osobowych podmiotowi nieuprawnionemu	oddalenie skargi
48.	16.07.2008r. II SAWa 917/08	DOLISDEC-257/08/10742	Wniosek o nakazanie usunięcia danych osobowych	odmowa wstrzymania wykonania decyzji
49.	5.08.2008r. II SAWa 66/08	DOLIS-440-200/07	Skarga na bezczynność GİODO	Umorzenie postępowania przez WSA w Warszawie
50.	7.08.2008r. IOSK 1218/07	GHDEC-DS-8506/1109,1110	Przetwarzanie danych osobowych	uchylenie wyroku WSA w Warszawie i decyzji GİODO
51.	7.08.2008r. IOSK 1091/07	GHDS-DEC-30306826,827	Przetwarzanie danych osobowych	oddalenie skargi kasacyjnej
52.	19.08.2008r. II SAWa 734/08	GHDEC-DIS-2158454/08	Przyznanie statusu administratora danych	uchylenie zaskarżonej decyzji
53.	19.08.2008r. II SAWa 735/08	GHDEC-DIS-2158454/08	Przyznanie statusu administratora danych	uchylenie zaskarżonej decyzji
54.	19.08.2008r. II SAWa 605/08	GHDEC-DIS-726400,6404/08	Przyznanie statusu administratora danych	uchylenie zaskarżonej decyzji
55.	29.08.2008r. II SAWa 1015/08	DOLISDEC- 33808/13593,13601,13604	Przetwarzanie danych osobowych	odrzućenie skargi
56.	2.09.2008r. II SAWa 971/08	GH-DOLIS-430314/07/6804,6805	Wniosek o sporządzenie i przesłanie kserokopii materiału dowodowego	odrzućenie skargi
57.	3.09.2008r. II SAWa 221/08	GHDEC-DOLIS- 27207/7160,7161	Przetwarzanie danych osobowych	odrzućenie skargi
58.	17.09.2008r. IOZ 682/08	DOLISDEC-257/08/10742	Wniosek o nakazanie usunięcia danych osobowych	oddalenie zażalenia na postanowienie WSA w Warszawie w przedmiocie odmowy wstrzymania wykonania decyzji
59.	18.09.2008r. IOSK 194/08	GHDEC-DOLIS-14707/3925	Wniosek o udostępnienie informacji publicznej	oddalenie skargi kasacyjnej
60.	30.09.2008r. II SAWa 1156/08	DOLISDEC- 34508/14201,14206,14209	Wniosek o nakazanie udostępnienia danych osobowych	odrzućenie skargi
61.	9.10.2008r. II SAWa 775/08	DOLISDEC- 19508/7496,7501,7502	Przetwarzanie danych osobowych	odrzućenie skargi
62.	9.10.2008r. II SAWa 906/08	GHDEC-DS-7406241,242,243	Wniosek o nakazanie usunięcia danych osobowych	oddalenie skargi
63.	10.10.2008r. II SAWa 1131/08	GHDEC-DIS-352/14500,14512/08	Zaprzestanie pozyskiwania danych osobowych na formularzach przetwarzanych w celach marketingowych, bez zgody osób, których dane dotyczą; usunięcie danych osobowych pozyskiwanych na ww. formularzach bez zgody osób, których dane dotyczą; zaprzestanie pozyskiwania danych osobowych kandydatów do pracy za pomocą testów psychometrycznych	odmowa wstrzymania wykonania zaskarżonej decyzji

64.	15.10.2008r. II SAWa 1233/08	DOL/DEC-39308/16162,16164,16167	Wniosek o nakazanie usunięcia danych osobowych	wstrzymanie wykonania decyzji
65.	28.10.2008r. II SAWa 763/08	DOL/DEC-23008/9111,9115,9117	Wniosek o usunięcie uchybień przy przetwarzaniu danych osobowych	uchylenie decyzji GODO
66.	29.10.2008r. IOSK 1301/08	GHDEC-DOL/5-20607/5496	Zabezpieczenie danych osobowych	oddalenie skargi kasacyjnej
67.	30.10.2008r. II SABWa 88/08	DOL/440-330/08	Przetwarzanie danych osobowych	odrzućcie skargi
68.	3.11.2008r. II SAWa 1003/08	DOL/DEC-30008/12622,12625,12626,12628,12630,2632,12633	Przetwarzanie danych osobowych	oddalenie skargi
69.	4.11.2008r. II SAWa 1550/07	GHDEC-DOL/5-15407/4023	Przetwarzanie danych osobowych	odrzućcie skargi
70.	18.11.2008r. II SAWa 1177/08	DOL/DEC-37508/15721,15725	Udostępnienie danych osobowych na stronie internetowej BIP	odrzućcie skargi
71.	25.11.2008r. IOSK 1743/07	GHDEC-DOL/5-1061307/1308	Przetwarzanie danych osobowych	uchylenie zaskarżonego wyroku WSA w Warszawie i decyzji GODO
72.	27.11.2008r. II SAWa 222/08	GHDEC-DOL/5-2707/3328,3329	Przetwarzanie danych osobowych	uchylenie zaskarżonej decyzji GODO
73.	27.11.2008r. II SAWa 526/08	DOL/POST-3708/2663,2664	Skarga na postanowienie GODO w przedmiocie przywróćcia terminu	uchylenie zaskarżonego postanowienia oraz poprzedzającego go postanowienia
74.	27.11.2008r. II SAWa 335/08	DOL/DEC-1/174,178/08	Przetwarzanie danych osobowych	odrzućcie skargi kasacyjnej
75.	27.11.2008r. II SAWa 903/08	GHDEC-DIS-254/1061608	Zaprzestanie przetwarzania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych pracowników Spółki	uchylenie zaskarżonej decyzji oraz decyzji poprzedzającej w zakresie punktu I ppkt 1 i ppk 2
76.	28.11.2008r. II SAWa 1165/08	DOL/DEC-35408/14530	Wniosek o nakazanie usunięcia danych osobowych	odmowa wstrzymania wykonania zaskarżonej decyzji
77.	4.12.2008r. II SAWa 917/08	DOL/DEC-25708/10742	Wniosek o nakazanie usunięcia danych	uchylenie zaskarżonej decyzji GODO
78.	12.10.2008r. II SAWa 615/08	DOL/DEC-18008/6930,6935	Przetwarzanie danych osobowych	oddalenie skargi
79.	19.12.2008r. IOSK 1466/08	DOL/DEC-39308/16162,16164,16167	Wniosek o nakazanie usunięcia danych osobowych	oddalenie zażalenia na postanowienie WSA w Warszawie przedmiocie wstrzymania wykonania zaskarżonej decyzji

**Informacje przekazane przez organy ścigania
w sprawach skierowanych w 2008 r.
przez Generalnego Inspektora Ochrony Danych Osobowych
zawiadomień o popełnieniu przestępstwa**

Informacja	Rok 2006	Rok 2007	Rok 2008
Umorzenie dochodzenia	2	17	18
Umorzenie dochodzenia w części	-	-	-
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	-	5	-
Umorzenie dochodzenia i odmowa podjęcia go na nowo	-	-	-
Wszczęcie dochodzenia	-	-	-
Odmowa wszczęcia dochodzenia	1	5	8
Wszczęcie śledztwa i jego umorzenie	-	2	-
Zawieszenie dochodzenia	-	2	-
Skierowanie sprawy do sądu	-	5	-
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	-	-	-
Brak informacji	-	-	5

Wykaz szkoleń przeprowadzonych przez GIODO w 2008 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	22.01.2008 r.	Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne
2.	28.01.2008 r.	Warszawa	uczestnicy obchodów Dnia Otwartego w Biurze GIODO z okazji Dnia Ochrony Danych Osobowych
3.	31.01.2008 r.	Bruksela	polscy eurodeputowani i pracownicy ich biur poselskich
4.	22.02.2008 r.	Warszawa	sędziowie i pracownicy Sądu Rejonowego w Gdyni
5.	28.02.2008 r.	Warszawa	pracownicy biur senatorskich
6.	29.02.2008 r.	Warszawa	pracownicy Ministerstwa Spraw Zagranicznych zatwierdzeni do wyjazdu na stanowiska konsuli realizujących postanowienia ustawy o Karcie Polaka
7.	03-05.03.2008 r.	Szklarska Poręba	kadra kierownicza Sądu Okręgowego we Wrocławiu
8.	04.03.2008 r.	Warszawa	pracownicy Fundacji Rozwoju Systemu Edukacji
9.	17.03. 2008 r.	Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne
10.	07.04.2008 r.	Warszawa	pracownicy Urzędu Komisji Nadzoru Finansowego
11.	14.04.2008 r.	Warszawa	pracownicy Urzędu Komisji Nadzoru Finansowego
12.	17.04.2008 r.	Warszawa	pracownicy Krajowej Izby Doradców Podatkowych
13.	22.04.2008 r.	Warszawa	kadra kierownicza i pracownicy Urzędu Zamówień Publicznych
14.	05.05.2008 r.	Warszawa	pracownicy Urzędu Komisji Nadzoru Finansowego
15.	06.05.2008 r.	Łomża	sędziowie Sądu Okręgowego w Łomży
16.	06.05.2008 r.	Warszawa	kadra kierownicza Ministerstwa Infrastruktury
17.	07.05.2008 r.	Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne
18.	14.05.2008 r.	Warszawa	dyrektorzy, naczelnicy oraz pracownicy Urzędu Zamówień Publicznych
19.	19.05.2008 r.	Nowy Sącz	pracownicy jednostek organizacyjnych Urzędu Miasta w Nowym Sączu oraz administratorzy danych osobowych
20.	21.05.2008 r.	Warszawa	pracownicy Funduszu Gwarantowanych Świadczeń Pracowniczych
21.	30.05.2008 r.	Legionowo	pracownicy Wydziału Bezpieczeństwa Teleinformatycznego Biura Ochrony Informacji Niejawnych Komendy Głównej Policji

22.	30.05.2008 r.	Warszawa	pracownicy Urzędu Komisji Nadzoru Finansowego
23.	05.06.2008 r.	Warszawa	radcy zrzeszeni w Krajowej Radzie Radców Prawnych
24.	06.06.2008 r.	Wrocław	spotkanie Generalnego Inspektora Ochrony Danych Osobowych ze studentami Uniwersytetu Wrocławskiego
25.	09.06.2008 r.	Warszawa	funkcjonariusze Komendy Głównej Straży Granicznej
26.	12.06.2008 r.	Warszawa	pracownicy Ministerstwa Spraw Zagranicznych
27.	13.06.2008 r.	Warszawa	pracownicy Urzędu Komisji Nadzoru Finansowego
28.	16.06.2008 r.	Poznań	pracownicy Wielkopolskiego Urzędu Wojewódzkiego w Poznaniu
29.	17.06.2008 r.	Poznań	pracownicy Urzędu Marszałkowskiego Województwa Wielkopolskiego w Poznaniu
30.	27.06.2008 r.	Warszawa	pracownicy Kancelarii Prezesa Rady Ministrów
31.	30.06.2008 r.	Warszawa	pracownicy Kancelarii Prezydenta RP
32.	30.06.2008 r.	Warszawa	pracownicy Urzędu Komisji Nadzoru Finansowego
33.	07.07.2008 r.	Legionowo	sluchacze Centrum Szkolenia Policji w Legionowie
34.	08.07.2008 r.	Słupsk	sluchacze Szkoły Policji w Słupsku
35.	09.07.2008 r.	Pila	sluchacze Szkoły Policji w Pile
36.	10.07.2008 r.	Katowice	sluchacze Szkoły Policji w Katowicach
37.	11.07.2008 r.	Katowice	sluchacze Szkoły Policji w Katowicach
38.	14.07.2008 r.	Szczytno	sluchacze Szkoły Policji w Szczytnie
39.	10.09.2008 r.	Warszawa	pracownicy Kancelarii Prezydenta RP
40.	15.09.2008 r.	Zgierz	kuratorzy zawodowi i społeczni I Zespołu Kuratorskiej Służby Sądowej Sądu Rejonowego w Zgierzu
41.	18.09.2008 r.	Wólka Milanowska	pracownicy Urzędu Marszałkowskiego Województwa Świętokrzyskiego
42.	19.09.2008 r.	Warszawa	pracownicy Komendy Głównej Policji
43.	24.09.2008 r.	Warszawa	pracownicy Ministerstwa Edukacji Narodowej
44.	29.09.2008 r.	Warszawa	pracownicy Komendy Głównej Policji
45.	30.09.2008 r.	Warszawa	pracownicy Komendy Głównej Policji
46.	02.10.2008 r.	Dębe	pracownicy Ministerstwa Zdrowia
47.	07.10.2008 r.	Jurata	pracownicy Komendy Głównej Policji
48.	07.10.2008 r.	Warszawa	sędziowie sądów apelacyjnych i okręgowych z terenu całej Polski

49.	13.10.2008 r.	Warszawa	pracownicy Związku Biur Porad Obywatelskich
50.	13.10.2008 r.	Zgierz	pracownicy I Zespołu Kuratorskiej Służby Sądowej Sądu Rejonowego w Zgierzu
51.	13.10.2008 r.	Olsztyn	pracownicy Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego
52.	15.10.2008 r.	Warszawa	pracownicy Kancelarii Prezydenta RP
53.	29.10.2008 r.	Warszawa	pracownicy Ministerstwa Edukacji Narodowej
54.	30.10.2008 r.	Warszawa	pracownicy Poczty Polskiej
55.	04.11.2008 r.	Warszawa	pracownicy Mazowieckiego Urzędu Wojewódzkiego
56.	05.11.2008 r.	Kraków	pracownicy 16 urzędów kontroli skarbowej oraz Departamentu Kontroli Skarbowej Ministerstwa Finansów
57.	17.11.2008 r.	Warszawa	pracownicy Kancelarii Senatu RP
58.	17.11.2008 r.	Warszawa	pracownicy Ministerstwa Spraw Zagranicznych
59.	18.11.2008 r.	Warszawa	pracownicy Ministerstwa Edukacji Narodowej
60.	21.11.2008 r.	Poznań	pracownicy Urzędu Miasta Poznania
61.	27.11.2008 r.	Włocławek	pracownicy Sądu Okręgowego we Włocławku
62.	28.11.2008 r.	Włocławek	pracownicy Sądu Okręgowego we Włocławku
63.	15.12.2008 r.	Bruksela	pracownicy Ambasady RP w Brukseli

**Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych
wydanych w 2008 roku w sprawach o wyrażenie zgody
na przekazanie danych osobowych za granicę**

L.p.	Data wydania decyzji/postanowienia	Nazwa podmiotu	Sygnatura decyzji/postanowienia
1.	2008-03-26	Celiński, Reczek i Tymiński Sp. J.	DESIWM/DEC-199/7656/08 decyzja umarzająca postępowanie
2.	2008-03-26	PwC Polska Sp. z o. o. Shared Services Sp. Komandytowa, Warszawa	DESIWM/DEC-197/7652/08 decyzja umarzająca postępowanie
3.	2008-03-26	I. Smith, K. Czarnecka-Żochowska, M. Ignatowicz, Doradcy Podatkowi Sp. komandytowa, Warszawa	DESIWM/DEC-196/7648/08 decyzja umarzająca postępowanie
4.	2008-06-13	PricewaterhouseCoopers Polska Sp. z o. o., Warszawa	DESIWM/DEC-360/14983/08 wyrażenie zgody na przekazanie danych
5.	2008-06-13	PwC Polska Sp. z o. o., Warszawa	DESIWM/DEC-359/14981/08 wyrażenie zgody na przekazanie danych
6.	2008-06-13	PricewaterhouseCoopers Sp. z o.o., Warszawa	DESIWM/DEC-361/14986/08 wyrażenie zgody na przekazanie danych
7.	2008-07-02	General Motors Polska Sp. z o.o., Warszawa	DESIWM/DEC-407/16702/08 wyrażenie zgody na przekazanie danych
8.	2008-07-21	Dorsey&Whitney, Londyn; Corbis Polska Sp. z o. o.	DESIWM/POST-216/18423/08 postanowienie dotyczące zwrotu wniosku z uwagi na nieuiszczenie należności tytułem opłaty skarbowej
9.	2008-12-10	Peek&Cloppenburg Sp. z o.o., Warszawa	DESIWM/DEC-805-34147/08 wyrażenie zgody na przekazanie danych
10.	2008-12-23	GlaxoSmithKline Services Sp. z o.o., Warszawa	DESIWM/DEC-870/35786/08 decyzja umarzająca
11.	2008-12-23	GlaxoSmithKline Consumer Healthcare Sp. z o.o., Warszawa	DESIWM/DEC-868/35783/08 decyzja umarzająca postępowanie
12.	2008-12-04	ABN AMRO (Polska) S.A.	DESIWM/POST-358/33638/08 postanowienie zawieszające postępowania na wniosek strony
13.	2008-12-23	GlaxoSmithKline GSK Comercial Sp. z o.o., Warszawa	DESIWM/DEC-869/35785/08 decyzja umarzająca postępowanie