

**Generalny Inspektor
Ochrony Danych Osobowych**

**SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH
W ROKU 2009**

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 2009 r. do 31 grudnia 2009 r.

SPIS TREŚCI

Część I. Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych

1. Informacje ogólne	5
2. Biuro Generalnego Inspektora Ochrony Danych Osobowych	6
2.1 Struktura organizacyjna	6
2.2 Pracownicy Biura GIODO	7
2.3 Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2009 rok	7

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

1. Informacje ogólne	8
2. Kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych	10
2.1 Czynności kontrolne	10
2.2 Kontrola przetwarzania danych osobowych w wybranych obszarach	11
2.2.1 Administracja publiczna	11
2.2.2 Bezpieczeństwo publiczne	12
2.2.3 Sądy, prokuratura, komornicy	13
2.2.4 Internet	13
2.2.5 Telekomunikacja	15
2.2.6 Zatrudnienie	16
2.2.7 Biura obrotu nieruchomościami	19
2.2.8 Karty miejskie	21
2.2.9 Inne	22
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych	23
3.1 Wydawanie decyzji	23
3.2 Decyzje w wybranych obszarach	27
3.2.1 Administracja publiczna	27
3.2.2 Sądy, prokuratura, komornicy	32
3.2.3 Banki i inne instytucje finansowe	32
3.2.4 Internet	37
3.2.5 Marketing	39

3.2.6 Sektor mieszkalnictwa	40
3.2.7 System Informacyjny Schengen	42
3.2.8 Telekomunikacja	43
3.2.9 Zatrudnienie	43
3.2.10 Ubezpieczenia społeczne, majątkowe i osobowe	47
3.2.11 Zdrowie	48
3.2.12 Inne	49
4. Prowadzenie rejestru zbiorów danych osobowych oraz udzielanie informacji o zarejestrowanych zbiorach	54
5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych	61
6. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych	76
6.1 Interpretacja przepisów	77
6.2 Działalność informacyjna	95
6.2.1. Współpraca ze środkami masowego przekazu	95
6.2.2. Publikacje	99
6.2.3. Szkolenia, staże, wymiana pracowników	100
6.2.4. Konkursy	103
6.2.5. Konferencje, seminaria, spotkania	105
6.2.6. Internet	113
6.2.7. Inne informacje	115
7. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych	117
7.1 Międzynarodowe spotkania i konferencje	122
7.2 Wizyty robocze	125
7.3 Warsztaty Rozpatrywania Spraw	126
Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2009 roku	127
Część IV. Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych	152

Załączniki

Załącznik nr 1	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2009 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego.....	156
Załącznik nr 2	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2009 do podmiotów prywatnych	161
Załącznik nr 3	Wykaz kontroli przeprowadzonych w 2009 roku	165
Załącznik nr 4	Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2009 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych	178
Załącznik nr 5	Informacje przekazane przez organy ścigania w sprawach skierowanych w 2009 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa	186
Załącznik nr 6	Wykaz szkoleń przeprowadzonych przez GODO w 2009 r.	187
Załącznik nr 7	Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych wydanych w 2009 roku w sprawach o wyrażenie zgody na przekazanie danych osobowych za granicę...	189

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 – rozporządzenia Ministra Spraw Wewnętrznych i Administracji:

- a) 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 z 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 ob. jętych 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) z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536) – wydane na podstawie art. 46a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia,
- c) 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).

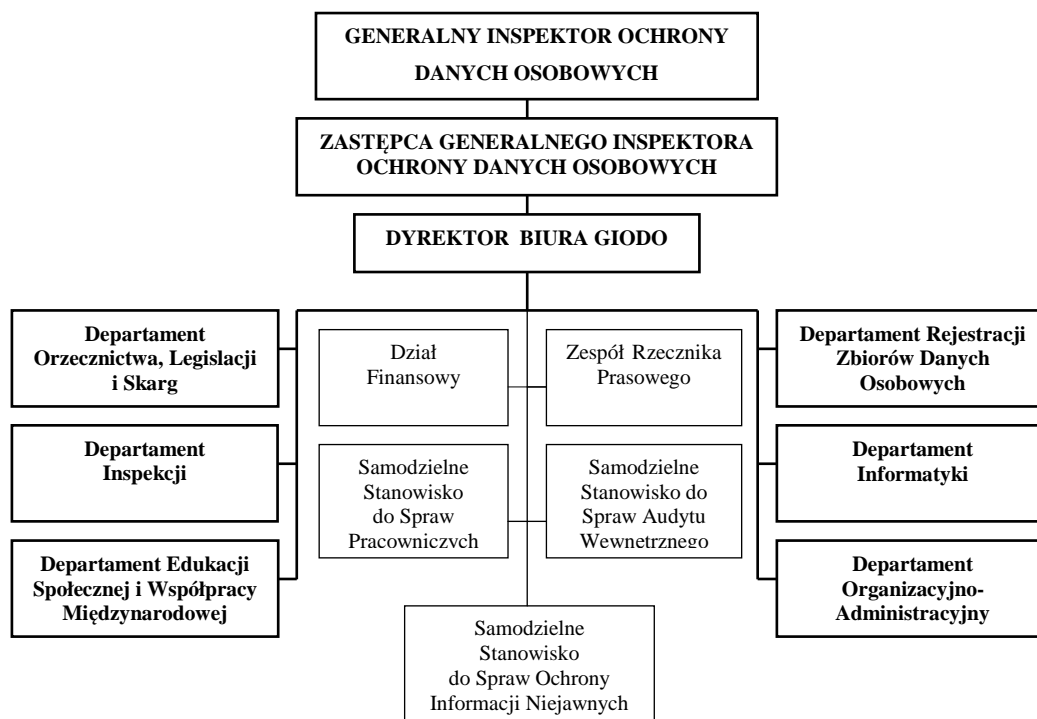
Na system ochrony danych osobowych składają się też przepisy szczególne innych ustaw, które regulują kwestie związane z przetwarzaniem danych osobowych przez różne podmioty. Podmioty publiczne, w myśl zasady praworządności wyrażonej w art. 7 Konstytucji Rzeczypospolitej Polskiej, działają wyłącznie na 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. 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 Biura Generalnego Inspektora Ochrony Danych Osobowych.

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



Generalny Inspektor wykonuje swoje zadania bezpośrednio lub przy pomocy Dyrektora Biura, dyrektorów jednostek organizacyjnych Biura oraz innych osób wskazanych w Regulaminie Organizacyjnym.²

2.2. Pracownicy Biura GIODO

Stan zatrudnienia w Biurze GIODO na 31 grudnia 2009 r. wyniósł 119,5 etatów (pełne etaty). Na stanowiskach merytorycznych zatrudnionych było 107 osób, a na stanowiskach pomocniczych 16 osób. Wyższe wykształcenie posiadało 100 pracowników, w tym 71 legitymowało się wykształceniem wyższym prawniczym.

Zatrudnienie w poszczególnych jednostkach organizacyjnych Biura GIODO na koniec 2009 r. przedstawia się następująco:

- GIODO - 1 osoba
- Zastępca GIODO – 1 osoba
- Asystent GIODO – 1 osoba
- Dyrektor Biura – 1 osoba
- Zespół Rzecznika Prasowego [ZRP] – 4 osoby
- Departament Edukacji Społecznej i Współpracy Międzynarodowej [DESiWM] – 10 osób
- Departament Informatyki [DIF] – 15 osób,
- Departament Inspekcji [DIS] – 17 osób,
- Departament Orzecznictwa, Legislacji i Skarg [DOLiS] – 29 osób,
- Departament Rejestracji Zbiorów Danych Osobowych [DRZDO] – 17 osób,
- Departament Organizacyjno-Administracyjny [DOA] – 17 osób,
- Dział Finansowy – 3 osoby
- Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby
- Samodzielne Stanowisko ds. Pracowniczych – 2 osoby
- Samodzielne Stanowisko ds. Audytu – 1 osoba

2.3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2009 r.

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2009 r. wynosił: 13 717 tys. zł, w tym:

wynagrodzenia	9 291 tys. zł
pochodne od wynagrodzeń	1 432 tys. zł

² 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.

wydatki majątkowe	70 tys. zł
pozostałe wydatki	2 924 tys. zł

Wydatki zrealizowane przez GIODO w 2009 roku wyniosły: 13 657 tys. zł, w tym:

wynagrodzenia	9 288 tys. zł
pochodne od wynagrodzeń	1 428 tys. zł
wydatki majątkowe	70 tys. zł
pozostałe wydatki	2 871 tys. zł

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 takich operacjach, jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych. Przy czym pod pojęciem dane osobowe należy rozumieć 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.³ 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,

³ 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.

- 2) celowości – dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane 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 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.

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, w godzinach od 6.00 do 22.00, 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 przesłuchiwania 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, a także zlecenia sporządzania ekspertyz i opinii.

Wymienionym uprawnieniom towarzyszy obowiązek kierownika jednostki kontrolowanej oraz osoby fizycznej będącej administratorem danych, 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, tzn. 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. 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 2009 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził łącznie **220 kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy.

2.2.1 Administracja publiczna

W okresie sprawozdawczym przeprowadzono **11 kontroli w wybranych urządach pracy**.⁴ Zakresem kontroli objęto zabezpieczenie przez urzędy pracy danych osobowych interesantów, a także sposób przetwarzania danych osób zgłaszających się w celu załatwienia sprawy w urzędzie za pośrednictwem Internetu.

Na podstawie ustaleń kontrolnych należy pozytywnie ocenić poziom spełnienia przez ww. podmioty wymogów określonych w przepisach o ochronie danych osobowych, bowiem w dziesięciu urządach pracy nie stwierdzono uchybień w zakresie objętym kontrolą.

W jednym przypadku zastrzeżenia wzbudził sposób dopełnienia przez urząd pracy obowiązku informacyjnego (tzn. osób, które za pomocą systemu informatycznego ustalały termin wizyty w urzędzie, nie informowano o prawie dostępu do treści swoich danych oraz prawie ich poprawiania oraz o tym, że podanie danych jest niezbędne w celu dokonania rezerwacji terminu wizyty), a także brak należytego zabezpieczenia danych osobowych, polegający na niezastosowaniu szyfrowanych łączy podczas transferu danych w przypadku rejestracji użytkownika w systemie informatycznym. Ponadto szafy z dokumentacją zawierającą dane osobowe nie były wyposażone w zamki i znajdowały się w pomieszczeniach, w których przyjmowani byli interesanci.

Zakresem kontroli objęto również sposób przetwarzania danych osób zgłaszających się w celu załatwienia sprawy w urzędzie za pośrednictwem Internetu. W urządach pracy funkcjonują bowiem Elektroniczne Urzędy Podawcze, które stwarzają możliwość przesłania wniosków (formularzy) z wykorzystaniem sieci. W celu skorzystania z elektronicznej skrzynki podawczej użytkownik musi

⁴ Np. DIS-K-421/121/09, DIS-K-421/168/09, DIS-K-421/172/09 i DIS-K-421/195/09.

otworzyć stronę internetową Ministerstwa Pracy i Polityki Społecznej i wypełnić odpowiedni formularz przyporządkowany do konkretnej sprawy. Transmisja danych poprzez elektroniczną skrzynkę podawczą odbywa się za pomocą łączy szyfrowanych protokołem https. Wnioski z elektronicznej skrzynki podawczej wpływają na skrzynkę mailową właściwego urzędu pracy. Z uwagi na to, że wysłanie wniosku za pomocą elektronicznej skrzynki podawczej wymaga posiadania kwalifikowanego podpisu elektronicznego, z Elektronicznego Urzędu Podawczego korzystają wyłącznie pracodawcy.

2.2.2 Bezpieczeństwo publiczne

W okresie sprawozdawczym, w związku z obecnością Polski w strefie Schengen, przeprowadzonych zostało **7 kontroli podmiotów uprawnionych do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych SIS oraz w celu wglądu do danych SIS**. Tego rodzaju kontrolami zostały objęte przede wszystkim sądy.⁵ 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 (Dz. U. Nr 165, poz. 1170 z późn. zm.).

Na podstawie materiału dowodowego zebranego w toku przeprowadzonych kontroli stwierdzono, że użytkownicy systemu informatycznego wykorzystywanego w sądach do dostępu do danych SIS nie mają możliwości dokonywania zmiany hasła dostępu do tego systemu. Ponadto kontrole wykazały, że w niektórych sądach nie została opracowana dokumentacja stanowiąca politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych lub dokumentacja ta nie uwzględniała systemu informatycznego, za pośrednictwem którego realizowany był dostęp do danych SIS. Częstym uchybieniem było także umożliwienie dostępu do danych SIS osobom, które nie odbyły szkolenia z zakresu bezpieczeństwa i ochrony danych SIS, wymaganego zgodnie z art. 25 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej.⁶ W pojedynczych przypadkach stwierdzono ponadto, że program antywirusowy zainstalowany na stanowisku dostępowym do danych SIS nie posiadał aktualnej bazy antywirusowej oraz, że w ewidencji osób upoważnionych do przetwarzania danych osobowych nie zostały uwzględnione uprawnienia osób dopuszczonych do przetwarzania danych w systemie informatycznym wykorzystywanym w sądach do dostępu do danych SIS. W związku ze stwierdzonymi nieprawidłowościami w procesie przetwarzania danych

⁵ Np. DIS-K-421/84/09, DIS-K-421/93/09, DIS-K-421/117/09.

⁶ Art. 25 ust. 1. Organ uprawniony do wykorzystywania danych poprzez Krajowy System Informatyczny jest obowiązany do przeszkolenia z zakresu bezpieczeństwa i ochrony danych wszystkich osób mających dostęp do Krajowego Systemu Informatycznego.

osobowych, Generalny Inspektor skierował do Ministra Sprawiedliwości, który administracyjnie i technicznie wspomaga sądy w zakresie dostępu do SIS oraz pełni nadzór administracyjny nad czynnościami sądów, żądanie podjęcia działań mających na celu usunięcie uchybień.⁷

2.2.3 Sądy, prokuratura, komornicy

W okresie sprawozdawczym przeprowadzono **19 kontroli u komorników sądowych**.⁸ Podczas 7 z nich nie stwierdzono uchybień. Większość z przeprowadzonych kontroli wykazała nieprawidłowości w procesie przetwarzania danych osobowych przy użyciu systemu informatycznego. Stwierdzane w tym zakresie uchybienia dotyczyły przede wszystkim nie zapewnienia przez system informatyczny służący do przetwarzania danych osobowych odnotowania źródła pochodzenia danych oraz sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie ww. informację.

Stwierdzono ponadto, że niektórzy komornicy sądowi nie zastosowali środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności nie zabezpieczyli danych przed ich udostępnieniem osobom nieupoważnionym lub zabranieniem przez osobę nieuprawnioną, gdyż nie zabezpieczyli właściwie akt osobowych pracowników i uczestników postępowań komorniczych oraz nie odnotowywali faktu wynoszenia akt spraw komorniczych w celu podjęcia czynności egzekucyjnych w terenie. Zdarzały się też uchybienia dotyczące dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, takie jak np. pominięcie w instrukcji zarządzania systemem informatycznym informacji dotyczących jednego z systemów informatycznych służących do przetwarzania danych osobowych. Z uwagi na to, że administratorzy danych niezwłocznie podejmowali działania polegające na usuwaniu uchybień stwierdzonych w toku prowadzonych postępowań administracyjnych, wydawane były decyzje umarzające postępowania.⁹

2.2.4 Internet

W okresie sprawozdawczym u przedsiębiorców prowadzących portale internetowe przeprowadzono łącznie **26 kontroli**,¹⁰ w tym **17 kontroli sektorowych**.

Do najczęstszych uchybień stwierdzonych w ich toku należało naruszanie obowiązku zgłoszenia do rejestracji Generalnemu Inspektorowi prowadzonych zbiorów danych osobowych oraz nienależyte zabezpieczenie danych osobowych, polegające na niezastosowaniu środków ochrony

⁷ Pismo z 23.09.2009 r. DIS-K-421/84/09/34653.

⁸ Np. kontrole DIS-K-421/146/09, DIS-K-421/148/09, DIS-K-421/163/09, DIS-K-421/173/09 i DIS-K-421/182/09.

⁹ Np. DIS/DEC-1174/43217/09, DIS/DEC-1237/46117/09, DIS/DEC-1263/46990/09 i DIS/DEC-1277/47648/09.

kryptograficznej wobec danych osobowych przesyłanych przy użyciu sieci publicznej, a także wobec danych wykorzystywanych do uwierzytelniania podczas logowania do portalu internetowego. Jednym z najsłabszych punktów w bezpieczeństwie przetwarzania danych w portalach internetowych, w tym głównie w portalach typu społecznościowego, było także brak zapewnienia wiarygodnej informacji o źródłach wprowadzania danych do serwisu. Zidentyfikowano w tym zakresie dwa zasadnicze problemy. Pierwszy to ograniczona liczba informacji o rejestrujących się w danym serwisie osobach. Często informacje te ograniczone były jedynie do adresu poczty elektronicznej lub loginu w danym serwisie. Drugim problemem była wiarygodność wprowadzanych danych. W przypadku wykorzystywania do identyfikacji użytkownika serwisu wyłącznie adresu poczty elektronicznej, często sprawdzane jest jedynie istnienie takiego adresu w chwili rejestrowania się w danym serwisie, bez żadnych dalszych działań w zakresie określenia tożsamości osób posługujących się tym adresem. W niektórych przypadkach adresy e-mail były jedynymi danymi osobowymi przetwarzanymi w serwisie i były to dane pozyskane bez jakiegokolwiek weryfikacji tożsamości osób, które się nimi posługują lub posługiwały. Ponadto w wielu serwisach istnienie wskazanego adresu poczty elektronicznej wymagane było wyłącznie do utworzenia konta w serwisie, bez potrzeby jego dalszego utrzymywania.

Jednostki kontrolowane miały również duże problemy z prawidłowym wypełnieniem obowiązków dotyczących przetwarzania danych osobowych przy użyciu systemów informatycznych. Systemy informatyczne służące do przetwarzania danych osobowych nie zapewniały m.in. odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz niezarejestrowania w systemie odrębnego identyfikatora dla każdego użytkownika posiadającego dostęp do danych osobowych przetwarzanych w systemie informatycznym. W kilku przypadkach stwierdzono, że osoby, których dane dotyczą, nie mają zapewnionej swobody w wyrażaniu zgody na przetwarzanie danych osobowych dla celów związanych z korzystaniem z portalu i w celu reklamy, badania rynku oraz zachowań i preferencji usługobiorców, dla celów statystycznych oraz działań marketingowych. Ponadto ustalono, że niektórzy poddani kontroli przedsiębiorcy prowadzący portale internetowe nie opracowali i nie wdrożyli dokumentacji, o której mowa § 3 ust. 1 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych¹⁰, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

¹⁰ Np. DIS-K-421/6/09, DIS-K-421/11/09, DIS-K-421/15/09, DIS-K-421/25/09, DIS-K-421/33/09, DIS-K-421/45/09, DIS-K-421/61/09 i DIS-K-421/86/09.

¹¹ § 3 ust. 1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją”; ust. 2. Dokumentację,

a także pozyskiwali szerszy zakres danych osobowych pracowników (m.in. o nazwisko rodowe matki) niż wynikający z przepisów art. 22¹ § 1, § 2 i § 4 Kodeksu pracy.¹² Pojedyncze kontrole wykazały ponadto przetwarzanie bez podstawy prawnej danych o nałogach osób korzystających z portalu oraz niedopełnienie wobec użytkowników portalu obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych.¹³

W związku z uchybieniami stwierdzonymi w toku kontroli wydane zostały decyzje nakazujące usunięcie uchybień w procesie przetwarzania danych osobowych oraz decyzje umarzające postępowanie w zakresie nieprawidłowości usuniętych przez jednostki kontrolowane w toku postępowania.¹⁴ W wydanych decyzjach Generalny Inspektor nakazał m.in. zapewnienie użytkownikom opcjonalności w kwestii wyrażenia zgody na przetwarzanie danych osobowych, odrębnie dla celów związanych z korzystaniem z portalu i w celu reklamy, badania rynku oraz zachowań i preferencji usługobiorców, dla celów statystycznych oraz działań marketingowych. Decyzje nakazujące dotyczyły zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi i spełnienia obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, wobec osób, których dane dotyczą.

2.2.5 Telekomunikacja

W 2009 r. przeprowadzono **7 kontroli u dostawców usług telekomunikacyjnych**. Cztery kontrole¹⁵ zostały przeprowadzone w związku z realizowanym przez Grupę Roboczą Art. 29 badaniem wdrażania przez kraje członkowskie Unii Europejskiej dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę

o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej; ust. 3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

¹² 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.

¹³ Art. 24 ust. 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.

¹⁴ Np. DIS/DEC-258/11009/09, DIS/DEC-390/17359/09, DIS/DEC443/19249/09, DIS/DEC-287/13013/09, DIS/DEC-1327/48391/09, DIS/DEC-583/23647/09, DIS/DEC-410/18720/09, DIS/DEC-827/30231/09, DIS/DEC-1086/39944/09, DIS/DEC-1055/38764/09, DIS/DEC/-910/33153/09, DIS/DEC-1289/47989/09.

2002/58/WE (Dz. Urz. UE L z 2006 r. Nr 105, poz. 54). Zakresem kontroli objęto zagadnienia wskazane na formularzu „Wspólne badanie wdrażania dyrektywy o zatrzymywaniu danych: kwestionariusz” opracowanym przez Grupę Roboczą Art. 29 ds. ochrony danych. Zagadnienia te dotyczyły między innymi zakresu przechowywanych danych o ruchu oraz zastosowanych rozwiązań w celu zapewnienia bezpieczeństwa informatycznego, a w szczególności sposobów identyfikacji i autoryzacji użytkowników oraz zastosowanych metod szyfrowania danych. Dokonane ustalenia zostały wykorzystane do sporządzenia raportu, który został przesłany Grupie Roboczej Art. 29.

2.2.6 Zatrudnienie

W okresie sprawozdawczym skontrolowano **35 pracodawców, w tym 20 kontroli przeprowadzono w ramach tzw. kontroli sektorowej.**¹⁶ Zakresem kontroli objęto dane osobowe pracowników oraz kandydatów do pracy. W toku 6 kontroli nie stwierdzono uchybień w procesie przetwarzania danych osobowych.

Przeprowadzone kontrole wykazały, że pracodawcy przetwarzający dane osobowe mieli problemy z prawidłowym wykonaniem obowiązków określonych w art. 24 ust. 1 ustawy o ochronie danych osobowych, tj. z realizacją obowiązku informacyjnego wobec osób, których dane dotyczą. Obowiązek informacyjny nie był realizowany w zakresie wszystkich okoliczności wymienionych w ww. przepisie ustawy o ochronie danych osobowych lub był realizowany w niepełnym zakresie, np. z pominięciem informacji o prawie dostępu do treści swoich danych oraz ich poprawiania, dobrowolności lub obowiązku podania danych. Jeden z administratorów informował natomiast, iż dane nie będą udostępniane innym podmiotom, mimo że dane były przekazywane do innej spółki. W toku kontroli stwierdzono także sytuacje powierzenia przetwarzania danych osobowych w ramach zlecenia obsługi księgowej i archiwizacji, mimo iż pracodawca nie zawarł ze zleceniobiorcą pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 ustawy o ochronie danych osobowych. Do częstych uchybień stwierdzanych w toku kontroli należało naruszanie art. 22¹ § 1 Kodeksu pracy, gdyż zakres przetwarzanych danych wykraczał poza katalog danych wskazany w powołanym przepisie, np. dane obejmowały nazwisko rodowe matki pracownika wpisywane do kwestionariusza osobowego. Ponadto przeprowadzane były testy określające przydatność kandydata do wykonywania pracy na danym stanowisku, w wyniku których pracodawca otrzymywał dodatkowe informacje dotyczące cech kandydata do pracy w następujących kategoriach: prawdomówność, kradzież (skłonność do kradzieży mienia/pieniędzy), obsługa klienta (czy jest agresywny, niecierpliwy, niegrzeczny czy też pomocny, uprzejmy, bezkonfliktowy), normy (czy ma tendencje do przekraczania norm i łamania przepisów) itd. W wyniku prowadzenia testów

¹⁵ Kontrole DIS-K-421/65/09, DIS-K-421/67/09, DIS-K-421/68/09 i DIS-K-421/65/09.

¹⁶ Np. kontrole DIS-K-421/81/09, DIS-K-421/91/09, DIS-K-421/102/09, DIS-K-421/112/09 i DIS-K-421/134/09.

pozyskano również informacje o tym, czy kandydat do pracy był skazany za przestępstwo oraz czy widnieje w rejestrze skazanych.

Szczególny przypadek poszerzenia zakresu danych względem katalogu wskazanego w art. 22¹ § 1 Kodeksu pracy polegał na przetwarzaniu danych biometrycznych pracowników w celu rejestracji czasu ich pracy. Linie papilarne pobierane były z palców dłoni poprzez urządzenie skanujące i następnie przetwarzane na zapis cyfrowy. Tego typu praktyki miały miejsce u 5 skontrolowanych pracodawców. Zastrzeżenia Generalnego Inspektora budził także sposób wyrażania przez kandydatów do pracy zgody na przetwarzanie ich danych osobowych. Stwierdzone w tym zakresie uchybienia związane były m.in. z treścią oświadczenia o wyrażeniu zgody, z którego nie wynikało w sposób jednoznaczny, że osoby, których dane dotyczą, godzą się na przetwarzanie ich danych osobowych. Zastrzeżenia budziła także konstrukcja klauzuli zgody, w ramach której umieszczonych zostało kilka oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych w różnych celach.

Kontrole wykazały również, że niektórzy poddani kontroli pracodawcy mieli problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Uchybienia w tym zakresie polegały na nieopracowaniu procedury regulującej sposób postępowania z kluczami do pomieszczeń, w których są przetwarzane dane osobowe, na przechowywaniu dokumentacji w szafach niewyposażonych w zamki lub na otwartym regale, a także na ustawieniu monitora komputera (na którym są przetwarzane dane osobowe), w sposób umożliwiający wgląd w te dane osobom nieupoważnionym. W nielicznych przypadkach stwierdzono, że do przetwarzania danych osobowych dopuszczone zostały osoby nieposiadające upoważnień nadanych przez administratora danych, brak było ewidencji osób upoważnionych do przetwarzania danych osobowych lub nie zawarto w niej wszystkich wymaganych elementów, określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych,¹⁷ np. identyfikatorów użytkowników systemu informatycznego oraz daty ustania i zakresu upoważnienia do przetwarzania danych osobowych. Ustalono również, że opracowane przez kontrolowanych administratorów danych dokumenty stanowiące politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, nie zawierały wszystkich elementów wskazanych w § 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.¹⁸

¹⁷ 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.

¹⁸ § 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

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 oraz sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie wszystkie informacje, o których mowa w § 7 ust. 1 ww. rozporządzenia.¹⁹ Do częstych uchybień należało również zmienianie hasła uwierzytelnienia do systemów informatycznych rzadziej niż co 30 dni. Kilka z przeprowadzonych kontroli wykazało ponadto, że w systemach informatycznym służących do przetwarzania danych osobowych nie zostały zastosowane mechanizmy kontroli dostępu do tych danych, tj. dostęp do systemu nie wymagał wprowadzenia identyfikatora i dokonania uwierzytelnienia lub kilku użytkownikom systemu informatycznego przydzielony został wspólny identyfikator. W pojedynczych przypadkach stwierdzono brak zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, niewykonywanie na bieżąco kopii zapasowych oraz przechowywanie kopii zapasowych w miejscu, które nie zapewniało ich zabezpieczenia przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

W związku z uchybieniami stwierdzonymi w toku kontroli wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości już usuniętych w toku postępowania.²⁰ W wydanych decyzjach Generalny Inspektor nakazał m.in. usunięcie danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników przetwarzanych w celu ewidencji czasu pracy oraz zaprzestanie zbierania danych w tym zakresie, usunięcie danych osobowych kandydatów do pracy

między 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.

¹⁹ § 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.

pozyskanych w wyniku przeprowadzenia za pomocą systemu informatycznego testów określających przydatność do wykonywania pracy i zaprzestanie zbierania danych w tym zakresie. Nakazanie usunięcia dotyczyło też zaprzestania zbierania takich danych, jak nazwisko rodowe matki pracownika, a także zapewnienie kandydatom do pracy swobody wyrażenia zgody na przetwarzanie danych osobowych w celach rekrutacji prowadzonych w przyszłości i udostępniania danych innym podmiotom.

2.2.7 Biura obrotu nieruchomościami

W 2009 r. przeprowadzono **16 kontroli podmiotów zajmujących się pośrednictwem w obrocie nieruchomościami**, w tym 2 podmiotów zajmujących się rzeczoznawstwem majątkowym.²¹ Zakresem kontroli objęto dane osobowe klientów, dane osób pozyskiwane w związku ze sporządzaniem przez rzeczoznawców majątkowych operatów szacunkowych, dane pracowników oraz kandydatów do pracy przetwarzane przez te podmioty. W toku 8 kontroli nie stwierdzono uchybień w procesie przetwarzania danych osobowych w zakresie objętym kontrolą.

Przeprowadzone kontrole wykazały, że niektóre podmioty miały problemy z prawidłowym wypełnieniem obowiązku, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych. Uchybienia w tym zakresie dotyczyły w szczególności nieudzielania osobom, których dane dotyczą, informacji o prawie dostępu do treści swoich danych i ich poprawiania oraz o dobrowolności podania danych. W jednym przypadku kontrolowana jednostka w ogóle nie realizowała wobec swoich klientów obowiązku informacyjnego. Do częstych nieprawidłowości należało również niedopełnianie przez podmioty zajmujące się pośrednictwem w obrocie nieruchomościami obowiązku aktualizacji informacji dotyczących zbiorów danych osobowych zawartych w zgłoszeniach zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi.

Kontrolowane jednostki miały problemy z prawidłowym wykonaniem obowiązków określonych w rozdziale 5 ustawy o ochronie danych osobowych. Nieprawidłowości dotyczyły w szczególności niezastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych (np. przechowywanie dokumentacji zawierającej dane osobowe w pomieszczeniu, które nie zostało zabezpieczone przed dostępem osób nieupoważnionych; brak zabezpieczenia serwera, na którym przetwarzane były dane osobowe, przed dostępem osób nieupoważnionych), niezawarcia w ewidencji osób upoważnionych do przetwarzania danych osobowych wszystkich informacji określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych (np. daty nadania i ustania oraz zakresu upoważnienia do przetwarzania danych osobowych

²⁰ Np. decyzje nr DIS/DEC-1175/43655/09, DIS/DEC-1172/43212/09, DIS/DEC-1206/44991/09, DIS/DEC-1189/44066/09, DIS/DEC-999/37016/09, DIS/DEC-1139/41929/09, DIS/DEC-1056/38787/09, DIS/DEC-934/34058/09, DIS/DEC-1106/40727/09, DIS/DEC-634/25708/09, DIS/DEC-920/33576/09 i DIS/DEC-1208/45000/09.

i identyfikatora użytkownika w systemie informatycznym), a w polityce bezpieczeństwa elementów wskazanych w § 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (np. wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe).

Niektóre kontrole wykazały również uchybienia w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych, dotyczące w szczególności niezapewnienia przez systemy informatyczne służące do przetwarzania danych osobowych odnotowania m.in. daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego te dane osobowe, niezmienniania hasła uwierzytelnienia bądź zmieniania go rzadziej niż co 30 dni, braku wymaganej liczby znaków (co najmniej 8) w hasłach służących do uwierzytelniania użytkowników w systemach, które posiadają dostęp do sieci Internet oraz przyznania jednego identyfikatora dwóm użytkownikom systemu informatycznego.

W pojedynczych przypadkach inspektorzy stwierdzili brak podstawy prawnej przetwarzania danych osób, które podały swoje dane osobowe za pośrednictwem infolinii, zawarcie w umowach pośrednictwa klauzuli zgody na przetwarzanie danych osobowych, które nie pozwalały klientowi na podjęcie swobodnej decyzji, na rzecz którego z podmiotów wskazanych w klauzuli wyraża zgodę na przetwarzanie danych w celach marketingowych oraz brak określenia zakresu przetwarzania danych w umowie powierzenia przetwarzania danych osobowych.

W związku z uchybieniami stwierdzonymi w toku kontroli wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości już usuniętych przez jednostki kontrolowane w toku postępowania.²² W wydanych decyzjach Generalny Inspektor nakazał m.in. dokonanie aktualizacji zgłoszenia zbioru danych osobowych, uzupełnienie ewidencji osób upoważnionych do przetwarzania danych osobowych o zakres upoważnienia do przetwarzania danych oraz o identyfikator użytkownika, szyfrowanie danych osobowych przesyłanych za pośrednictwem sieci publicznej i dopełnienie obowiązku informacyjnego wynikającego z art. 24 ust. 1 ustawy, wobec osób, których dane dotyczą.

²¹ Np. kontrole DIS-K-421/23/09, DIS-K-421/31/09, DIS-K-421/37/09, DIS-K-421/39/09, DIS-K-421/51/09, DIS-K-421/64/09 i DIS-K-421/73/09.

²² Np. decyzje DIS/DEC-352/15651/09, DIS/DEC-411/18722/09, DIS/DEC-444/19255/09, DIS/DEC-586/23654/09 i DIS/DEC-555/22716/09.

2.2.8 Karty miejskie

W 2009 r. przeprowadzono **11 kontroli podmiotów zajmujących się transportem miejskim**.²³ Zakresem ww. kontroli objęto przetwarzanie danych osobowych w związku z wydawaniem i obsługą tzw. spersonalizowanych kart miejskich – nośników elektronicznych biletów długookresowych.

Największe zastrzeżenia inspektorów wzbudził zakres przetwarzanych danych osobowych pasażerów w celu wydania i obsługi spersonalizowanych kart miejskich. Niektóre z przeprowadzonych kontroli wykazały bowiem, iż na kartach tych kodowany jest nr PESEL ich użytkowników, w celu identyfikacji użytkownika karty oraz w celu kontroli biletów. Kwestionowano ponadto przetwarzanie wizerunku osób, które złożyły wniosek o wydanie spersonalizowanej karty miejskiej, przetwarzanie numeru tej karty w trakcie dokonywania kolejnych skasowań, jeśli kasowania nie miały na celu aktywacji biletu zakodowanego na karcie oraz danych o ruchu pasażerów komunikacji miejskiej (tzw. dane geolokalizacyjne) w zakresie m.in. daty i godziny skasowania, numeru linii autobusowej oraz numeru bocznego autobusu, w którym dokonano skasowania biletu. Konsekwencją gromadzenia ww. danych było bowiem naruszenie przez takie podmioty zasady adekwatności danych w stosunku do celu przetwarzania, wyrażonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Na podstawie wyników kontroli stwierdzono również, że niektóre podmioty zajmujące się transportem miejskim nie zapewniły, aby dane użytkowników spersonalizowanej karty miejskiej były przetwarzane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania tych danych. Podmioty te nie opracowały bowiem procedur, jak również nie ustaliły terminów usuwania danych osobowych ze zbioru w przypadku, gdy cel ich przetwarzania zostanie osiągnięty. Większość kontrolowanych jednostek nie dopełniła także obowiązku dokonania aktualizacji informacji zawartych we wnioskach składanych podczas rejestracji zbiorów danych osobowych u Generalnego Inspektora m.in. w zakresie określenia podstaw prawnych, celu i zakresu przetwarzania danych osobowych w zbiorze. Do nielicznych należały natomiast uchybienia polegające na niedopełnieniu w pełnym zakresie wobec osób, których dane dotyczą, obowiązku informacyjnego określonego w art. 24 ust. 1 ustawy o ochronie danych osobowych, na przetwarzaniu danych o stanie zdrowia pasażerów korzystających ze spersonalizowanej karty miejskiej bez podstawy prawnej wskazanej w art. 27 ust. 2 ustawy o ochronie danych osobowych oraz na niespełnieniu wymogów dotyczących zabezpieczenia danych osobowych o charakterze formalnym (m.in. niewyznaczenie administratora bezpieczeństwa informacji, niezawarcie w dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wszystkich elementów wynikających z § 4 i § 5 ww. rozporządzenia i dopuszczenie do przetwarzania danych osobowych osób

²³ Np. kontrole DIS-K-421/88/09, DIS-K-421/113/09, DIS-K-421/140/09 i DIS-K-421/154/09.

nieposiadających upoważnień nadanych przez administratora danych) oraz technicznym (m.in. zmienianie haseł uwierzytelnienia do systemów informatycznych, w których przetwarzane są dane osobowe, rzadziej niż co 30 dni i brak wykorzystywanych do uwierzytelnienia środków kryptograficznej ochrony danych, które są przesyłane w sieci publicznej).

W związku ze stwierdzonymi w toku kontroli uchybieniami w procesie przetwarzania danych osobowych, Generalny Inspektor wydał decyzje²⁴ nakazujące usunięcie danych dotyczących wizerunków osób, którym wydano spersonalizowaną kartę miejską i numerów PESEL zakodowanych na karcie, a także określenie terminów usuwania danych pozyskanych za pomocą wniosków o wydanie spersonalizowanej karty miejskiej, które powinny być przetwarzane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2.2.9 Inne

W okresie sprawozdawczym w podmiotach nienależących do sektorów omówionych w poprzednich rozdziałach przeprowadzono **34 kontrole** zgodności przetwarzania danych z przepisami o ochronie danych osobowych.²⁵ Grupa tych podmiotów jest bardzo zróżnicowana i obejmuje m.in. podmioty wykonujące działalność gospodarczą w zakresie tworzenia systemów informatycznych, badania Internetu, biura podróży, podmioty zajmujące się produkcją, handlem i usługami.

Analizując wyniki kontroli należy stwierdzić, że najwięcej uchybień związanych z prawidłowym wykonywaniem przez jednostki kontrolowane obowiązków wynikających z przepisów ustawy o ochronie danych osobowych, dotyczyło w szczególności naruszenia zasady adekwatności przetwarzanych danych, jak również przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Zdarzały się również przypadki 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 ww. rozporządzenia.

²⁴ Np. decyzje DIS/DEC-598/24248/09, DIS/DEC-29/1781/10 i DIS/DEC-54/1981/10.

²⁵ Np. kontrole DIS-K-421/3/09, DIS-K-421/14/09, DIS-K-421/18/09, DIS-K-421/35/09 i DIS-K-421/76/09.

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 z tym Generalny Inspektor wydał decyzje nakazujące usunięcie wszystkich stwierdzonych w toku kontroli uchybień oraz umarzające postępowanie w zakresie nieprawidłowości już usuniętych w toku postępowania.²⁶ W szczególności nakazał 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 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.

Na podstawie ustaleń z kontroli przeprowadzonych w 2009 r. można stwierdzić, że w porównaniu z latami ubiegłymi osoby odpowiedzialne za przetwarzanie danych osobowych wykazały większą świadomość zagrożeń związanych z przetwarzaniem danych osobowych, a tym samym świadomość konieczności zapewnienia odpowiednich środków organizacyjnych i technicznych zapewniających ochronę tych danych. Konsekwencją było większe wyczulenie na prawidłowe dopełnienie obowiązków wynikających z przepisów o ochronie danych osobowych. 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.

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

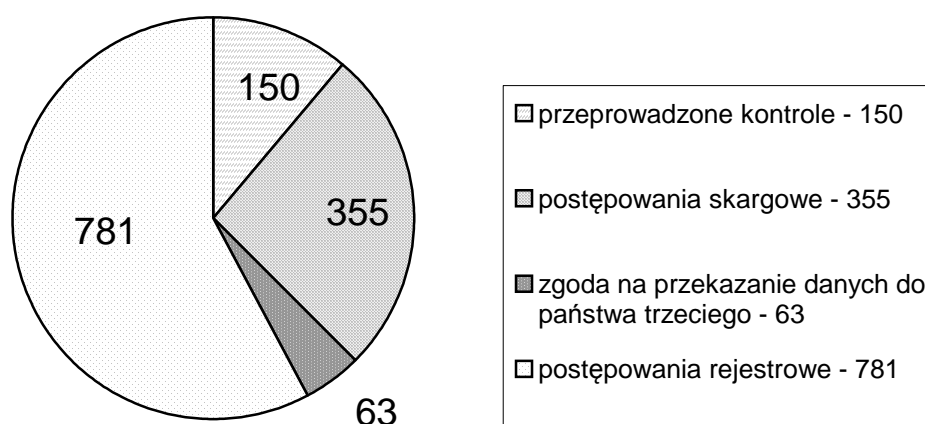
3.1. Wydawanie decyzji

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

²⁶ Np. decyzje DIS/DEC-973/35153/09, DIS/DEC/390/17359/09, DIS/DEC/286/130006/09, DIS/DEC/1109/40731/09 i DIS/DEC-366/16756/09.

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 2009 r. Generalny Inspektor wydał **1349 decyzji administracyjnych**, w tym 781 dotyczyło postępowań rejestrowych, 150 zostało wydanych w związku z przeprowadzonymi kontrolami, 355 wydano na skutek postępowania zainicjowanego skargą, zaś 63 dotyczyły zgody na przekazanie danych do państwa trzeciego.



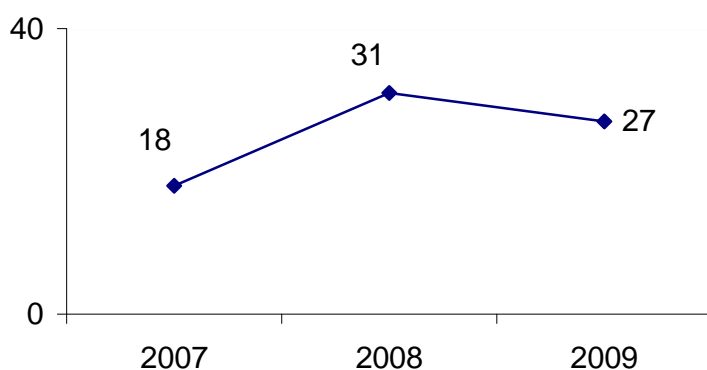
Wykres 1: Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2009 r.

W analizowanym roku sprawozdawczym 2009 Generalny Inspektor Ochrony Danych Osobowych skierował do organu powołanego do ścigania przestępstw **27 zawiadomień o popełnieniu przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych**. Jak co roku, najwięcej zawiadomień o popełnieniu przestępstwa złożonych zostało w związku z postępowaniami prowadzonymi na skutek skarg wniesionych do Generalnego Inspektora (**20 zawiadomień**). Spośród nich najwięcej dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego z przeanalizowanego w art. 49 ust. 1 ustawy o ochronie danych osobowych, przetwarzania danych przez podmioty nieuprawnione, art. 51 ust. 1 ustawy - udostępnienia danych osobowych podmiotom nieuprawnionym oraz art. 52 – naruszenia obowiązku zabezpieczenia danych przed zabraniami przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Przeważająca część zawiadomień dotyczyła spraw o naruszenie ochrony danych osobowych na stronach internetowych oraz – podobnie jak w latach ubiegłych – w związku z prowadzoną przez dane podmioty działalnością marketingową.

Natomiast **7 zawiadomień** miało związek z **przeprowadzonymi kontrolami**. W czterech przypadkach zawiadomienia dotyczyły przestępstwa wskazanego w art. 49 ustawy o ochronie danych osobowych, w jednym - przestępstwa wymienionego w art. 51 ustawy o ochronie danych osobowych, w jednym - przestępstw określonych w art. 51 i 52 ustawy o ochronie danych osobowych, a w jednym przestępstw wskazanych w art. 52, 53 i 54 ustawy o ochronie danych osobowych. Na skutek złożonych zawiadomień w trzech przypadkach prowadzone dochodzenie zostało umorzone, a w jednym przypadku prokuratura odmówiła wszczęcia dochodzenia. Natomiast w pozostałych trzech przypadkach prokuratura po wszczęciu dochodzenia nie przekazała żadnych informacji o sposobie zakończenia postępowania. W tych przypadkach, w których prokuratura umorzyła dochodzenie, Generalny Inspektor Ochrony Danych Osobowych skierował do Prokuratora Generalnego wystąpienia z prośbą o podjęcie na nowo umorzonych postępowań. Wskazywał przy tym, że decyzja o ich umorzeniu podjęta została wyłącznie na podstawie zeznań złożonych przez przedstawiciela jednostki kontrolowanej. Natomiast pominięte zostały zeznania pracownika Biura Generalnego Inspektora Ochrony Danych Osobowych i materiał dowodowy wynikający z zawiadomienia o popełnieniu przestępstwa wraz z załączonymi do niego dokumentami, przez co nieuwzględnione zostały istotne ustalenia dokonane w toku przeprowadzonej kontroli. W jednym przypadku skutkiem skierowanego wystąpienia do Prokuratora Generalnego było podjęcie na nowo umorzonego postępowania. Pozostałych **20 zawiadomień** miało związek z napływającymi do Generalnego Inspektora skargami.

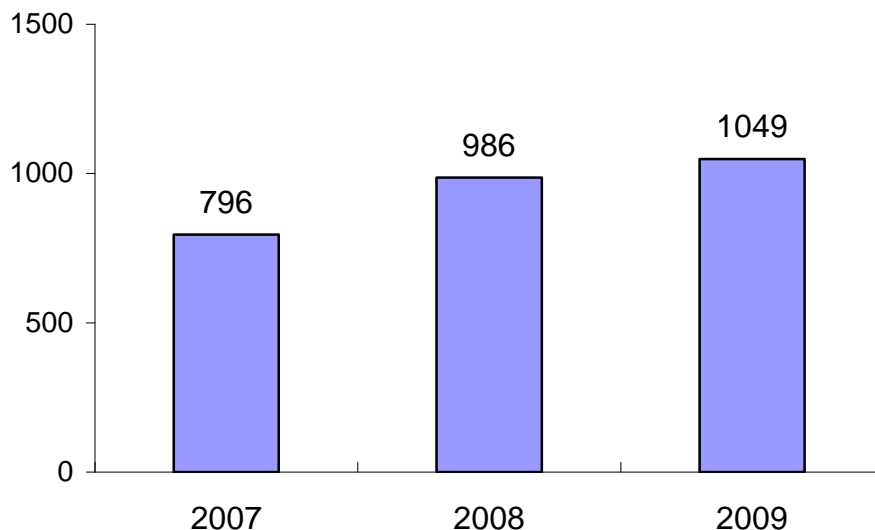
W podsumowaniu należy stwierdzić, że w porównaniu do poprzedniego okresu sprawozdawczego zmalała liczba spraw, w których organ skierował zawiadomienia o podejrzeniu popełnienia przestępstwa. Wynika to niewątpliwie z podjętych przez Generalnego Inspektora intensywnych działań w zakresie propagowania idei ochrony danych osobowych oraz bardziej stanowcze egzekwowanie od różnych podmiotów przestrzegania przepisów ustawy.

Liczbę **zawiadomień o popełnieniu przestępstwa** składanych przez Generalnego Inspektora w latach 2007–2009 przedstawia Wykres 2.



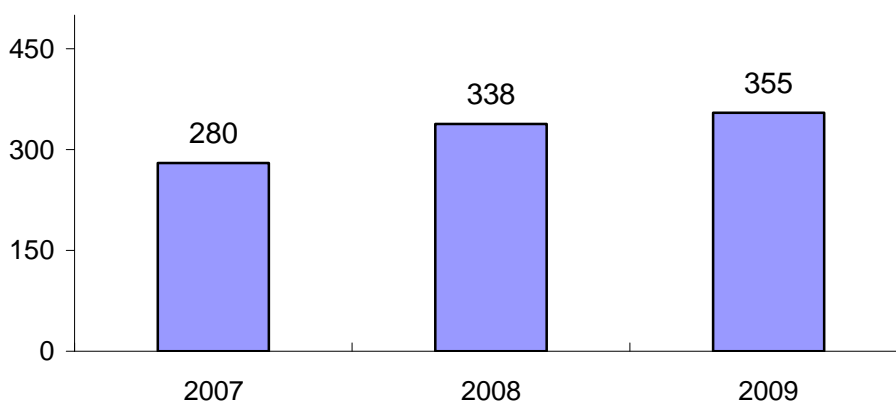
Wykres 2: Porównanie liczby zawiadomień o popełnieniu przestępstwa kierowanych przez GIODO w latach 2007–2009.

W 2009 r. do Departamentu Orzecznictwa, Legislacji i Skarg wpłynęło **1049 skarg** dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2008 liczba ta uległa zwiększeniu, co przedstawia Wykres 3.



Wykres 3: Liczbowe zestawienie skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007–2009.

W postępowaniach zainicjowanych tymi skargami wydanych zostało **355 decyzji administracyjnych**, z których **45** zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie [WSA] lub Naczelnego Sądu Administracyjnego (zał. 4). W porównaniu z rokiem 2008, w którym zaskarżonych zostało 69 decyzji, oznacza to spadek o 35 %.



Wykres 4: Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007–2009 w związku z rozpatrywanymi skargami.

Najważniejsze orzeczenia dotyczyły rozumienia pojęcia dane osobowe,²⁷ udostępnienia danych osobowych dziennikarzy na wniosek skarżącego²⁸ i udostępnienia danych osobowych osób objętych ochroną związku zawodowego.²⁹

Każda ze skarg wpływających do Biura Generalnego Inspektora Ochrony Danych Osobowych 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 2009 roku obejmował następujące obszary: 1) administracja publiczna, 2) sądy, prokuratura, komornicy, 3) banki i inne instytucje finansowe, 4) Internet, 5) marketing, 6) sektor mieszkalnictwa, 7) System Informacyjny Schengen (SIS), 8) telekomunikacja 9) zatrudnienie, 10) ubezpieczenia społeczne, majątkowe i osobowe, 11) zdrowie, 12) inne.

3.2. Decyzje w wybranych obszarach

3.2.1 Administracja publiczna

Najwięcej skarg wpływających w 2009 r. do Generalnego Inspektora Ochrony Danych Osobowych dotyczyło sektora administracji publicznej (**143 skargi**). Podobnie jak w latach ubiegłych, skarżący najczęściej wskazywali przypadki udostępnienia ich danych osobowych na stronach internetowych. W jednej z takich spraw GODO wydał decyzję³⁰ nakazującą marszałkowi województwa przywrócenie stanu zgodnego z prawem poprzez usunięcie ze strony internetowej Biuletynu Informacji Publicznej urzędu marszałkowskiego, danych osobowych skarżącego zawartych w jego oświadczeniach

²⁷ Numer IP jako dana osobowa – wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 3 lutego 2010 r. sygn. akt. II SA/Wa 1598/09, numer lokalu jako dana osobowa – wyrok Naczelnego Sądu Administracyjnego z 19 stycznia 2010 r., sygn. akt I OSK 491/09, wizerunek jako dana osobowa – wyrok Naczelnego Sądu Administracyjnego z 18 listopada 2009 r., sygn. akt I OSK 667/09.

²⁸ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 13 lutego 2009 r., sygn. akt 1570/08, wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 12 sierpnia 2009 r. sygn. akt II SA/Wa 754/09, wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 6 stycznia 2010 r. sygn. akt II SA/Wa 940/09,

²⁹ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 28 października 2009 r. sygn. akt II SA/Wa 16/09. Należy zaznaczyć, iż sprawa, w której zapadło ww. orzeczenie była opisywana w „Sprawozdaniu z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2008” s. 41-42.

³⁰ Decyzja GODO z 3 sierpnia 2009 r. DOLiS/DEC-752/09/28096,28098.

majątkowych za lata 2005 i 2006, w związku z zaprzestaniem pełnienia przez niego funkcji publicznej. W uzasadnieniu tego rozstrzygnięcia GODO wskazał, iż publikowanie oświadczeń majątkowych osoby, która zaprzestała pełnienia funkcji, w związku z którą oświadczenia te złożyła, narusza art. 23 ust. 1 ustawy o ochronie danych osobowych i oznacza poddanie danych osobowych skarżącego przetwarzaniu niezgodnemu z celami, dla których zostały one zebrane, a także oznacza ich przechowywanie w opisanej formie przez okres dłuższy, niż niezbędny dla osiągnięcia celu przetwarzania.

W omawianym okresie 2009 r. GODO wydał dwie decyzje nakazujące organom samorządu terytorialnego usunięcie danych osobowych ze strony internetowej Biuletynu Informacji Publicznej.³¹ W obu sprawach dane osobowe były zawarte w dokumentach stanowiących informację publiczną – decyzja administracyjna starosty oraz uchwała rady powiatu. W opinii GODO w sprawach tych realizacja uprawnienia w postaci ogłoszenia na stronie internetowej BIP informacji publicznej nie uwzględniała prawa skarżących do prywatności. Zgodnie z art. 5 ust. 2 ustawy o dostępie do informacji publicznej prawo do informacji publicznej, podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. W niniejszych sprawach skarżący nie pełnili funkcji publicznych, jak również nie zrezygnowali z przysługującego im prawa do prywatności. W tej sytuacji prywatność skarżących, jako dobro chronione prawem, powinno mieć pierwszeństwo przed innym dobrem prawem chronionym – dostępnością do informacji publicznej. Podkreślenia wymaga, że Trybunał Konstytucyjny wielokrotnie w wydanych orzeczeniach wyrażał pogląd, iż prawo dostępu do informacji nie ma charakteru bezwzględnego, a jego granice wyznaczone są m.in. przez konieczność respektowania praw i wolności innych podmiotów, w tym przez konstytucyjnie gwarantowane prawo do ochrony życia prywatnego.³² Trybunał Konstytucyjny stwierdził również, że w ramach zderzenia się dwu wartości – z jednej strony konstytucyjnego prawa do informacji, z drugiej prawa do prywatności – nie można bezwzględnie przyznać priorytetu temu pierwszemu. Nie istnieje formuła „zagwarantowania obywatelom dostępu do informacji za wszelką cenę.”³³ Trzeba zaznaczyć, iż ograniczenie udostępnienia danych osobowych skarżących nie oznacza, że nie stanowią one informacji publicznej, ale że zostały wyłączone z kategorii informacji podlegających ujawnieniu. Zdaniem GODO, przy upublicznieniu jedynie w celach informacyjnych decyzji administracyjnej starosty czy też uchwały rady powiatu zbędne było (nieadekwatne do celu) ujawnienie danych

³¹ Decyzja GODO z dnia 26 maja 2009 r. DOLiS/DEC-437/09, decyzja GODO z dnia 27 maja 2009 r. DOLiS/DEC-445/09.

³² Por. wyrok Trybunału Konstytucyjnego z 20 marca 2006 r. sygn. K. 17/2005.

osobowych skarżących. Usunięcie personaliów skarżących czy też ich zanonimizowanie w ogłoszonych w Biuletynie Informacji Publicznej dokumentach nie wpływa bowiem na czytelność dokonanego w ten sposób przekazu. W tych przypadkach treść decyzji administracyjnej starosty lub uchwały rady powiatu nie traci waloru informacyjnego, albowiem wynika z niej kto, kiedy i w jakiej sprawie publicznej zajął określone stanowisko.³⁴

W 2009 r. GODO wydał decyzję nakazującą straży miejskiej wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych poprzez usunięcie ze zbioru danych osobowych informacji o stanie zdrowia skarżącej³⁵ Organ wskazał, iż z treści art. 10a ustawy o strażach gminnych wynikało, że straż w celu realizacji ustawowych zadań mogła przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane: 1) w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia, 2) z rejestrów, ewidencji i zbiorów, do których straż posiada dostęp na podstawie odrębnych przepisów. Generalny Inspektor wskazał, iż brak było przepisów prawa, które wprost wskazywałyby, że to oskarżyciel publiczny – straż miejska (gminna) – miał obowiązek ustalać okoliczności dotyczące stanu zdrowia danej osoby w toku podejmowanych czynności, przed skierowaniem wniosku o ukaranie do sądu. Tego rodzaju okoliczności, jako mające znaczenie w szczególności dla obligatoryjnego udziału obrońcy w postępowaniu sądowym, mogły być ustalane już na etapie postępowania przed właściwym sądem. Świadczyć mógł o tym w szczególności fakt, iż art. 57 § 2 i 3 Kodeksu postępowania w sprawach o wykroczenia, określający warunki formalne, jakim musi odpowiadać wniosek o ukaranie, nie przewidywał, aby we wniosku zamieszczane były informacje o stanie zdrowia obwinionego. W art. 57 § 3 pkt 2 tejże ustawy wskazuje się bowiem wyłącznie, iż we wniosku powinny się znaleźć informacje dotyczące miejsca zatrudnienia obwinionego oraz, w miarę możliwości, dane o jego warunkach materialnych, rodzinnych i osobistych. Brak było więc wymogu umieszczania danych o stanie zdrowia.

W innej sprawie GODO zwrócił się do Ministra Zdrowia o podjęcie odpowiednich działań mających na celu zagwarantowanie zgodności przetwarzania danych osobowych świadczeniobiorców z przepisami ustawy o ochronie danych osobowych przekazywanych przez świadczeniodawców Narodowemu Funduszowi Zdrowia na podstawie art. 188 ust. 5 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.³⁶ Jak wynika z ustaleń dokonanych w niniejszej sprawie, związek lekarzy rodzinnych - pracodawców na podstawie pełnomocnictw (udzielonych mu

³³ Por. wyrok Trybunału Konstytucyjnego z 19 czerwca 2002 r. sygn. K. 11/2002.

³⁴ Por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 18 listopada 2008 r. sygn. II SA/Wa 1177/08.

³⁵ Decyzja GODO z dnia 12 października 2009 r. DOLiS/DEC-998/09/36971,36980,36983.

przez członków związku) pozyskiwał od członków związku dane pacjentów w celu przekazania ich Narodowemu Funduszowi Zdrowia, na podstawie z art. 188 ust. 5 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. W ocenie Generalnego Inspektora Ochrony Danych Osobowych, przepis ten nie przewidywał możliwości scedowania przez świadczeniodawcę określonego w tym przepisie obowiązku w drodze upoważnienia na rzecz innego podmiotu, np. związku. Zatem jeżeli wolą ww. świadczeniodawców było przekazywanie ww. danych do NFZ za pośrednictwem związku, jedyną konstrukcją, na podstawie której związek mógł pozyskiwać dane ww. osób w celu ich przekazania na rzecz NFZ, mogłaby być konstrukcja umowy powierzenia przewidziana w art. 31 ust. 1 ustawy o ochronie danych osobowych. Tak więc konieczne było zawarcie odpowiednich umów powierzenia przez ww. świadczeniodawców ze związkiem, określających cel i zakres przetwarzanych danych, co jednak nie miało miejsca.

W kolejnej sprawie GODO zwrócił się do Prezydenta Miasta o podjęcie stosownych działań celem wyeliminowania przypadków udostępnienia danych osobowych członków założycieli stowarzyszeń zwykłych, wobec których Prezydent pełni funkcję nadzorczą, w sytuacji braku ku temu podstaw prawnych. Impulsem do powyższego wystąpienia była skarga na udostępnienie przez ww. podmiot danych osobowych członków założycieli Komitetu Obrony Policjantów Stowarzyszenia Zwykłego na rzecz Komendanta Stołecznego Policji. Uznając powyższe działanie za pozbawione podstaw prawnych, organ ochrony danych osobowych wskazał, iż przepisy ustawy Prawo o stowarzyszeniach, które wyznaczają kompetencje Prezydenta w zakresie sprawowania nadzoru nad stowarzyszeniami, upoważniają go do podejmowania jedynie ściśle określonych działań nadzorczych, a kwestionowane udostępnienie danych osobowych stanowiło wykroczenie poza te uregulowania.³⁷

W trzech innych skargach na podmioty z sektora administracji publicznej najczęściej podnoszony był zarzut bezprawnego przetwarzania danych osobowych na stronach internetowych jednostek samorządu terytorialnego. Przetwarzanie to było wynikiem publikacji protokołu z sesji rady miejskiej, jak również zarządzenia organu samorządu terytorialnego zawierającego dane osobowe skarżących. W kolejnych sprawach skarżący kwestionowali pozyskiwanie danych osobowych przez organy samorządu terytorialnego w związku z przeprowadzeniem ankiety, ubieganiem się o pomoc zdrowotną czy też żądaniem udostępnienia informacji publicznej. Jedna ze skarg zawierała zarzut nieprawidłowego przetwarzania danych osobowych w toku prowadzonego przez organ samorządu terytorialnego postępowania administracyjnego. Polegało ono na włączeniu do akt postępowania dokumentów zawierających dane tzw. szczególnie chronione. Ponadto pojawiła się sprawa udostępnienia przez przewodniczącego rady powiatu podmiotom nieuprawnionym danych osobowych

³⁶ Pismo GODO z dnia 15 października 2009 r. DOLiS-440-374/09/37706,37818.

³⁷ Pismo z 26 marca 2009 r. DOLiS-440-516/08/10812/09.

zwartych w uchwale rady powiatu i protokole pokontrolnym sporządzonym przez członków komisji rewizyjnej tej rady.

W omawianym roku GODO zwrócił się do burmistrza o podjęcie odpowiednich działań w celu dostosowania procesu przetwarzania danych osobowych zebranych za pomocą ankiety w zbiorze danych osób niepełnosprawnych mieszkających na terenie gminy miejskiej do wymogów określonych przepisami ustawy o ochronie danych.³⁸ GODO wskazał, że chcąc uniknąć zarzutu naruszenia art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych, administrator danych osobowych osób niepełnosprawnych zawartych w opisanych ankietach (w niniejszej sprawie burmistrz), powinien był oprzeć proces przetwarzania ww. danych na którejś z przesłanek wymienionych w art. 27 ust. 2 pkt 1-10 ustawy o ochronie danych osobowych (np. pozyskać od osób, których ww. dane dotyczą, pisemną zgodę na ich przetwarzanie), jak również udzielić osobom, których dane dotyczą, informacji określonych w art. 24 ustawy o ochronie danych osobowych. Zdaniem GODO, należyte wywiązanie się z obowiązku zapewnienia adekwatności (relevantności) danych (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych) wymagało z kolei, aby administrator przetwarzał wyłącznie takie dane (takiego rodzaju i takiej treści), które były mu niezbędne dla realizacji celów, dla których były zebrane. Jednocześnie Generalny Inspektor Ochrony Danych Osobowych zaznaczył, iż konieczne było jednoznaczne i precyzyjne zdefiniowanie ww. celów realizowanych przez burmistrza, dla których zbierał on omawiane dane (i poinformowanie o tych celach osób, których dotyczą przetwarzane dane – art. 24 ust. 1 pkt 2 ustawy o ochronie danych osobowych). W kolejnej sprawie GODO zwrócił się do burmistrza o podjęcie działań mających na celu zapewnienie zgodności przetwarzanych danych osobowych dotyczących wysokości osiąganych dochodów rodziców dziecka z przepisami ustawy o ochronie danych osobowych, pozyskiwanych w trakcie rekrutacji do przedszkoli prowadzonych przez miasto.³⁹ Organ w wystąpieniu tym zalecił, by pozyskiwana była zgoda osoby zainteresowanej na przetwarzanie danych dotyczących osiąganych dochodów na potrzeby tejże rekrutacji. Pozwoli to bowiem na uniknięcie wątpliwości, co do legalności pozyskiwania i dalszego przetwarzania przedmiotowych danych, a zarazem świadczyć będzie o kierowaniu się przez burmistrza zasadą szczególnej staranności w procesie przetwarzania danych osobowych.

Analiza dotycząca działalności organu ochrony danych osobowych w sektorze „administracja publiczna” wykazuje, że wciąż 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

³⁸ Pismo GODO z 19 listopada 2009 r. DOLiS-440-701/09/42787.

³⁹ Pismo GODO z 18 grudnia 2009 r. DOLiS-440-236/09/47521.

o sprawach publicznych, administratorzy danych pomijają fakt istnienia prawa wynikającego z ustawy o ochronie danych osobowych.

3.2.2 Sądy, prokuratura, komornicy

W 2009 r. wpłynęły **43 skargi** dotyczące tego sektora. W jednej z nich GODO zwrócił Prezesowi Sądu Okręgowego w Warszawie uwagę na stosowaną przez sędziów praktykę załączania do akt postępowania dokumentów zawierających dane osobowe osób trzecich niebędących stroną w sprawie. Impulsem do tego wystąpienia stała się skarga na udostępnienie przez adwokata danych osobowych skarżącego, poprzez załączenie kopii postanowienia z jednej sprawy do akt innej sprawy.⁴⁰ W kolejnej sprawie GODO zwrócił się do Ministra Sprawiedliwości z prośbą o podjęcie działań mających na celu wyeliminowanie stosowanej przez prokuraturę praktyki polegającej na wpisywaniu na zwrotnym potwierdzeniu odbioru pism informacji wskazujących na charakter, w jakim ich adresat uczestniczy w prowadzonym postępowaniu. W opinii GODO, takie działanie było niezgodne nie tylko z przepisami ustawy o ochronie danych osobowych, ale również z przepisami Kodeksu postępowania karnego.⁴¹ Organ wskazał, że praktyka wpisywania na zwrotnym potwierdzeniu odbioru ww. informacji, była stosowana bez podstawy prawnej.

W związku z udostępnieniem przez komornika sądowego, pozyskanych w toku innego postępowania egzekucyjnego danych osobowych dłużnika jego wierzycielowi, mimo braku żądania, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Prezesa jednego z sądów rodzinnych o zobowiązanie komornika do zaniechania tego rodzaju praktyki w przyszłości, albowiem prowadzi ona do naruszenia przepisów ustawy o ochronie danych osobowych.⁴²

3.2.3 Banki i inne instytucje finansowe

W 2009 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **139** spraw dotyczących tego sektora. Wśród nich najczęściej pojawiały się te związane z przekazywaniem danych osobowych przez banki firmom windykacyjnym w związku z nieuregulowaniem przez osobę, której dane dotyczyły zobowiązań wobec banku, a także naruszeniem ustawy o ochronie danych osobowych przez bank w związku z przesyłaniem przez ten podmiot korespondencji adresowanej do osoby skarżącej na jej stary adres pomimo zgłoszenia informacji o nowym adresie do korespondencji. W jednej sprawie bank przetwarzał dane osobowe osoby skarżącej w celach marketingowych, mimo rozwiązania umowy kredytowej z klientem (adresatem korespondencji) oraz mimo złożenia pisemnego sprzeciwu wobec wykorzystywania w tym celu danych osobowych. Po interwencji GODO w tej sprawie bank wskazał, że do wykorzystywania danych w kwestionowany sposób doszło w wyniku

⁴⁰ Pismo z 28 kwietnia 2009 r. DOLiS-440-332/08/15130/09.

⁴¹ Pismo GODO z 26 listopada 2009 r. DOLiS-440-184/08/43888/09.

błądu pracownika banku, który nie wprowadził do systemu komputerowego odpowiedniej informacji o zakazie przetwarzania danych w celach marketingowych. Pracownik został przez bank pouczony o konieczności przestrzegania procedur, a sprzeciw osoby skarżącej został odnotowany w systemie banku.

Wiele spośród skarg na przetwarzanie danych osobowych przez banki dotyczyło przetwarzania danych skarżących w celach marketingowych, pomimo złożonego przez nich sprzeciwu. Skarżący wskazywali, iż ich dane były nadal przetwarzane w ww. celu, czego dowodem było otrzymywanie wraz z wyciągiem bankowym życzeń świątecznych⁴³ lub korespondencji reklamowej, mimo rezygnacji z usług banku i złożenia prośby o usunięcie danych z jego zasobów.⁴⁴ W jednej ze skarg skarżąca zakwestionowała sposób, w jaki posłużono się jej danymi w celu marketingu usług banku, wskazując, iż wraz z materiałami reklamowymi przesłano jej gotowy formularz umowy o korzystanie z reklamowanego produktu wraz z wpisanymi jej danymi osobowymi.⁴⁵ W kolejnej ze skarg dotyczących podnoszonej kwestii zarzucono bankowi, że przetwarza w celu marketingowym dane skarżącego, mimo że ten nigdy nie był klientem banku. Jak wskazano w treści skargi, bank wszedł w posiadanie jego danych wskutek złożenia przez niego wniosku o przeprowadzenie analizy zdolności kredytowej.⁴⁶

W omawianym okresie pojawiła się także skarga na bezprawne przetwarzanie danych osobowych przez pracownicę banku, która załączyła do akt postępowania rozwodowego wniosek kredytowy złożony wcześniej do tego banku przez jej męża (który jest stroną ww. postępowania).

Do GIODO wpłynęła także skarga na niewypełnienie przez bank wobec skarżącego obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych, tj. nieudzielenie odpowiedzi na wniosek skarżącego dotyczący żądania informacji o przetwarzaniu jego danych osobowych.⁴⁷ Przedmiotem wielu innych skarg na banki było także nielegalne, zdaniem skarżących, przekazywanie ich danych osobowych do Biura Informacji Kredytowej [BIK] oraz rejestrów dłużników.

W 2009 r. GIODO zwrócił się do Prezesa banku o uwzględnienie w działalności tego podmiotu zasad wynikających z ustawy o ochronie danych osobowych, zwłaszcza jej art. 26 ust. 1, stanowiącego o obowiązku administratora danych dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą⁴⁸. Jak wynika z analizy stanu faktycznego, bank 7 marca 2000 r. zawarł ze skarżącym umowę kredytu odnawialnego z możliwością jej przedłużenia, jeżeli

⁴² Pismo z 24 kwietnia 2009 r. DOLiS-440-873/08/14723/09.

⁴³ DOLiS-440-191/09.

⁴⁴ DOLiS-440-252/09.

⁴⁵ DOLiS-440-246/09.

⁴⁶ DOLiS-440-211/09.

⁴⁷ DOLiS-440-153/09.

⁴⁸ Pismo GIODO z dnia 23 lipca 2009 r. DOLiS-440-782/08/26750/09.

kredytobiorca spełni warunki wynikające z umowy. Jako że skarżący nie zapewnił na rachunku środków na spłatę kredytu, bank dokonał przeksięgowania zobowiązania do windykacji. Zamknięcie umowy kredytu odnawialnego nastąpiło 30 marca 2001 r., natomiast wierzytelność banku z tytułu kredytu odnawialnego została spłacona 19 czerwca 2001 r. Przekazanie danych osobowych skarżącego do BIK S.A. nastąpiło na podstawie umowy zawartej 22 czerwca 2001 r. pomiędzy BIK S.A. a bankiem, określającej zasady współpracy w zakresie zbierania i udostępniania informacji na podstawie art. 105 ust. 4 ustawy Prawo bankowe. Bank 19 sierpnia 2008 r. wystosował do BIK S.A. wniosek o usunięcie danych dotyczących zobowiązania z bazy BIK S.A. Dane zostały usunięte 28 sierpnia 2008 r. Jako prawdopodobną przyczynę niezaktualizowania informacji w kartotekach bankowych o spłacie kredytu przez skarżącego, a tym samym w bazie BIK S.A., bank wskazał błąd systemowy transferu danych lub nieprawidłowe wykonanie czynności przez osobę obsługującą system. GIOGO zasygnalizował, iż poprzez opisane działanie banku informacje zawarte w bazie BIK S.A. nie odzwierciedlały faktycznej sytuacji prawnej skarżącego, a tym samym narażały go na powstanie negatywnych dla niego skutków. Generalny Inspektor nie kwestionował udostępnienia danych osobowych przez bank innemu podmiotowi (w tej sytuacji BIK S.A.), gdyż w przedstawionym stanie faktycznym było to uzasadnione na podstawie obowiązujących przepisów prawa. Jednakże bank – jako administrator danych osobowych skarżącego – zobowiązany jest, zgodnie z art. 26 ust. 1 ustawy, dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: 1) przetwarzane zgodnie z prawem, 2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2, 3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. W sytuacji, gdy administrator nie wywiązuje się z powyższego obowiązku, osoba, której dane są przetwarzane, ma prawo domagać się sprostowania (także usunięcia) danych nieprawdziwych. W szczególności bank, jako instytucja zaufania publicznego, powinien zapewnić przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa.

W analizowanym roku sprawozdawczym GIODO zwrócił się od Przewodniczącego Komisji Nadzoru Finansowego z prośbą o zwrócenie instytucjom, nad którymi Przewodniczący sprawuje nadzór, w tym w szczególności bankom, uwagi na konieczność respektowania przepisów ustawy Prawo bankowe w odniesieniu do tajemnicy bankowej, w sytuacji, gdy podmioty te ulegają łączeniu, podziałowi lub przekształcaniu w rozumieniu przepisów ustawy Kodeks spółek handlowych, i jednocześnie przestrzegania zasad określonych w ustawie o ochronie danych osobowych.⁴⁹

⁴⁹ Pismo z dnia 30 lipca 2009 r. DOLiS-440-868/08/27821/09.

Przetwarzania danych osobowych przez instytucje finansowe dotyczyły także inne decyzje GODO. W jednej z nich organ nakazał bankowi zaprzestanie przetwarzania danych osobowych osoby skarżącej w celach marketingowych, wobec wyrażenia przez nią sprzeciwu. Organ, wbrew stanowisku banku uznał, iż przysyłanie wiadomości tekstowej SMS z informacją o zmianie oprocentowania produktów bankowych ma charakter reklamowy.⁵⁰

W omawianym okresie GODO zwrócił się do Prezesa Naczelnego Sądu Administracyjnego z wystąpieniem mającym na celu zwrócenie uwagi na dokonaną w jednym z wyroków wydanych przez NSA, interpretację przesłanki dopuszczalności przetwarzania danych osobowych określonej w art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych. Impulsem do wystosowania niniejszego pisma było uznanie przez sąd, iż wątpliwa jest prawna skuteczność zgody na przetwarzanie danych wyrażonej przez skarżącego poprzez wybór opcji „TAK” na formularzu internetowym, stanowiącym wniosek o korzystanie z usług banku. Mając na uwadze fakt, iż taka interpretacja może rodzić doniosłe skutki społeczno-prawne (i to dotyczące nie tylko przedmiotowej sprawy), GODO zwrócił uwagę na powyższą interpretację, która może pozostawać w sprzeczności z zajmowanym dotychczas przez sądy administracyjne stanowiskiem.⁵¹

W związku z uzyskaniem informacji, z której wynika, że pewien bank udostępnił osobom trzecim dane osobowe swojej klientki bez podstaw prawnej, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do tego podmiotu o podjęcie stosownych działań mających na celu wyeliminowanie powyższych nieprawidłowości w przyszłości. W przedmiotowej sprawie pracownik banku telefonicznie poinformował sąsiadów skarżącej o potrzebie jej natychmiastowego stawiennictwa w banku. Organ zwrócił uwagę bankowi, że każde przetwarzanie danych powinno mieć podstawę w przesłankach określonych w ustawie. Ponadto jednym z podstawowych obowiązków administratora danych jest zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym oraz dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.⁵²

W omawianym okresie GODO wystąpił do Prezesa Zarządu jednego z banków o uwzględnienie w działalności tego podmiotu przepisów ustawy o ochronie danych osobowych, zwłaszcza jej art. 36 ust. 1 stanowiącego o obowiązku administratora danych do zastosowania środków technicznych i organizacyjnych zapewniających odpowiednią ochronę danych osobowych przed m.in. umożliwieniem dostępu do nich osobom nieupoważnionym. Impulsem do skierowania niniejszego wystąpienia stało się rażące naruszenie przepisów ustawy o ochronie danych osobowych przez ten bank. Polegało ono na nienależytym zabezpieczeniu danych osobowych jego klientów, na skutek czego

⁵⁰ Decyzja z dnia 19 marca 2009 r. DOLiS/DEC-214/09/9765,976.

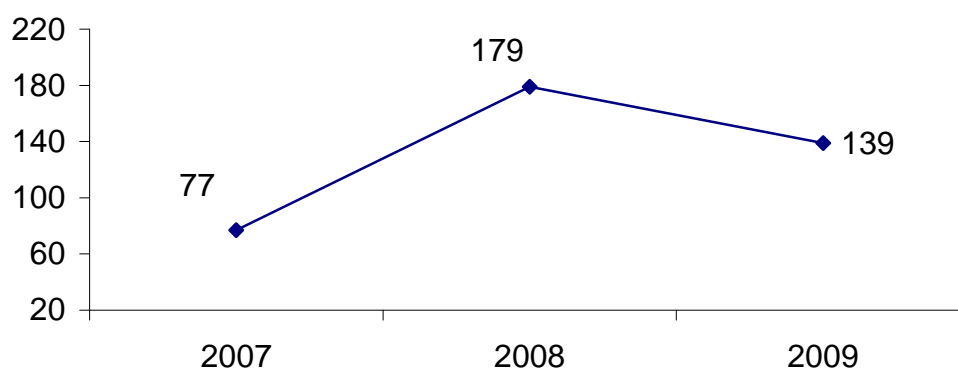
⁵¹ Pismo z 16 marca 2009 r. GI-DS-430-161/06/8944/09.

⁵² Pismo z 6 kwietnia 2009 r. DOLiS-440-939/08/12127/09.

osoby nieupoważnione miały możliwość uzyskania informacji zawartych w zestawieniach operacji dokonywanych na rachunkach bankowych tych klientów. Jak wynika ze zgromadzonego materiału dowodowego klienci Banku korzystający z usługi elektronicznego dostępu do ich rachunków bankowych, poprzez modyfikację treści adresu URL przeglądarki internetowej (polegającą na usunięciu oryginalnej części treści adresu URL i zastąpieniu jej nowym wpisem), mieli możliwość dostępu do ww. danych osobowych innych klientów banku. Podmiot ten przyznał, że sytuacja taka miała miejsce. Oświadczył następnie, iż zastosował dodatkowe środki zapewniające ochronę danych przetwarzanych w jego systemie informatycznym.⁵³ Powyżej opisane okoliczności stały się również podstawą do skierowania przez Generalnego Inspektora Ochrony Danych Osobowych wystąpienia do Prezesa Związku Banku Polskich o podjęcie działań zwracających bankom uwagę na konieczność respektowania przepisów ustawy o ochronie danych osobowych, zwłaszcza na art. 36 ust. 1.⁵⁴

W omawianym okresie GODO wydał również decyzję⁵⁵ nakazującą bankowi usunięcie danych osobowych skarżącej przetwarzanych przez ten podmiot, ponieważ pozyskane zostały z w wyroku sądowego. Jak wynika z ustaleń dokonanych przez organ, bank na potrzeby rozpatrzenia wniosku kredytowego skarżącej pozyskał jej dane z wyroku rozwodowego, a także powierzeniu skarżącej wykonywania władzy rodzicielskiej nad małoletnim synem oraz informacje dotyczące wysokości alimentów, które skarżąca otrzymywała na syna i o kosztach procesu. W ocenie Generalnego Inspektora Ochrony Danych Osobowych, pozyskanie przez bank informacji wynikających z ww. wyroku pozostawało w rażącej sprzeczności z przepisami ustawy o ochronie danych osobowych.

W podsumowaniu zauważyć należy, że w porównaniu z latami ubiegłymi znacznie zmalała liczba skarg dotyczących tego sektora. Przyczyn tego zjawiska można upatrywać we wzroście wśród pracowników banków i innych instytucji finansowych świadomości obowiązywania ustawy o ochronie danych osobowych i we właściwym jej stosowaniu.



Wykres 5: Zestawienie porównawcze liczby skarg dotyczących sektora bankowości, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

⁵³ Pismo GODO z 26 maja 2009 r. DOLiS-440-143/09/19041.

⁵⁴ Pismo GODO z 26 maja 2009 r. DOLiS-440-143/09/19043.

⁵⁵ Decyzja GODO z 24 września 2009 r. DOLiS/DEC-967/09/34781,34784.

3.2.4 Internet

W roku 2009 wpłynęło **88 spraw** dotyczących działalności podmiotów z tego sektora. Zarzuty, jakie najczęściej pojawiały się w skargach, to: bezprawne przetwarzanie danych osobowych przez właściciela portalu internetowego przy jednoczesnym braku możliwości ich usunięcia przez osobę, której dane dotyczą czy bezprawne udostępnienie danych osobowych przez administratora portalu innym jego użytkownikom. W jednej ze skarg pojawił się zarzut bezprawnego publikowania na stronach internetowych danych osobowych byłego pracownika firmy oraz bezprawne pozyskiwanie przez administratora portalu oferującego pomoc w zarządzaniu wydatkami, kopii wyciągów z rachunków bankowych i zawartych w nich danych osobowych. Ponadto GODO wszczął z urzędu postępowanie w sprawie upublicznienia przez administratora jednego z portali oferujących bilety lotnicze, danych osobowych użytkowników tego portalu, zaś w innej - zakwestionował legalność pozyskiwania przez administratora portalu danych osobowych w związku z rezerwacją biletów za pośrednictwem sieci Internet.

W jednej ze skarg GODO został poinformowany, że po zalogowaniu się przez skarżącego do swojego profilu na portalu społecznościowym pojawiają się reklamy pewnego produktu zachęcające do zakupu zalogowanego użytkownika poprzez użycie w ich treści jego imienia.⁵⁶ Natomiast w skardze na inny portal społecznościowy wskazano, iż mimo usunięcia konta z portalu i wbrew zapewnieniu otrzymanemu od jego administratora, że dane zostaną usunięte po 30 dniach, po upływie tego czasu dane osobowe osoby skarżącej były w dalszym ciągu przetwarzane.⁵⁷ GODO otrzymał również informację o umieszczeniu na jednej ze stron internetowych treści godzących w dobre imię skarżącego oraz zdjęcia z jego wizerunkiem.⁵⁸ W innej sprawie wskazano natomiast, że administrator jednego z portali internetowych, na których umieszczane są oferty osób poszukujących pracy, ujawnił CV osoby skarżącej bez jej zgody i wiedzy.⁵⁹

W analizowanym okresie do GODO wpłynęła także skarga na udostępnienie przez serwis aukcyjny danych osobowych osoby skarżącej w zakresie adresu zamieszkania w wyszukiwarce Google. Skarżąca wskazała, iż powyższe dane osobowe zostały przez pomyłkę udostępnione przez nią w zakładce „O mnie” na portalu aukcyjnym, a po ich usunięciu nadal „są pozycjonowane” w tej wyszukiwarce.⁶⁰

Organ ochrony danych osobowych był również adresatem wniosku o wszczęcie postępowania administracyjnego w sprawie nielegalnego pozyskania przez właściciela jednej z domen internetowych

⁵⁶ DOLiS-440-169/09, DOLiS-440-210/09.

⁵⁷ DOLiS-440-197/09.

⁵⁸ DOLiS-440-225/09.

⁵⁹ DOLiS-440-223/09.

⁶⁰ DOLiS-440-163/09.

danych osobowych pracowników skarżącego. Ponadto dane te były wykorzystywane podczas jego rozmów telefonicznych z tymi pracownikami, podczas których składał im propozycje zatrudnienia w swojej firmie.⁶¹ Skarżący, prosząc o zbadanie sprawy, wskazał, iż źródłem powyższych danych nie mogli być jego pracownicy, gdyż informacje, w posiadaniu których znajduje się właściciel domeny, stanowią tajemnicę przedsiębiorcy. Do GODO wpłynęła także prośba o kontrolę zgodności przetwarzania danych z przepisami ustawy o ochronie danych osobowych przez sklep, który umieścił dane osoby skarżącej będącej jego klientką, na swojej stronie internetowej.⁶²

W jednej ze spraw GODO wydał decyzję⁶³ nakazującą związkowi działkowców usunięcie danych osobowych skarżącego ze strony internetowej <http://www.pzd.pl> z wyłączeniem danych osobowych znajdujących się w Biuletynie Informacyjnym Krajowej Rady PZD. Ustalono, że w wyniku konfliktu pomiędzy skarżącym a PZD jego dane osobowe zostały zamieszczone na ww. stronach internetowych, co w opinii Generalnego Inspektora nie znajdowało oparcia w żadnej z przesłanek określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych. Natomiast kwestia opublikowania danych osobowych w Biuletynie Informacyjnym Krajowej Rady PZD nie podlega przepisom ustawy o ochronie danych osobowych, ponieważ biuletyn ten stanowi prasę w rozumieniu art. 7 ust. 2 Prawa prasowego.

W omawianym okresie sprawozdawczym GODO wydał decyzję⁶⁴ nakazującą spółce udostępnienie na rzecz skarżącego informacji o osobach, które dokonały wpisów na forum portalu internetowego spółki, posługując się wskazanymi przez skarżącego pseudonimami – w zakresie obejmującym informacje o numerach IP komputerów, z których dokonano ww. wpisów. W niniejszej sprawie organ uznał, iż udostępnienie skarżącemu żądanych informacji znajduje uzasadnienie w przepisie art. 29 ust. 2 ustawy o ochronie danych osobowych. Skarżący wyjaśnił bowiem, że zamierza wykorzystać ww. informacje dla ustalenia dalszych danych osób, które – w jego ocenie – dopuściły się bezprawnej ingerencji w sferę jego dóbr osobistych, tak aby możliwe było skierowanie przeciwko nim do sądu powództwa z tytułu naruszenia ww. dóbr prawnie chronionych. W sytuacji, gdy skarżący nie dysponował zasadniczo żadnymi informacjami o osobach, które dokonały przedmiotowych wpisów, nie można zasadnie przyjąć, że podjęte przez niego działania służące ustaleniu tożsamości tych osób, w celu pociągnięcia ich do odpowiedzialności cywilnej w związku z treścią wpisów, nie mieściły się w pojęciu jego wiarygodnie uzasadnionych potrzeb. Oczywiście jest, że pozyskanie (przetwarzanie) danych osobowych w ww. celu w każdym przypadku zostanie uznane przez osoby, których dane te dotyczą, za sprzeczne z ich interesem. Okoliczność ta – zwłaszcza mając na uwadze prawne gwarancje obrony przed roszczeniami strony przeciwnej – nie świadczy jednak

⁶¹ DOLiS-440-215/09.

⁶² DOLiS-440-233/09.

⁶³ Decyzja GODO z 4 maja 2009 r. DOLiS/DEC-358/09.

o naruszeniu ich praw i wolności. Przyjęcie przeciwnego stanowiska skutkowałoby bezzasadną ochroną tego, kto mógł dopuścić się bezprawnej ingerencji w sferę prawnie chronionych interesów innej osoby (zwłaszcza przekonany o anonimowości, jaką gwarantuje mu sieć Internet) przed ewentualną odpowiedzialnością za jego działania. Ocena natomiast zasadności zarzutów stawianych wobec autorów wpisów pozostaje w kompetencjach właściwego miejscowo i rzeczowo sądu powszechnego.

3.2.5 Marketing

W roku 2009 organ ds. ochrony danych osobowych był adresatem **57 skarg** kwalifikujących się do tego sektora. Najczęściej pojawiającymi się zarzutami były: przetwarzanie danych osobowych w celach marketingowych własnych produktów i usług bez zgody osoby, której dane te dotyczyły, brak opcjonalności wyrażenia zgody na przetwarzanie danych w celach marketingowych przy składaniu zamówienia drogą internetową, nierespektowanie prośby o usunięcie danych osób skarżących z bazy firmy⁶⁵ oraz niewypełnienie obowiązku informacyjnego z art. 25 ustawy o ochronie danych osobowych. W uzasadnionych przypadkach Generalny Inspektor najczęściej występował do administratorów danych z tego sektora z sygnalizacjami wskazującymi uchybienia związane z przetwarzaniem danych osobowych.

Nierespektowanie sprzeciwu osoby, której dane dotyczą, na przetwarzanie jej danych osobowych stało się dla GODO impulsem do wystąpienia do Prezesa Zarządu Stowarzyszenia Marketingu Bezpośredniego [SMB] o podjęcie działań uczulających spółkę trudniącą się wysyłaniem ofert marketingowych do respektowania przepisów o ochronie danych osobowych poprzez niezwłoczne odnotowywanie w swoich systemach sprzeciwów wobec przetwarzania danych osobowych w celach marketingowych, zaprzestanie przysyłania ofert reklamowych osobom, które je złożyły oraz wypełnianie wobec klientów obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych.⁶⁶

Na uwagę zasługuje zwłaszcza sprawa,⁶⁷ w której skarżący, pomimo złożenia sprzeciwu na przetwarzanie przez bank dotyczących go danych osobowych w celach marketingowych - czemu bank nie zaprzeczył i co odnotował w swoich systemach informatycznych – nadal przysyłał skarżącemu informacje, tyle że za pośrednictwem serwisu transakcyjnego banku. W ocenie banku przesłanie skarżącemu materiału reklamowego tą drogą nie stanowiło przetwarzania jego danych osobowych w celach marketingowych, gdyż nie musiał on zapoznawać się z treścią komunikatu (poprzez jego kliknięcie i przejście do szczegółów) oraz takie działanie wynikało z nałożonego na bank przepisami Prawa bankowego obowiązku przysyłania klientom komunikatów do rachunku. Generalny

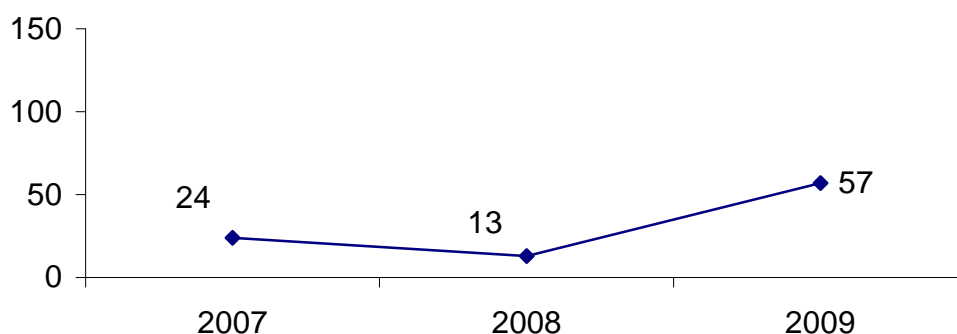
⁶⁴ Decyzja GODO z 21 września 2009 r. DOLiS/DEC-936/09/34335,34344.

⁶⁵ DOLiS-440-202/09.

⁶⁶ Pismo z 16 marca 2009 r. DOLiS-440-303/08/8960/09.

Inspektor Ochrony Danych Osobowych w treści decyzji podkreślił, iż przesłana do skarżącego przez bank wiadomość nie dotyczyła wykonywania umowy rachunku, który w banku ma skarżący, a stanowiła informację o całkiem nowym produkcie tego podmiotu. Sformułowania, którymi posłużył się bank w wiadomości przesłanej skarżącemu, należało uznać za sugestywne, zrozumiałe, zwięzłe, łatwe do zapamiętania, jak również odwołujące się do interesów ekonomicznych odbiorcy, przez co swoją charakterystyką odpowiadające tekstom reklamowym.

W podsumowaniu należy wskazać, iż utrzymujący się od dwóch lat roku systematyczny spadek liczby skarg na podmioty z tego sektora, w 2009 r. uległ gwałtownemu załamaniu i w odniesieniu do 2008 r. wzrósł ponad trzykrotnie, co obrazuje *Wykres 6*.



Wykres 6: Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych w celach marketingowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

3.2.6 Sektor mieszkalnictwa

Skargi wpływające na podmioty z tego sektora (**57**) 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 (listy dłużników spółdzielni ze wskazaniem numeru lokalu i kwoty zadłużenia, rozliczenia kosztów zużycia wody itd.), przekazanie skierowanej do spółdzielni mieszkaniowej korespondencji mieszkańcom bloku, udostępnienie przez spółdzielnię mieszkaniową aktów notarialnych dotyczących zakupu mieszkania i darowizny, którą skarżący uczynił na rzecz żony,⁶⁷ zamieszczanie przez wspólnotę mieszkaniową danych osobowych lokatorów na stronie internetowej⁶⁸ czy ogłaszanie na stronie internetowej spółdzielni mieszkaniowej informacji o nieprawomocnym wyroku, jaki zapadł w sprawie z powództwa o unieważnienie uchwały rady nadzorczej spółdzielni⁷⁰ itd. W tego typu sprawach upublicznianie danych co do zasady naruszało ustawę o ochronie danych osobowych. Ponadto

⁶⁷ Decyzja GIODO z 4 listopada 2009 r. DOLiS/DEC-1104/09/40590,40594.

⁶⁸ DOLiS-440-1039/09.

⁶⁹ DOLiS-440-997/09.

żaden z przepisów ustawy Prawo spółdzielcze nie zezwala na upublicznienie informacji o zadłużeniu czynszowym poprzez zamieszczenie ich na powszechnie dostępnych tablicach ogłoszeń, do których dostęp mogły mieć również osoby trzecie. 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 omawianym okresie Generalny Inspektor Ochrony Danych Osobowych wystąpił do Prezesa Zarządu Krajowej Rady Spółdzielczej z prośbą o wprowadzenie rozwiązań, które uniemożliwią ujawnianie w protokołach lustracji spółdzielni mieszkaniowych danych osobowych osób informujących o okolicznościach podlegających badaniu w trakcie prowadzonej lustracji. Impulsem do powyższego wystąpienia była skarga złożona przez członków jednej ze spółdzielni mieszkaniowych do Krajowej Rady Spółdzielczej i w związku z tym dane tych osób zostały umieszczone – w różnych kontekstach – w protokole lustracji. GODO, uzasadniając swoje wystąpienie, wskazał, iż tego rodzaju ujawnienie danych narusza zasady celowości i adekwatności przetwarzania danych osobowych.⁷¹

W jednej z analizowanych przez GODO spraw zarząd spółdzielni mieszkaniowej przesłał osobom zainteresowanym przeniesieniem własności lokali pisma zawierające informacje o zaskarżeniu uchwały tego podmiotu oraz dane osoby skarżącej, która ten środek odwoławczy wniosła. Działanie takie zostało uznane za niezgodne z przepisami ustawy o ochronie danych osobowych, ponieważ nie znajdowało podstawy w przesłankach określonych w ustawie, zwłaszcza że stronami postępowania, w toku którego została zaskarżona uchwała, były spółdzielnia i skarżąca, a nie osoby zainteresowane przeniesieniem własności lokali.⁷²

W omawianym okresie GODO zwrócił się do spółdzielni mieszkaniowej o dostosowanie procesu przetwarzania danych osobowych do wymogów ustawy o ochronie danych osobowych poprzez zaniechanie udostępniania dla celów sprawozdawczych danych osobowych spółdzielców w zbyt szerokim zakresie.⁷³ Organ w wystąpieniu tym wskazał, iż spółdzielnia mieszkaniowa jako administrator danych na podstawie art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych zobowiązana była do dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zobowiązana była zapewnić, aby dane te były adekwatne w stosunku do celów, w jakich są przetwarzane. Adekwatność ta powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga byłaby zachowana, jeżeli administrator przetwarzałby dane (a więc także udostępniał) tylko w takim zakresie, w jakim było to niezbędne do wypełnienia celu tego działania. Jak wynika ze stanu faktycznego, spółdzielnia udostępniła dane osobowe skarżących w celu

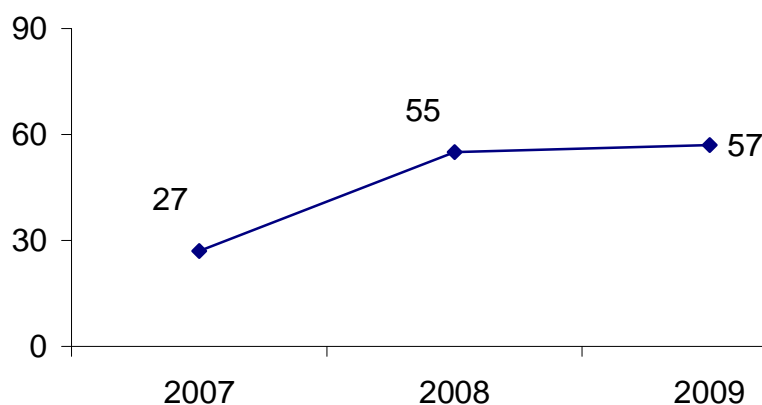
⁷⁰ DOLiS-440-212/09.

⁷¹ Pismo z dnia 24 marca 2009 r. DOLiS-440-877/08/10453/09.

⁷² Pismo z 16 kwietnia 2009 r. DOLiS-440-755/08/14594/09.

sprawozdawczym. Jednakże w ocenie organu sprawozdanie pozbawione tych danych nie utraciłoby waloru informacyjnego, albowiem wynikałoby z niego kiedy, w jakich sprawach i z jakim rezultatem prezes zarządu spółdzielni czy też spółdzielnia występowali przed sądem. Zatem udostępnienia ww. danych osobowych nie można było uznać za niezbędne. Nie miał bowiem znaczenia fakt, że przedmiotowe postępowania sądowe były jawne, ponieważ okoliczność ta nie zwalniała spółdzielni z obowiązku dochowania należytej staranności w procesie przetwarzania danych osobowych skarżących, tj. zapewnienia, aby ich dane były adekwatne do celu, w jakim są przetwarzane (udostępniane).

W podsumowaniu należy stwierdzić, że w analizowanym roku 2009 odnotowano wzrost liczby skarg na przetwarzanie danych przez ww. podmioty, w szczególności w przedmiocie upubliczniania danych osobowych.



Wykres 7: Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych osobowych z zakresu mieszkalnictwa, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

3.2.7 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 Wizowej⁷⁴ 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.

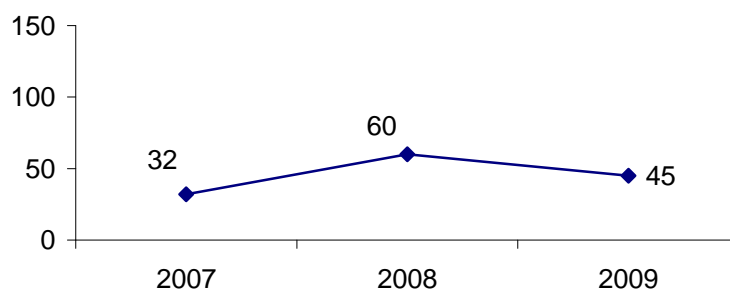
⁷³ Pismo z 15 grudnia 2009 r. DOLiS-440-475/09/46898.

⁷⁴ 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.

W 2009 roku Generalny Inspektor Ochrony Danych Osobowych rozpatrzył **27 spraw** z tego sektora, tj. o 20 więcej niż w roku 2008. W sprawach tych skarżący najczęściej żądali usunięcia ich danych osobowych, ponieważ w ich ocenie zostały one bezpodstawnie zamieszczone w tym systemie.

3.2.8 Telekomunikacja

W 2009 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **45 skarg** na podmioty z tego sektora.



Wykres 8: Zestawienie porównawcze liczby skarg dotyczących sektora telekomunikacji, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

Skargi te najczęściej dotyczyły udostępnienia przez operatora danych osobowych firmie windykacyjnej w celu dochodzenia zaległych świadczeń wynikających z umowy o świadczenie usług telekomunikacyjnych, nierespektowania sprzeciwu osób skarżących wobec przetwarzania ich danych w celach marketingowych⁷⁵ oraz dokonywania kserokopii dowodu osobistego i faktury wystawionej przez dotychczasowego operatora w związku z przenoszeniem numeru telefonu do innej sieci i posługiwanie się uzyskanymi w ten sposób danymi w celu egzekwowania od niej należności, której istnienie osoba skarżąca kwestionowała.⁷⁶ W jednej ze spraw operator telekomunikacyjny przetwarzał dane osobowe w celach marketingowych, pomimo wniesienia sprzeciwu w tym zakresie, tłumacząc ten fakt wystąpieniem błędu w systemie informatycznym firmy telemarketingowej, tj. podmiotu przetwarzającego dane na zlecenie Spółki w związku z realizowaniem kampanii marketingowej. Tak więc sprzeciw ten nie został odnotowany w systemie ww. podmiotu.⁷⁷ W innej sprawie, jeden z operatorów telekomunikacyjnych – nie legitymując się żadną z przesłanek wymienionych w art. 23 ust. 1 pkt. 1-5 ustawy o ochronie danych osobowych - udostępnił dane osobowe skarżącego w regionalnej książce telefonicznej bez podstawy prawnej.

⁷⁵ DOLiS-440-263/09, DOLiS-440-156/09.

⁷⁶ DOLiS-440-227/09.

⁷⁷ Pismo GIODO z 9 czerwca 2009 r. DOLiS-440-156/09/21050.

3.2.9 Zatrudnienie

W 2009 r. wpłynęło **99 skarg** na postępowanie pracodawców w związku z procesem rekrutacji i zatrudnianiem pracowników. Jak co roku znalazły się wśród nich skargi na pracodawców żądających od związków zawodowych ujawnienia danych osobowych osób objętych ochroną związkową. W takich sprawach GODO wydawał decyzje administracyjne, w których wskazywał na bezzasadność pozyskiwania tego typu zbiorczych informacji przez pracodawcę bez wyraźnej legitymacji ustawowej. Pojawiały się też skargi na udostępnienie dokumentów z akt osobowych pracownika bez jego zgody i wiedzy.⁷⁸

W sprawach związanych z pozyskiwaniem przez pracodawcę informacji o osobach korzystających z ochrony związku zawodowego, GODO wydał decyzje nakazujące usunięcie uchybień w tym zakresie. Wskazał przy tym, że pozyskiwanie to jest dopuszczalne jedynie w sytuacji, gdy przepisy prawa pracy przewidują w stosunku do tych osób współdziałanie pracodawcy z zakładową organizacją związkową w indywidualnych sprawach, zgodnie z art. 23² Kodeksu pracy. Organ wskazał, iż przepis art. 30 ust. 2¹ ustawy o związkach zawodowych, nie upoważnia pracodawcy do wnoszenia o przekazanie przez związek danych osobowych pracowników korzystających z ochrony związku w formie imiennej listy. Zdaniem Generalnego Inspektora, realizacja takiego wniosku skutkowałaby pozyskaniem danych osobowych pracowników objętych ochroną związkową również na zapas, co w świetle przepisów ustawy o ochronie danych osobowych jest niedopuszczalne. Należy przy tym podkreślić, że Generalny Inspektor nie kwestionuje prawa pracodawcy do pozyskiwania informacji o pracownikach korzystających z ochrony związkowej, ale jedynie sposób realizacji tego prawa. Zdaniem Generalnego Inspektora, pracodawca, 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.

W 2009 r. GODO wydał również decyzję administracyjną, mocą której nakazał spółce - byłemu pracodawcy skarżącego - usunięcie jego danych zawartych w ekspertyzie z zakresu badania pisma ręcznego. Organ uznał, że nie istniał żaden przepis prawa, który upoważniałby prezesa spółki do udostępnienia danych skarżącego przetwarzanych w jego aktach osobowych w celu sporządzenia ekspertyzy grafologicznej mającej na celu zidentyfikowania autora anonimowego pisma szkalującego prezesa spółki.⁷⁹

⁷⁸ DOLiS-440-262/09, DOLiS-440-255/09.

⁷⁹ Decyzja z 16 marca 2009 r. DOLiS/DEC-200/09/8968,8970.

Adresatem kolejnej decyzji⁸⁰ był bank, któremu GODO nakazał przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych osób w nim zatrudnionych na podstawie umów o pracę oraz umów cywilno-prawnych poprzez usunięcie danych osobowych dotyczących relacji rodzinnych i osobistych tych osób z innymi osobami zatrudnionymi w banku. Bank ten wprowadził bowiem obowiązek informowania przez osoby w nim zatrudnione na podstawie powyższych umów o relacjach rodzinnych i osobistych z innymi osobami zatrudnionymi w tym podmiocie według ustalonego wzoru formularza. Jako cel pozyskiwania tych informacji przywołał konieczność zapewnienia bezpieczeństwa jego funkcjonowania jako instytucji zaufania publicznego od strony organizacyjno-formalnej. Generalny Inspektor Ochrony Danych Osobowych zakwestionował powyższą argumentację, wskazując, że z uwagi na wątpliwości w przedmiocie swobody wyrażania zgody przez pracowników ogólną podstawą, na jakiej powinno się opierać żądanie przez pracodawcę od pracowników podania danych osobowych stanowi art. 22¹ Kodeksu pracy. Jednakże w niniejszej sprawie nie będzie miał on zastosowania, ponieważ nie stanowi on podstawy do pozyskiwania danych osobowych we wskazanym zakresie. Organ zaznaczył, że przyczyn ewentualnych nieprawidłowości w funkcjonowaniu banku nie należy upatrywać w braku informacji o relacjach osobistych i rodzinnych pracowników, lecz w braku czy złym funkcjonowaniu mechanizmów, które wystąpieniu takim negatywnym zjawiskom powinny zapobiegać.

GODO wystąpił również do Prezesa Zarządu jednej ze spółek o zmodyfikowanie klauzuli zawierającej zgodę na przetwarzanie danych osobowych oraz informację o przetwarzaniu danych osobowych, zamieszczonej w dokumencie przekazywanym osobom, których dane są zbierane w związku z procesem rekrutacji oraz na stronie internetowej i dostosowanie jej do wymogów wynikających z ustawy o ochronie danych osobowych. W ocenie Generalnego Inspektora, powyższa klauzula nie spełnia określonych w przepisach ustawy wymogów dotyczących przede wszystkim treści obowiązku informacyjnego w przypadku zbierania danych osobowych od osoby, której dane dotyczą. Organ stwierdził, że konieczne jest oddzielenie klauzuli zawierającej informacje, o których mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, od klauzuli ze zgodą na przetwarzanie danych osobowych oraz uzupełnienie jej o informację dotyczącą adresu siedziby administratora danych i dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.⁸¹

Na uwagę zasługuje jedna ze spraw, w której GODO wydał decyzję⁸² nakazującą spółce wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego poprzez usunięcie ze strony internetowej spółki jego danych osobowych w zakresie wizerunku, imienia,

⁸⁰ Decyzja GODO z 19 maja 2009 r. DOLiS/DEC-400/09.

⁸¹ Pismo GODO z 28 maja 2009 r. DOLiS-440-85/09/19574.

⁸² Decyzja GODO z 9 czerwca 2009 r. DOLiS/DEC-515/09/21191,21193.

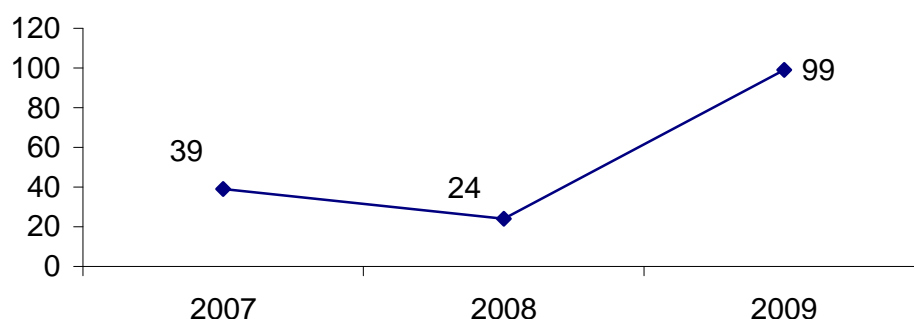
nazwiska i adresów poczty elektronicznej. Z analizy tej sprawy wynika, że skarżący był pracownikiem spółki. Po ustaniu stosunku pracy spółka nie usunęła ze strony internetowej ww. danych osobowych skarżącego. W przedłożonych wyjaśnieniach wskazała natomiast, iż podejrzewa go o dopuszczenie się naruszeń w związku z prowadzoną przez niego działalnością konkurencyjną. Z tego tytułu, w celu dochodzenia od niego roszczeń, spółka gromadziła materiał dowodowy, którego istotnym elementem były pracownicze konta e-mail skarżącego. Wskazano bowiem, że na jeden z tych adresów były klient spółki przesłał e-mail, co stanowi dowód na prowadzenie przez skarżącego działalności konkurencyjnej w okresie trwania zatrudnienia. W ocenie Generalnego Inspektora Ochrony Danych Osobowych, powyższa argumentacja nie zasługiwała na uwzględnienie. Co prawda spółka ma prawo dochodzić swych roszczeń i w tym celu i na tej podstawie przetwarzać dane osobowe, jednakże w niniejszej sprawie ciągła aktywność przedmiotowych adresów e-mail oraz udostępnianie na stronie internetowej spółki zdjęć skarżącego niewątpliwie naruszało jego prawa i wolności chociażby w zakresie dotyczącym jego wizerunku. Skarżący nie jest już pracownikiem spółki. Prowadzi obecnie własną działalność gospodarczą, z którą chce być utożsamiany. Ciągła aktywność, a zarazem możliwość przesyłania wiadomości na przedmiotowe adresy e-mail, pośrednio nadal utożsamiają osobę skarżącego ze spółką, co w obecnej sytuacji daje fałszywy obraz osoby skarżącego. Ponadto osoba, do której zgodnie z jej identyfikatorem zawartym w adresie kierowana jest korespondencja, nie ma możliwość zapoznania się nią, co z kolei stanowi przejaw naruszenia wolności tej osoby do prawa komunikowania się oraz ochrony tajemnicy jej korespondencji.

Ponadto GIODO skierował do Ministra Sprawiedliwości wniosek o zwrócenie szczególnej uwagi na konieczność respektowania przepisów ustawy o ochronie danych osobowych przy udostępnianiu danych osobowych z Krajowego Rejestru Karnego działającego przy Ministerstwie Sprawiedliwości.⁸³ Impulsem do niniejszego wystąpienia stała się skarga dotycząca udostępnienia danych osobowych przez Krajowy Rejestr Karny na rzecz pracodawcy (spółdzielni), czego bezpośrednim następstwem było wypowiedzenie umowy o pracę. W ramach przeprowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych postępowania wyjaśniającego ustalono, że dane osoby zostały udostępnione spółdzielni na skutek błędnej interpretacji przepisów ustawy o Krajowym Rejestrze Karnym. W złożonym przez ww. spółdzielnię wniosku o udostępnienie danych z Rejestru jako podstawę prawną uzasadniającą konieczność pozyskania danych wskazano bowiem „art. 15 § 3 ustawy Prawo Spółdzielcze w zw. z art. 2 ust. 1 i 3 statutu spółdzielni”. W odniesieniu natomiast do art. 6 ust.1 pkt 10 ww. ustawy regulującej działalność Rejestru, prawo do uzyskania informacji o osobach, których dane osobowe zgromadzone zostały w Rejestrze, przysługuje pracodawcom, w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg

⁸³ Pismo GIODO z 10 sierpnia 2009 r. DOLiS-440-756/08/29280/09.

niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej. Literalne brzmienie ww. przepisu ustawy o Krajowym Rejestrze Karnym nie pozostawia żadnych wątpliwości co do braku możliwości powołania się przy wnioskowaniu o udostępnienie danych z Rejestru na normy wynikające z przepisów rangi niższej niż ustawowa. Organ uznał więc, że Krajowy Rejestr Karny nie może udostępniać danych osobowych na podstawie np. zapisów statutów spółek, spółdzielni czy stowarzyszeń.

W roku sprawozdawczym 2009 odnotowano gwałtowny, ponad czterokrotny, wzrost liczby skarg dotyczących sektora zatrudnienia, co obrazuje Wykres 9.



Wykres 9: Zestawienie porównawcze liczby skarg dotyczących sektora zatrudnienia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

3.2.10 Ubezpieczenia społeczne, majątkowe i osobowe

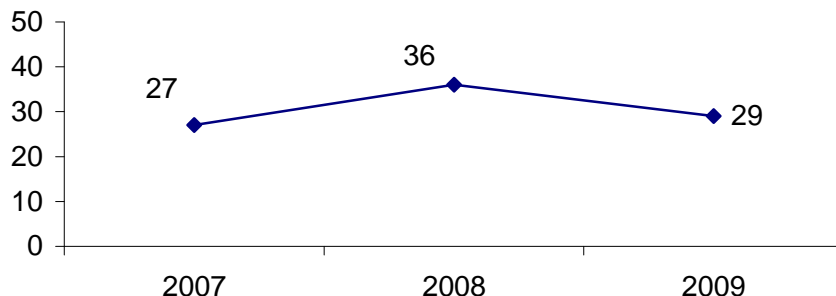
Niniejszy sektor obejmuje sprawy przetwarzania danych osobowych w związku z ubezpieczeniem społecznym, majątkowym i osobowym. Skargi dotyczyły przede wszystkim kwestii legalności pozyskania przez podmioty prowadzące działalność ubezpieczeniową danych osobowych osób skarżących, udostępniania z ich zbiorów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

W 2009 r. wpłynęło **29 skarg** na podmioty z tego sektora. Wśród nich znalazły się skargi, w których na przykład wnioskodawca skarżył się na odmowę udostępnienia przez zakład ubezpieczeń danych osobowych z prowadzonego przez tę instytucję zbioru danych, jako niezbędnych do dochodzenia przez niego roszczeń od osoby, której danych żądał. A w drugiej sprawie była odwrotna sytuacja, inny wnioskodawca skarżył się, że zakład ubezpieczeń udostępnił dokumentację zawierającą jego dane osobowe osobie, z którą pozostaje on w sporze, i która dołączyła uzyskane dokumenty do akt postępowania sądowego.

Adresatem innej skargi było towarzystwo ubezpieczeń, które udostępniło dane osobowe skarżącej zawarte w dokumentacji szkodowej, w tym numer konta bankowego, osobie odpowiedzialnej za powstałą szkodę.⁸⁴ Inna skarga stanowiła z kolei wniosek o udostępnienie skarżącemu przez towarzystwo ubezpieczeniowe żądanych przez niego dokumentów oraz ustosunkowanie się do działań towarzystwa podjętych w sprawie skarżącego.⁸⁵ W odpowiedzi GODO wskazał skarżącemu, iż nie jest kompetentny do udostępniania dokumentów ani dokonywana oceny stosunku zobowiązaniowego łączącego strony umowy cywilnoprawnej.

W innych analizowanych sprawach skarżący podnosili, że np. ich dane osobowe były nadal przetwarzane, mimo wypowiedzenia umowy ubezpieczenia samochodu, albo że firma ubezpieczeniowa dokonuje kserokopii całej strony pocztowej książki nadawczej i włącza ją do akt toczącego się postępowania, ujawniając w ten sposób zawarte tam informacje o przedsiębiorcach. Organ w odpowiedzi na tą ostatnią skargę stwierdził, iż informacje związane ściśle z prowadzoną działalnością gospodarczą i identyfikujące podmiot w obrocie gospodarczym nie podlegają ochronie przewidzianej w ustawie o ochronie danych osobowych.

Podsumowując, należy zauważyć, że w porównaniu do lat ubiegłych zmalała liczba skarg dotyczących przetwarzania danych osobowych w sektorze ubezpieczeń (zob. Wykres 10).



Wykres 10: Zestawienie porównawcze liczby skarg dotyczących sektora ubezpieczeń, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

3.2.11 Zdrowie

W 2009 r. wpłynęło **7 skarg** dotyczących tego sektora. W skargach najczęściej wskazywano na przypadki przesyłania pacjentom przez niepubliczne placówki medyczne dokumentacji medycznej innego pacjenta,⁸⁶ udostępniania ich danych dotyczących zdrowia oraz przyjmowanych leków osobie trzeciej⁸⁷ czy fałszowania dokumentacji medycznej pacjentów w celu wyłudzenia pieniędzy z NFZ.⁸⁸

⁸⁴ DOLiS-440-154/09, DOLiS-440-151/09.

⁸⁵ DOLiS-440-254/09.

⁸⁶ DOLiS-440-186/09.

⁸⁷ DOLiS-440-239/09.

⁸⁸ DOLiS-440-164/09.

Do GIODO skierowano ponadto anonimową informację o działalności związku lekarzy rodzinnych - pracodawców, który żądali od swoich członków przedstawiana im list pacjentów oraz sprawozdań z wykonywanych świadczeń medycznych (zawierających również dane wrażliwe pacjentów).⁸⁹ Organowi ds. ochrony danych osobowych wskazano także, że na stronie internetowej jednego ze szpitali znajdują się dane osobowe pacjentów, np. imiona, nazwiska, numery PESEL oraz wyniki ich badań.⁹⁰

Natomiast inna skarga dotycząca omawianej tematyki zawierała prośbę o zbadanie przez GIODO formularza stosowanego przez hotel, w którym konieczne jest podanie przez gościa szczegółowych informacji o stanie zdrowia, w tym informacji o przebytych chorobach. Odmowa udostępnienia tych danych wiązała się z brakiem możliwości skorzystania z usług tego podmiotu.⁹¹ W innej sprawie GIODO pozyskał informację, iż niepubliczny zakład opieki zdrowotnej po zakończeniu prowadzenia działalności polegającej na świadczeniu usług medycznych pozostawił w pomieszczeniach, w których prowadził tą działalność, dokumentację medyczną pacjentów. W związku z powyższym GIODO zwrócił się do wojewody o podjęcie określonych działań i zabezpieczenie tej dokumentacji zgodnie z przepisami prawa.⁹²

Pojawiła się również sprawa, w której były pacjentki Izby Porodowej jednego z wojewódzkich szpitali specjalistycznych skarżyły się, że ich dane, jak imię, nazwisko, wiek, rodzaj schorzeń, przebieg leczenia i wykonane procedury medyczne zostały udostępnione podczas spotkania u burmistrza miasta poświęconego nieprawidłowościom w funkcjonowaniu⁹³ tej placówki. W przedmiotowej sprawie dyrektor szpitala - za pośrednictwem burmistrza miasta - udostępnił dane osobowe pacjentek dyrektorowi Miejskiego Zespołu Opieki Zdrowotnej. Wobec braku podstaw prawnych takiego udostępniania, GIODO wystąpił do dyrektora szpitala o podjęcie stosowanych działań celem wyeliminowania tego rodzaju praktyk w przyszłości. W sprawie tej GIODO interweniował dwukrotnie. Organ wskazał, że w pełni rozumie intencję dyrektora szpitala i podziela pogląd o konieczności eliminowania wszelkich zaniedbań i nieprawidłowości w procesie udzielania świadczeń medycznych. Jednakże przetwarzanie danych osobowych pacjentów nie może odbywać się z naruszeniem ustawy o ochronie danych osobowych.⁹⁴

3.2.12 Inne

Wśród skarg, które Generalny Inspektor Ochrony Danych Osobowych badał w 2009 r., wyodrębnić należy te, które z racji swojego przedmiotu nie mogły być zakwalifikowane do wcześniej

⁸⁹ DOLiS-440-190/09.

⁹⁰ DOLiS-440-209/09.

⁹¹ DOLiS-440-207/09.

⁹² Pismo z 26 lutego 2009 r. DOLiS-440-113/09/6532.

⁹³ Pismo z 25 marca 2009 r. DOLiS-440-903/08/10600/09.

przedstawionych kategorii spraw. Ich liczba wyniosła **315**, co w porównaniu z rokiem 2008, gdzie spraw tych było 478, wskazuje na znaczny ich spadek.

Skargi te dotyczyły m.in. bezprawnego – bo bez zgody i wiedzy osób skarżących – ujawniania ich danych osobowych w publikowanych powszechnie książkach telefonicznych, udostępniania faktur na zakup towaru zawierających dane osobowe osób skarżących osobom trzecim przez wystawców tych faktur, bezprawnego wykorzystywania przez pielęgniarkę środowiskową danych osobowych osób skarżących w celu wykazania w Narodowym Funduszu Zdrowia tych osób jako jej podopiecznych oraz wykorzystywania danych osobowych przez różnego rodzaju firmy windykacyjne w celu dochodzenia należności za zakupione towary i usługi.

W odniesieniu do tego sektora wpłynęła także skarga na nieprawidłowe doręczanie korespondencji na nieaktualny adres, pomimo wskazania administratorowi aktualnego adresu do korespondencji, co mogło spowodować ujawnienie danych osobowych osobom nieuprawnionym. GODO był również adresatem prośby o wyjaśnienie, w jaki sposób jedna z fundacji weszła w posiadanie danych osobowych skarżącej i przesłała jej wypełniony druk z prośbą o darowiznę.⁹⁵

Wiele ze skarg zaliczonych do tej kategorii dotyczyło udostępnienia danych osobowych skarżących firmom windykacyjnym przez podmioty, z którymi łączył ich stosunek zobowiązaniowy.⁹⁶ W jednej z nich wskazano, że firma windykacyjna, przesyłając dłużnikom wezwanie do zapłaty, na dowód legalności swego działania przesyłała im kopię umowy o cesję wierzytelności wraz z fragmentem alfabetycznej listy osób, w stosunku do których na podstawie tej umowy prowadzi działania windykacyjne.⁹⁷

W tym okresie organ wydał również decyzję administracyjną, mocą której nakazał dowódcy jednostki wojskowej spełnienie wobec skarżącej obowiązku informacyjnego, o którym mowa w art. 33 ustawy o ochronie danych osobowych. Organ uznał, iż pismo skarżącej spełniało wymogi pozwalające na uznanie go za wniosek złożony w trybie art. 33 ustawy oraz wskazał, iż na administratorze danych ciąży obowiązek udzielenia informacji, nawet gdyby była to odpowiedź negatywna.⁹⁸ W innej decyzji administracyjnej GODO nakazał firmie ubezpieczeniowej usunięcie danych skarżących pozyskanych od miejskiego zakładu gospodarowania nieruchomościami [ZGN]. Organ uznał, że udostępnienie danych skarżących zawartych w pełnomocnictwie do dokonania czynności związanych z wykupem lokalu złożonym w ZGN nastąpiło bez podstawy prawnej. Uznano, iż wskazany przez firmę ubezpieczeniową art. 25 ust. 1 ustawy o działalności ubezpieczeniowej⁹⁹ nie legalizuje powyższego

⁹⁴ Pismo GODO z 5 maja 2009 r. DOLiS-440-903/08/16044/09.

⁹⁵ DOLiS-440-204/09.

⁹⁶ DOLiS-440-242/09, DOLiS-440-228/09.

⁹⁷ DOLiS-440-175/09.

⁹⁸ Decyzja z 10 marca 2009 r. DOLiS/DEC-164/09/8239,8244.

⁹⁹ Zgodnie z brzmieniem tego przepisu sądy, prokuratura, Policja oraz inne organy i instytucje, na wniosek zakładu ubezpieczeń, w zakresie zadań przez ten zakład ubezpieczeń wykonywanych i w celu ich wykonania, w związku z

działania, gdyż było to pełnomocnictwo szczególne i nie dotyczyło kwestii reprezentowania skarżącej przed tym podmiotem¹⁰⁰ (decyzja nieprawomocna). Ponadto w związku z udostępnieniem powyższych informacji przez ZGN, organ wystąpił do prezydenta miasta o podjęcie odpowiednich działań mających na celu zapewnienie legalności udostępniania danych osobowych przez podległe mu zakłady gospodarowania nieruchomościami na rzecz innych podmiotów, stosownie do wymogów ustawy o ochronie danych osobowych.¹⁰¹

W kolejnej sprawie organ wystąpił także do Prezesa Zarządu Miejskiego Przedsiębiorstwa Gospodarki Nieruchomościami jednego z miast, w związku z umieszczeniem w piśmie skierowanym do osoby trzeciej danych osobowych skarżących bez ich zgody. W postępowaniu wyjaśniającym ustalono, iż wzywając członka wspólnoty mieszkaniowej do respektowania regulaminu porządku domowego, podmiot ten udostępnił mu dane osobowe pozostałych członków wspólnoty, którzy zainicjowali postępowanie w tej sprawie.¹⁰²

Znaczna liczba skarg, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w 2009 r., dotyczyła odmowy udostępnienia przez administratorów danych osobowych z posiadanych przez nich zbiorów danych w celu wykorzystania do sporządzenia prawidłowego pod względem formalnym pozwu do sądu powszechnego. W sprawach tych postępowanie kończyło się nakazem udostępnienia wnioskodawcy żądanych danych osobowych. W kolejnej decyzji Generalny Inspektor Ochrony Danych Osobowych nakazał spółdzielni udostępnienie danych osobowych w zakresie informacji o wykupieniu mieszkania oraz numeru księgi wieczystej lokalu mieszkalnego. Powyższe dane osobowe niezbędne były spółce do dokonania wpisu hipoteki przymusowej, aby zabezpieczyć i ostatecznie wyegzekwować swoją wierzytelność. Spółdzielnia, powołując się na przepisy ustawy o ochronie danych osobowych, odmówiła udostępnienia żądanych danych osobowych. Natomiast w wyjaśnieniach przesłanych organowi wskazała, iż w związku z posiadaniem przez spółkę tytułu wykonawczego, powinna ona skierować wniosek do komornika, który ma prawo żądać takich informacji. Generalny Inspektor Ochrony Danych Osobowych uznał stanowisko spółdzielni za bezpodstawne, ponieważ wniosek spółki o udostępnienie przedmiotowych danych osobowych spełniał wymogi określone w art. 29 ustawy o ochronie danych osobowych. Ponadto w ocenie organu wykorzystanie danych przez wierzyciela w celu dochodzenia swoich wierzytelności nie może być uznane za naruszenie praw i wolności osób, których dane dotyczą. Prawo do prywatności nie ma

wypadkiem lub zdarzeniem będącym podstawą ustalania odpowiedzialności, udzielają informacji o stanie sprawy oraz udostępniają zebrane materiały, jeżeli są one niezbędne do ustalenia okoliczności tych wypadków i zdarzeń losowych oraz wysokości odszkodowania lub świadczenia.

¹⁰⁰ Decyzja z 10 marca 2009 r. DOLiS/DEC-180/09/8363,8366,8369,8371,8372.

¹⁰¹ Pismo z 10 marca 2009 r. DOLiS-440-228/07/8374/09.

¹⁰² Pismo z 3 marca 2009 r. DOLiS-440-848/08/7218/09.

bowiem charakteru absolutnego, a jego ochrona nie może odbywać się kosztem braku poszanowania praw innych osób.¹⁰³

W omawianym okresie GODO wydał również decyzję¹⁰⁴ nakazującą klubowi piłkarskiemu usunięcie ze swoich zbiorów danych osobowych skarżącego. Klub ten przetwarzał dane osobowe skarżącego dotyczące zakupu przez niego biletów na trybunę odkrytą, wyjazdu grupy kibiców klubu na mecz i udziału skarżącego w zamieszkach w trakcie meczu. W związku z powyższym organ wskazał, że zgodnie z art. 13 ust. 1 ustawy o bezpieczeństwie imprez masowych, organizator meczu piłki nożnej zapewnia identyfikację osób uczestniczących w imprezie. Zakres przetwarzanych danych identyfikujących osoby uczestniczące obejmuje w przypadku meczu piłki nożnej – imię i nazwisko oraz numer PESEL, a w razie gdyby nie został on nadany – rodzaj, serię i numer dokumentu potwierdzającego tożsamość (ust. 4 pkt 1), w przypadku rozgrywek meczów piłki nożnej w ramach ligi zawodowej – imię i nazwisko, wizerunek twarzy oraz numer PESEL, a w razie gdy nie został on nadany – rodzaj, serię i numer dokumentu potwierdzającego tożsamość (ust. 4 pkt 2). Dane, o których mowa w ust. 4, są przechowywane przez organizatora przez okres 2 lat od dnia odbycia się meczu piłki nożnej (ust. 5). Przetwarzanie danych osobowych skarżącego przez klub, wobec upływu terminu o którym mowa w art. 13 ust. 5 ww. ustawy, odbywało się natomiast bez podstawy prawnej. W związku z powyższym, działając na podstawie art. 18 ust. 1 pkt 6 ustawy, Generalny Inspektor nakazał klubowi usunięcie danych osobowych skarżącego przetwarzanych w zbiorach danych tego podmiotu.

W analizowanym roku sprawozdawczym GODO zwrócił się do prezesa firmy z sektora paliwowo-energetycznego o podjęcie działań w celu dostosowania treści stosowanych przez tę Spółkę wzorców formularzy „Umowy kompleksowej dostarczania paliwa gazowego”, służących do aktualizacji umów sprzedaży paliwa zawartych przed 1 lipca 2007 r. do wymogów ustawy o ochronie danych osobowych.¹⁰⁵ Organ powziął wątpliwości co do zgodności przetwarzania danych osobowych pozyskiwanych za ich pomocą z wymogami ustawy o ochronie danych osobowych. Spółka pozyskiwała bowiem od swoich klientów, będących osobami fizycznymi, dane osobowe w zakresie ich numeru NIP, adresu do korespondencji, numeru telefonu oraz adresu poczty elektronicznej, a ich podanie, jak wynikało z treści formularza, było niezbędne dla zawarcia przedmiotowej umowy. W niniejszej sprawie brak było przepisów prawa, które stanowiłyby podstawę do zbierania w celu zawarcia kompleksowej umowy dostarczania paliwa gazowego od odbiorców indywidualnych danych osobowych innych niż imię, nazwisko, adres zamieszkania oraz identyfikujący osobę fizyczną numer PESEL. Nie ulegało wątpliwości, iż powyższy zakres danych był również wystarczający do realizacji zawartej umowy oraz dochodzenia ewentualnych roszczeń wynikających z jej niewykonania. Wobec

¹⁰³ Decyzja z 6 kwietnia 2009 r. DOLiS/DEC-273/09/12240,12242,12243.

¹⁰⁴ Decyzja GODO z 31 sierpnia 2009 r. DOLiS/DEC-875/09/31524,31527.

¹⁰⁵ Pismo GODO z 12 sierpnia 2009 r. DOLiS-440-269/09.

powyższego Generalny Inspektor Ochrony Danych Osobowych stwierdził, że pozyskiwanie innych kategorii danych osobowych niż wskazane powyżej może się odbyć wyłącznie za zgodą osoby zainteresowanej.

Natomiast w związku z uzyskaniem informacji o wykonywaniu okazjonalnych zdjęć uczniom szkoły podstawowej przez podmiot prowadzący w tym zakresie działalność gospodarczą, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do dyrektora szkoły o zachowanie szczególnej staranności w przedmiocie ochrony wizerunku oraz prywatności uczniów.¹⁰⁶ Organ wskazał, iż szkoła oprócz wypełniania swoich dydaktyczno-wychowawczych obowiązków, powinna jednocześnie czuwać nad zapewnieniem prawa do ochrony prywatności i wizerunku dzieci. Za naruszenie prawa do takiej ochrony może być uznane wykonanie dziecku fotografii, nawet za zgodą dziecka. Generalny Inspektor Ochrony Danych Osobowych podkreślił, że ustawodawca przepisami Kodeksu cywilnego, co do zasady, uzależnił skuteczność oświadczeń woli (w tym oświadczeń wyłączających bezprawność wkraczania w prawa osób) składanych przez osoby małoletnie, od faktu ich potwierdzenia przez rodziców czy też opiekunów prawnych małoletnich, a w przypadku dzieci, które nie ukończyły lat trzynastu, wykluczył możliwość skutecznego składania takich oświadczeń. Jednocześnie w przedmiotowym wystąpieniu zostało zaznaczone, iż dzieci nie są w pełni świadome konsekwencji podejmowanych przez siebie działań. W związku z powyższym wskazane jest, aby decyzję o wykonaniu zdjęć dziecka przez podmiot prowadzący działalność w tym zakresie, podejmowali rodzice lub opiekunowie prawni dzieci, nie zaś same dzieci.

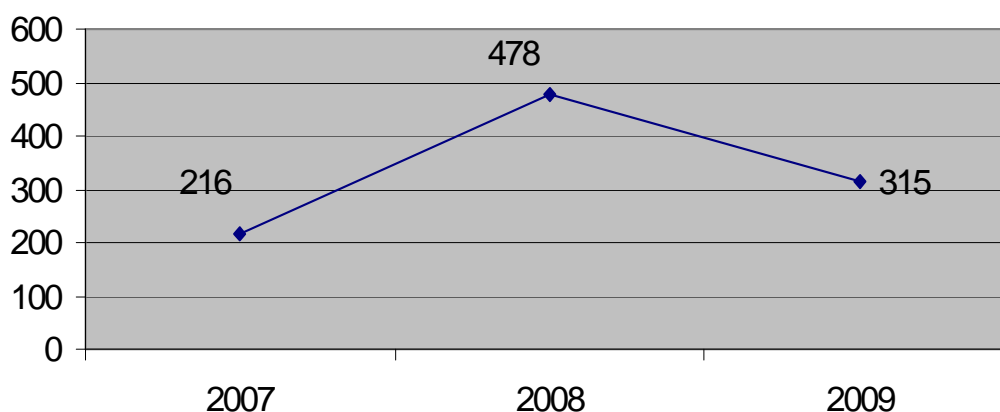
GIODO wydał również decyzję nakazującą uczelni publicznej udostępnienie skarżącej danych osobowych jej syna w zakresie obejmującym informację o ewentualnym przyznaniu mu stypendium.¹⁰⁷ Giodo wskazał, iż skarżąca w sposób wiarygodny w kierowanych do uczelni pismach uzasadniła potrzebę pozyskania informacji odnośnie do ewentualnego przyznania jej synowi stypendium. Złożony przez nią wniosek w podanym zakresie odpowiadał też wymogom formalnym wynikającym z brzmienia art. 29 ust. 3 ustawy o ochronie danych osobowych - miał bowiem formę pisemną, został umotywowany (potrzebą wykorzystania ww. informacji dla celu dochodzenia roszczeń związanych ze spoczywającym na skarżącej obowiązkiem alimentacyjnym wobec syna), zawierał informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych (w korespondencji z uczelnią skarżąca kilkakrotnie podawała imię, nazwisko i adres syna), wskazywał ich zakres i przeznaczenie. Jednocześnie, mając na uwadze prawne gwarancje ochrony przed roszczeniami zgłaszanymi w postępowaniu sądowym (w tym także w sprawach dotyczących alimentacji), brak było postaw by uznać, że udostępnienie skarżącej informacji o ewentualnym przyznaniu jej synowi stypendium wiązałoby się z naruszeniem jego praw czy wolności. Przyjęcie przeciwnego stanowiska - skutkujące

¹⁰⁶ Pismo Giodo z 7 września 2009 r. DOLiS-440-63/09/32439.

¹⁰⁷ Decyzja z 13 października 2009 r. DOLiS/DEC-1025/09/37281,37287,37293.

pozbawieniem osoby zobligowanej do alimentacji dostępu do informacji na temat sytuacji finansowej alimentowanego - oznaczałoby w istocie bezzasadną ochronę tego ostatniego przed roszczeniami wynikającymi ze zmiany jego sytuacji finansowej. Z tych samych powodów nie można było uznać, że udostępnienie skarżącej informacji o ewentualnym przyznaniu jej synowi stypendium stanowiłoby istotne naruszenie jego dóbr osobistych lub dóbr osobistych innych osób (art. 30 pkt 4 ustawy). Oczywiście było zarazem, że zadośćuczynieniu wnioskowi skarżącej w omawianym zakresie nie stała na przeszkodzie żadna z pozostałych okoliczności wymienionych w art. 30 ustawy o ochronie danych osobowych (pkt. 1–3).

W analizowanym okresie, w stosunku do roku poprzedniego, o 163 zmalała liczba skarg dotyczących przetwarzania danych osobowych w szeroko rozumianym sektorze „Inne”, co przedstawia Wykres 11



Wykres 11: Zestawienie porównawcze liczby skarg z sektora „Inne”, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007–2009.

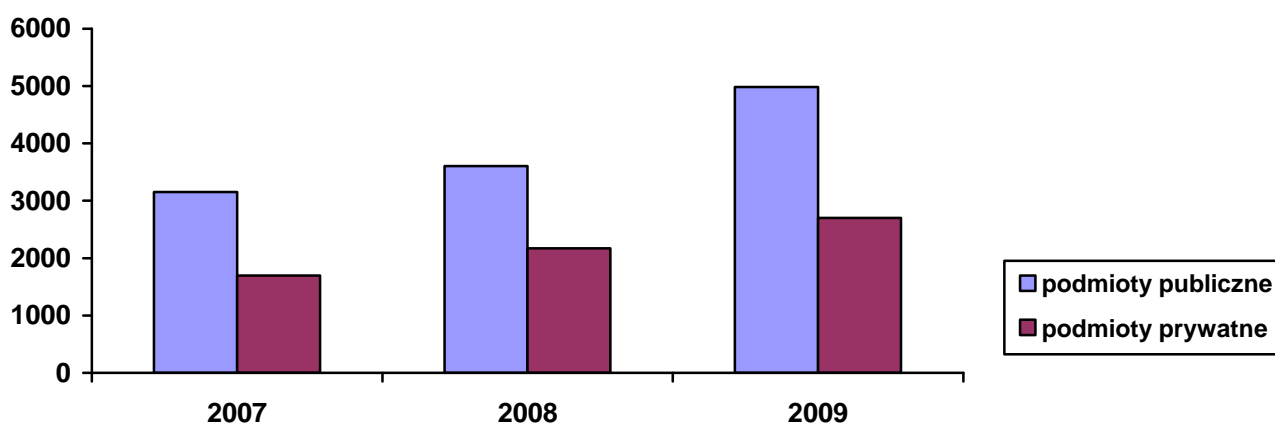
Wynikać to może z konsekwentnej polityki informacyjnej GIODO zmierzającej do upowszechnienia wiedzy o prawach i obowiązkach zarówno administratorów danych, jak i osób, których dane dotyczą.

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. Zadanie to, realizowane w Departamencie Rejestracji Zbiorów Danych Osobowych, skorelowane zostało z nałożonym na administratorów danych obowiązkiem zgłaszania zbiorów danych osobowych

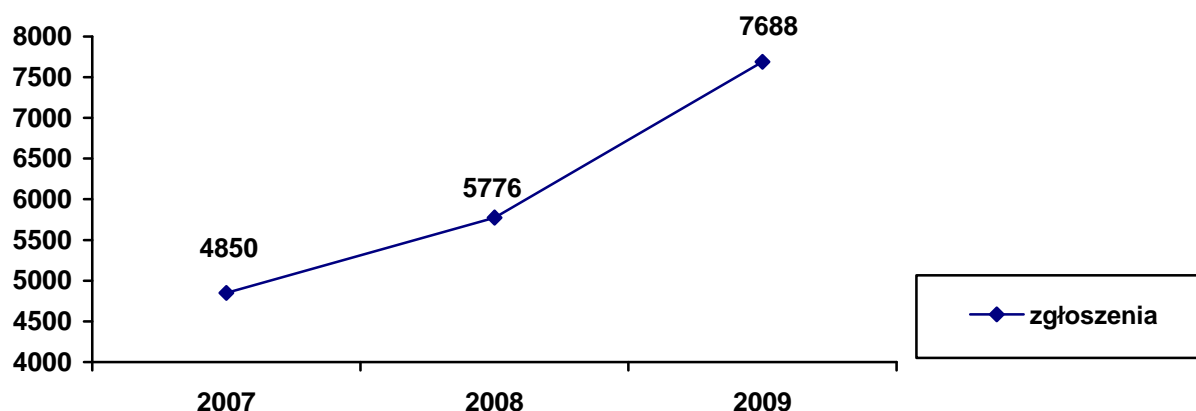
do rejestracji.¹⁰⁸ Prowadzenie ogólnokrajowego rejestru umożliwia Generalnemu Inspektorowi Ochrony Danych Osobowych m.in. sprawowanie kontroli nad prawidłowością procesu przetwarzania danych osobowych, a także zapewnia obywatelom dostęp do informacji o administratorach danych i prowadzonych przez nich 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 2009 roku w związku z prowadzoną przez Generalnego Inspektora Ochrony Danych Osobowych intensywną działalnością edukacyjną i informacyjną w zakresie zasad ochrony danych osobowych i obowiązków związanych z ich realizacją, w tym obowiązku zgłoszenia do rejestracji prowadzonych zbiorów danych, znacznemu zwiększeniu uległa liczba wpływających zgłoszeń do rejestracji (w 2008 r. wpłynęło – 5776 zgłoszeń, w 2009 r. – **7688** zgłoszeń). Należy odnotować, iż najwięcej zgłoszeń pochodziło od podmiotów publicznych (**4984**), a wśród nich tradycyjnie najwięcej zbiorów zgłosiły jednostki samorządu terytorialnego. Natomiast podmioty prywatne zgłosiły do rejestracji **2704** zbiory danych osobowych.



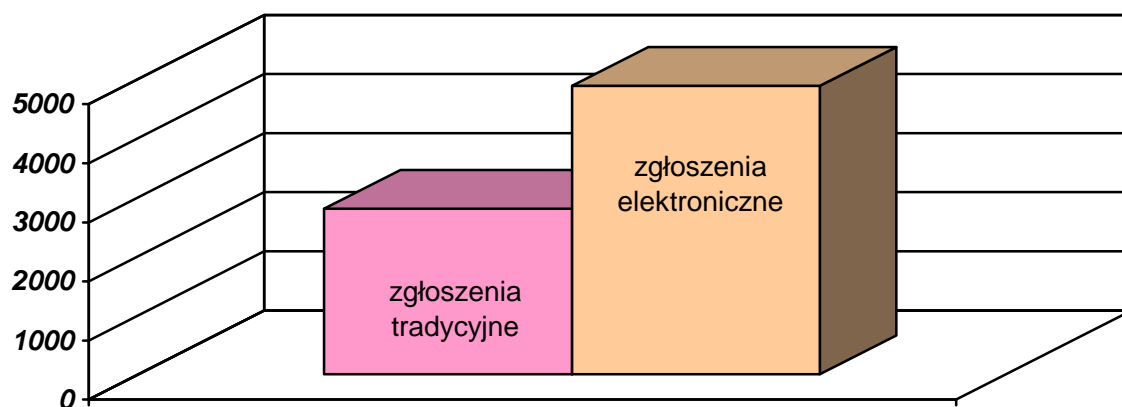
Wykres 12: Zestawienie zbiorów danych zgłoszonych do rejestracji przez podmioty z sektora publicznego i sektora prywatnego w latach 2007-2009.

¹⁰⁸ 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.



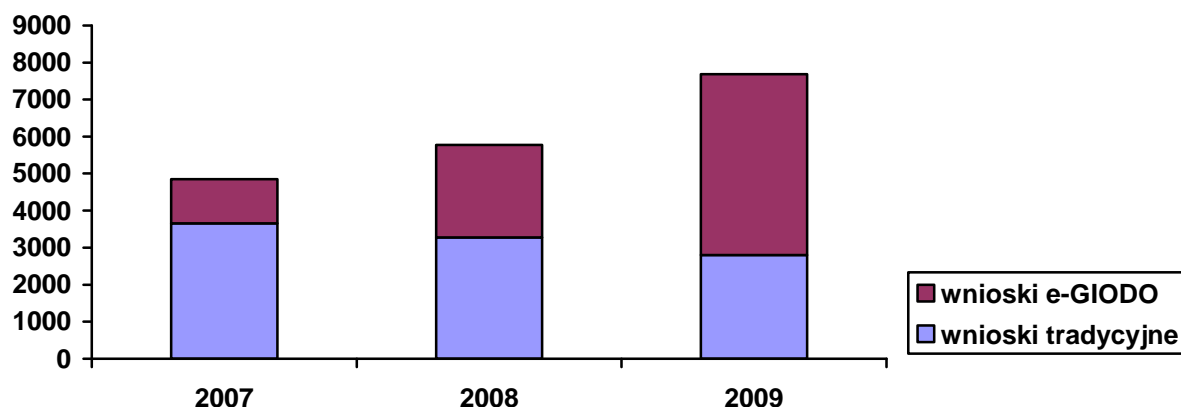
Wykres 13: Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2007-2009.

Zauważalny jest zatem znaczny wzrost - w porównaniu z ubiegłymi latami - liczby zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych. Wynika on ze wzrostu świadomości prawnej w zakresie ochrony danych osobowych, w tym obowiązku rejestracji zbiorów danych osobowych. Dominującymi pod względem ilościowym były zgłoszenia pochodzące od jednostek samorządu terytorialnego (gmin i powiatów) oraz zbiorów danych prowadzonych na podstawie przepisów ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów.¹⁰⁹ Należy podkreślić, iż w omawianym okresie na ogólną liczbę 7688 zgłoszeń zbiorów, które wpłynęły do rejestracji, **4885** zostało wypełnionych przy użyciu udostępnionego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych programu wspomagającego wypełnianie formularza zgłoszenia. Stanowi to **63,5 %** ogólnej liczby zgłoszeń dokonanych w 2009 r.



Wykres 14: Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonywanych w 2009 r. w formie tradycyjnej i przy użyciu programu wspomagającego.

¹⁰⁹ Dz. U. Nr 192, poz. 1378 z późn. zm. Przepisy powołanej ustawy wprowadziły nowe zasady przyznawania świadczeń alimentacyjnych, co z kolei doprowadziło do wzrostu liczby zgłoszeń zbiorów danych osobowych dotyczących danych osób uprawnionych do alimentów.



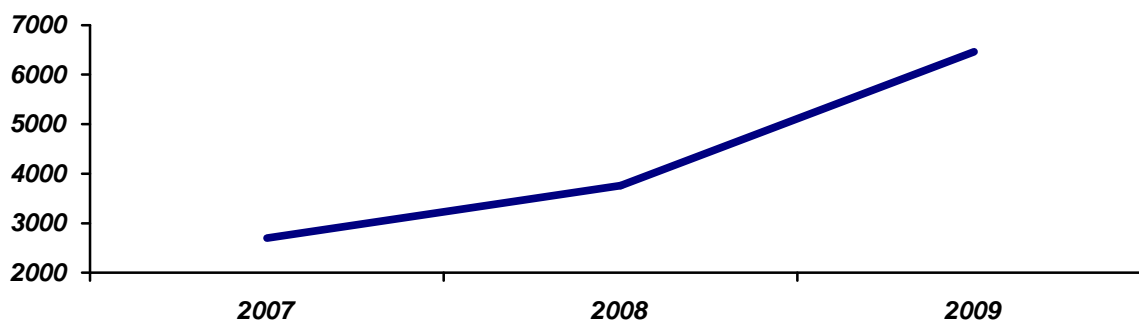
Wykres 15: Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2007-2009 w formie tradycyjnej i przy użyciu programu wspomagającego, udostępnionego na stronie www.giodo.gov.pl

Mimo iż program wspomagający wypełnianie formularza zgłoszenia cieszy się dużym zainteresowaniem administratorów danych, to jednak należy zauważyć, iż **w roku 2009 tylko 397 zgłoszeń zostało złożonych z użyciem bezpiecznego podpisu elektronicznego**, co stanowi zaledwie **8 %** zgłoszeń wypełnionych przy użyciu tego programu.

W sytuacji gdy wnioskodawca nie był zobowiązany do zgłoszenia zbioru danych osobowych do rejestracji (np. nie posiadał statusu administratora, korzystał ze zwolnienia na podstawie art. 43 ust. 1 ustawy) Generalny Inspektor Ochrony Danych Osobowych informował go o tym, powołując odpowiednie przepisy ustawy o ochronie danych osobowych. W 2009 r. wysłał łącznie **418** takich pism.

Należy zwrócić uwagę, iż administratorzy danych, przy wypełnianiu formularza zgłoszenia, nadal popełniali wiele błędów. W toku postępowań rejestracyjnych skierowano do wnioskodawców **1509 pism wskazujących braki w nadesłanych zgłoszeniach z prośbą o ich wyjaśnienie**. Do najczęściej powtarzających się uchybień należały: niekompletne informacje o sposobie wypełnienia warunków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy o ochronie danych osobowych, jak również niewłaściwy (zbyt szeroki), w stosunku do celu przetwarzania danych, zakres danych osobowych pozyskiwanych do zbioru.

W wyniku prowadzonych postępowań wyjaśniających w większości przypadków dochodzi do rejestracji zbioru. W okresie sprawozdawczym **do rejestru** prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych **zostało wpisanych 6465 zbiorów danych**.

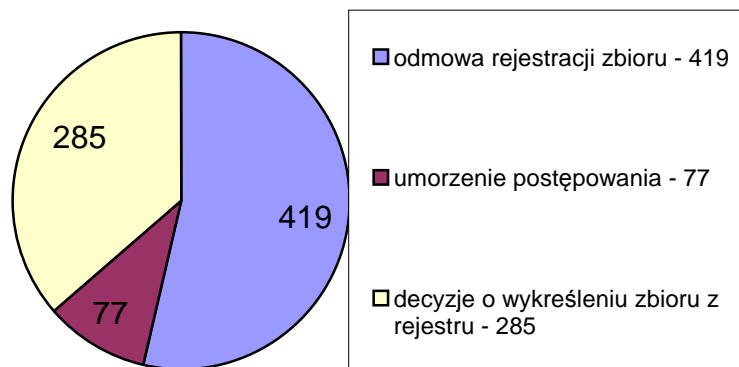


Wykres 16: Zestawienie porównawcze zarejestrowanych przez GODO zbiorów danych osobowych w latach 2007-2009.

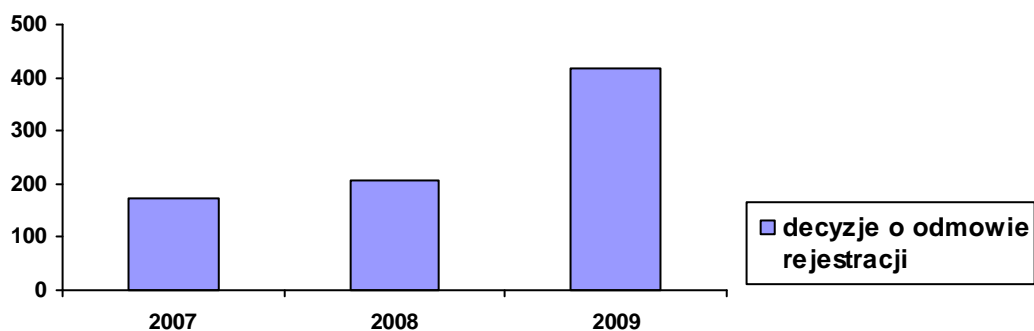
W przypadku, gdy administrator danych nie podał w zgłoszeniu informacji określonych w art. 41 ust. 1 ustawy lub ze zgłoszenia wynikało, iż przetwarzanie danych narusza zasady określone w art. 23-30 ustawy bądź urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w rozporządzeniu wykonawczym do ustawy, GODO odmawiał rejestracji zgłoszonego zbioru.¹¹⁰ W 2009 r. Generalny Inspektor Ochrony Danych Osobowych wydał **419 decyzji o odmowie rejestracji zbioru danych**, przede wszystkim ze względu na brak wyczerpującego opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy (część E zgłoszenia). W wielu przypadkach deklarowany przez administratorów danych poziom bezpieczeństwa przetwarzania danych w systemie informatycznym nie spełniał też warunków określonych w rozporządzeniu wykonawczym do ustawy (część F zgłoszenia). Bardzo często wyjaśnienia wymagała podstawa prawna prowadzenia zbioru (nawet wśród podmiotów publicznych), cel zbierania danych lub ich udostępniania. Zdarzały się przypadki, że zgłoszenia pochodziły od podmiotów niebędących – w świetle ustawy o ochronie danych osobowych – administratorami danych.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych w **77** sprawach podjął **decyzję o umorzeniu postępowania**, zaś w **285** wydał **decyzję o wykreśleniu** zbioru danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych. We wszystkich decyzjach przesłanką wykreślenia było zaprzestanie przetwarzania danych w zarejestrowanym zbiorze.

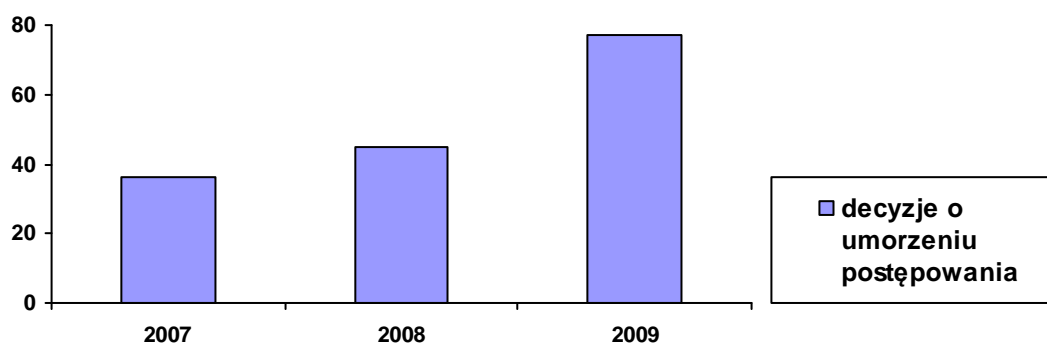
¹¹⁰ Przesłanki odmowy rejestracji zbioru danych określone zostały w art. 44 ust.1 ustawy.



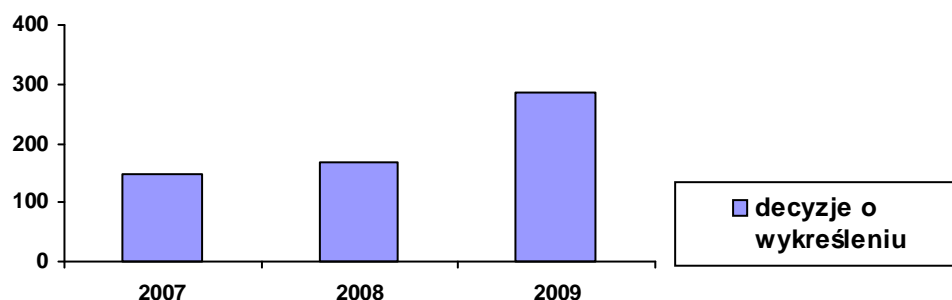
Wykres 17: Liczbowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych, wydanych przez GODO w 2009 r.



Wykres 18: Zestawienie porównawcze decyzji o odmowie rejestracji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.



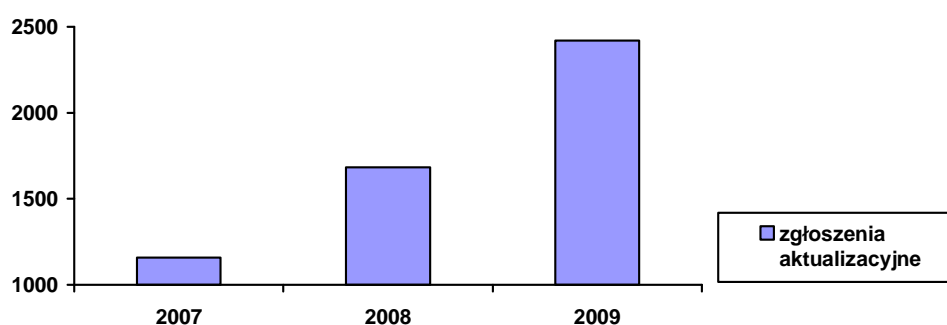
Wykres 19: Zestawienie porównawcze decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.



Wykres 20: Zestawienie porównawcze decyzji o wykreśleniu zbioru danych z rejestru wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007–2009.

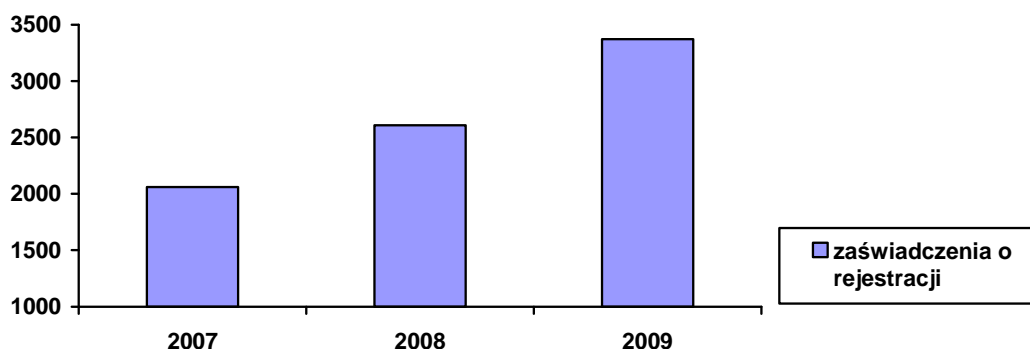
Prowadzony przez Generalnego Inspektora Ochrony Danych Osobowych ogólnokrajowy jawny rejestr zbiorów danych osobowych umożliwia obywatelom dostęp do informacji o administratorach danych i zgłoszonych przez nich zbiorach danych osobowych. Zasada jawności rejestru zbiorów danych osobowych realizowana jest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

W roku sprawozdawczym 2009, GODO rozpatrzył **2419 zgłoszeń aktualizacyjnych** dokonanych 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. W szczególności chodziło o przypadki zmiany systemu przetwarzania danych w zbiorze, tj. przejście z systemu tradycyjnego na informatyczny.



Wykres 21: Liczbowe zestawienie zgłoszeń aktualizacyjnych rozpatrzonych przez GODO w latach 2007-2009.

W omawianym okresie Generalny Inspektor Ochrony Danych Osobowych wydał ponadto z urzędu bądź na żądanie administratora danych **3374 zaświadczenia o zarejestrowaniu zbioru**.

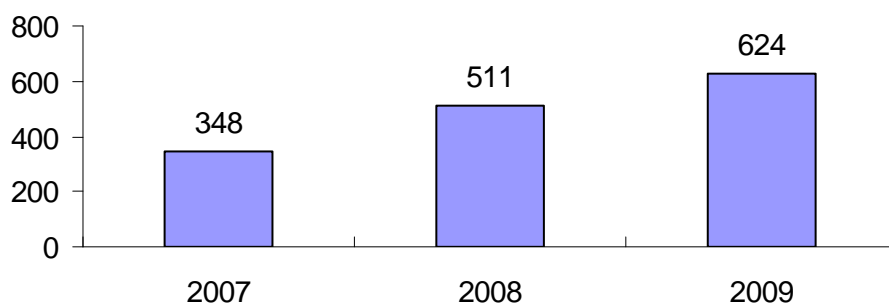


Wykres 22: Zestawienie porównawcze liczby zaświadczeń o zarejestrowaniu zbioru danych osobowych wydanych przez GODO w latach 2007-2009.

5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych

Stosownie do treści art. 12 pkt 4 ustawy o ochronie danych osobowych, do podstawowych zadań Generalnego Inspektora Ochrony Danych Osobowych należy opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych.

W analizowanym okresie sprawozdawczym do Biura Generalnego Inspektora wpłynęły do zaopiniowania **624 projekty aktów prawnych**, a zatem o 113 więcej niż w roku poprzednim.



Wykres 23: Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

W okresie objętym sprawozdaniem, w odniesieniu do wielu analizowanych aktów prawnych Generalny Inspektor wyraził jednoznacznie negatywną opinię. Tak też było w stosunku do projektu *ustawy o zmianie ustawy o dostępie do informacji publicznej*¹¹¹ przewidującego uznanie za publiczną informacji o stanie zdrowia osób sprawujących urząd Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów. Generalny Inspektor, wypowiadając się w tej kwestii podkreślił, że zaproponowane w treści projektu rozwiązania naruszają konstytucyjne prawo do ochrony danych osobowych

i prywatności wymienionych osób. Powołał odpowiednie przepisy polskiej ustawy zasadniczej, wskazując, że przemawiają one za zachowaniem przez ustawodawcę daleko idącej wstrzeźliwości w kwestii uchwalania przepisów skutkujących upublicznieniem danych o stanie zdrowia, nawet gdyby miało to dotyczyć osób piastujących w Rzeczypospolitej Polskiej najwyższe funkcje publiczne. Ponadto organ do spraw ochrony danych osobowych zaznaczył, iż biorąc pod uwagę okoliczność, że dane o stanie zdrowia dotyczą sfery prywatności, a niekiedy wręcz intymności osoby fizycznej, bezsporne jest, iż akt prawny nakazujący podanie do publicznej wiadomości tego typu informacji stanowi daleko idącą ingerencję w wyżej wymienione prawa. Zachodzi zatem potrzeba skontrolowania, czy spełnione zostały przesłanki dopuszczalności wkroczenia w sferę konstytucyjnych praw i wolności obywateli określone w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.¹¹² Generalny Inspektor zaznaczył, iż choć zakres prawa do prywatności i prawa do ochrony danych osobowych osób sprawujących funkcje publiczne jest zdecydowanie węższy niż „zwykłych obywateli”, to brak jest podstaw do przyjęcia, że prawa te nie znajdują wobec tych osób zastosowania.¹¹³

Dokonując analizy ww. projektu z punktu widzenia zasad zawartych w art. 31 ust. 3 Konstytucji RP, Generalny Inspektor zauważył, iż zaproponowane regulacje naruszają zasadę proporcjonalności stosowaną w przypadku tzw. kolizji praw konstytucyjnych i nie spełniają wymogu „konieczności w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób”. Podniósł również, iż przewidziane w art. 61 ustawy zasadniczej tzw. prawo do informacji zostało ukształtowane jako prawo obywatela do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Wątpliwe jest zatem, czy w zakresie tego prawa w ogóle mieści się uprawnienie do uzyskiwania informacji o stanie zdrowia osób sprawujących funkcje publiczne. Zarówno bowiem z punktu widzenia prawa europejskiego,¹¹⁴ jak i ustawodawstwa polskiego,¹¹⁵ dane o stanie zdrowia podlegają szczególnej ochronie. Generalny Inspektor wskazał także, iż nawet gdyby przyjąć wykładnię, że informacja o stanie zdrowia osób sprawujących funkcje publiczne w zakresie, w jakim ten stan zdrowia wpływa na wykonywanie przez te osoby ich funkcji, jest objęta prawem do informacji w rozumieniu art. 61 Konstytucji Rzeczypospolitej Polskiej, to przyjęte w projekcie ustawy o zmianie ustawy o dostępie do informacji publicznej rozwiązania, zakładające absolutny

¹¹¹ DOLiS-070-1/09.

¹¹² Zgodnie z art. 31 ust. 3 ustawy zasadniczej, 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.

¹¹³ Stanowisko znalazło swoje odbicie także w *Deklaracji w sprawie swobody debaty politycznej w mediach* Komitetu Ministrów Rady Europy z dnia 12 lutego 2004 r.

¹¹⁴ Np. art. 8 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.

¹¹⁵ Art. 27 ustawy o ochronie danych osobowych.

prymat prawa do informacji nad prawem do ochrony danych osobowych i prywatności osób sprawujących urząd Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów,¹¹⁶ są nie do pogodzenia z zasadą proporcjonalności, o której była mowa wyżej. Powołał przy tym jeden z wyroków Trybunału Konstytucyjnego¹¹⁷, podkreślając, iż autorzy projektu nie wskazali w uzasadnieniu powodów, dla których widzą potrzebę tak istotnego wkroczenia w sferę prywatności Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów, jakim jest upublicznienie informacji o ich stanie zdrowia, w tym wyników badań lekarskich. Generalny Inspektor zaznaczył, iż w jego opinii konieczność taka nie zachodzi, gdyż dla potwierdzenia zdolności psychicznej i fizycznej do sprawowania urzędu wystarczające byłoby podanie do publicznej wiadomości treści – wydanego na podstawie szczególnych przepisów prawa¹¹⁸ – zaświadczenia lekarskiego. Przedmiotowy projekt nie tylko zaś w sposób nieuzasadniony narusza prawo do ochrony danych osobowych i prywatności osób wymienionych w art. 1 ust. 1a ustawy o dostępie do informacji publicznej,¹¹⁹ lecz może także godzić w prawa – niesprawujących żadnych funkcji publicznych – ich najbliższych. Przewidziany w art. 6a ustawy o dostępie do informacji publicznej¹²⁰ obowiązek publikacji wyników badań nie zawiera bowiem jakichkolwiek ograniczeń, a zatem publicznemu udostępnieniu mogłyby podlegać także wyniki badań o charakterze intymnym.

Wśród projektów aktów prawnych, które wpłynęły w 2009 r. do zaopiniowania przez GODO, znalazł się projekt *rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2010*.¹²¹ Zastrzeżenia GODO wzbudziły zwłaszcza unormowania w badaniu o symbolu 1.21.12(034) „Narodowy spis powszechny ludności i mieszkań 2011 r. – opracowanie wyników spisu próbnego.” Uwzględniając fakt, że informacja o istnieniu (nieistnieniu) niepełnosprawności i jej stopniu stanowi daną o stanie zdrowia podlegającą szczególnej ochronie, w myśl art. 27 ust. 2 pkt 2¹²² ustawy o ochronie danych osobowych, tylko przepis rangi ustawowej

¹¹⁶ Wyłączenie ograniczenia prawa do informacji publicznej ze względu na prywatność osoby fizycznej – art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej – Dz. U. Nr 112, poz. 1198 z późn. zm., w brzmieniu nadanym przez art. 1 pkt 2 projektu ustawy; publikowanie danych o stanie zdrowia w sieci Internet, gdzie będą powszechnie dostępne przez nieograniczony czas, nie zaś jedynie przez okres sprawowania funkcji – art. 7 ust. 1a ustawy o dostępie do informacji publicznej, dodany przez art. 1 pkt 4 projektu.

¹¹⁷ W wyroku z 12 grudnia 2005 roku (sygn. K. 32/2004) Trybunał stwierdził, iż „konieczność w demokratycznym państwie prawnym to zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić określone wartości w sposób lub stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawo lub wolność ograniczają”.

¹¹⁸ Art. 229 § 8 pkt 2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (t.j. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) oraz rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 roku w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy (Dz. U. Nr 69, poz. 332 z późn. zm.).

¹¹⁹ Dodany przez art. 1 pkt 1 opiniowanego projektu.

¹²⁰ Dodany przez art. 1 pkt 3 projektu.

¹²¹ Projekt rozporządzenia wydany na podstawie delegacji zawartej w art. 18 ustawy z dnia 29 czerwca 1995 roku o statystyce publicznej – Dz. U. Nr 88, poz. 439 z późn. zm.

¹²² Art. 27 ust. 2 pkt 2 ustawy stanowi, iż przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

może ustanawiać kompetencję organu do przetwarzania takiej danej. Tymczasem przedstawiony do zaopiniowania projekt rozporządzenia nakłada na: Kasę Rolniczego Ubezpieczenia Społecznego, Narodowy Fundusz Zdrowia, Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych, powiatowe zespoły do spraw orzekania o niepełnosprawności, starostwa powiatowe i urzędy gmin, obowiązek przekazania Głównemu Urzędowi Statystycznemu danych osób niepełnosprawnych, w tym także informacji o stopniu niepełnosprawności tych osób. Rozwiązanie przyjęte w projekcie rozporządzenia jednoznacznie narusza zatem dyspozycję art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych. Co więcej – pozyskiwanie przez Główny Urząd Statystyczny, na zasadzie obowiązku, informacji o istnieniu (nieistnieniu) niepełnosprawności i jej stopniu, w ogóle nie znajduje uzasadnienia, zwłaszcza w kontekście przepisów rozporządzenia nr 763/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie spisów powszechnych ludności i mieszkań, który to akt prawa wspólnotowego nie nakłada obowiązku przekazywania Eurostatowi informacji o niepełnosprawności mieszkańców Państw Członkowskich, obliuguje zaś te Państwa do podjęcia wszelkich środków w celu spełnienia wymogów dotyczących ochrony danych (art. 4 ust. 2 rozporządzenia). Ponadto biorąc pod uwagę, że art. 27 ust. 1 ustawy o ochronie danych osobowych uznaje za dane podlegające szczególnej ochronie m.in. dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, zaś umieszczenie osoby w zakładzie karnym lub areszcie śledczym następuje na podstawie orzeczenia sądu (prawomocnego lub wykonalnego), sam fakt przebywania określonej osoby w zakładzie karnym (areszcie śledczym) jest daną sensytywną, gdyż bezpośrednio ujawnia zapadłe wobec tej osoby orzeczenie sądowe. W tym stanie rzeczy, stosownie do ww. art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, tylko przepis rangi ustawowej może ustanawiać kompetencję organu do przetwarzania takiej danej. Wobec powyższego Generalny Inspektor zakwestionował nałożenie w projekcie opiniowanego rozporządzenia na Ministra Sprawiedliwości obowiązku przekazania Głównemu Urzędowi Statystycznemu danych identyfikujących osoby pozbawione wolności oraz osoby przebywające w zakładach poprawczych.

Organ do spraw ochrony danych osobowych zwrócił uwagę, iż informacja o narodowości ujawnia pochodzenie etniczne, a niekiedy także rasowe człowieka. W opinii Generalnego Inspektora Ochrony Danych Osobowych, przesądza to o uznaniu przetwarzania danych o narodowości za przetwarzanie danych szczególnie chronionych w rozumieniu art. 27 ustawy o ochronie danych osobowych. Co za tym idzie – w świetle dyspozycji art. 27 ust. 2 pkt 2 tejże ustawy - nieprawidłowe jest zamieszczanie w akcie prawnym o randze niższej niż ustawa przepisów nakazujących przetwarzanie informacji o narodowości. Dlatego też organ do spraw ochrony danych osobowych wystąpił przeciwko zawartym w opiniowanym projekcie unormowaniom obligującym Urząd do Spraw Cudzoziemców i urzędy gmin do przekazywania Głównemu Urzędowi Statystycznemu informacji o narodowości cudzoziemców. Ponadto Generalny Inspektor wskazał, iż art. 35 ust. 1 pkt 4 ustawy

o statystyce publicznej upoważnił służby statystyki publicznej do zbierania dla celów statystycznych jedynie informacji o obywatelstwie osób fizycznych zamieszkujących na terytorium Rzeczypospolitej Polskiej.

Odnosząc się nadal do przedmiotowego projektu rozporządzenia, Generalny Inspektor zwrócił uwagę, iż jego akceptacji nie może zyskać przewidziana w projekcie rozporządzenia (pkt 8. „Źródła danych”) propozycja pozyskiwania na potrzeby powszechnego spisu rolnego w 2010 r. danych z systemów informacyjnych Zakładu Ubezpieczeń Społecznych w sytuacji, gdy projekt ustawy o powszechnym spisie rolnym w 2010 r. (wersja z dnia 05.05.2009 r.) w ogóle nie przewiduje zbierania danych z tego źródła (badanie o symbolu 1.45.29(142) „Powszechny Spis Rolny i badanie metod produkcji rolnej”).

Kolejnym projektem, który podlegał opiniowaniu przez Generalnego Inspektora Ochrony Danych Osobowych w analizowanym okresie sprawozdawczym, był projekt *ustawy o narodowym spisie powszechnym ludności i mieszkań w 2011 r.*¹²³ W wystosowanej opinii do tego projektu¹²⁴ organ do spraw ochrony danych osobowych uznał, iż zaproponowane w nim rozwiązania pozostają w oczywistej sprzeczności z wcześniej dokonanymi uzgodnieniami, a co za tym idzie – nie mogą zyskać jego akceptacji.

Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę, że art. 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej zakazuje władzom publicznym pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Zastrzeżenia GODO wzbudziła już sama koncepcja utworzenia przez Główny Urząd Statystyczny [GUS] na potrzeby narodowego spisu powszechnego ludności i mieszkań w 2011 r. megabazy danych osób przebywających na terytorium Rzeczypospolitej Polskiej. Wbrew bowiem stanowisku prezentowanemu przez Główny Urząd Statystyczny, przyjęcie w pełnym zakresie unormowań projektu tej ustawy nakazujących określonym podmiotom: ministrowi właściwemu do spraw finansów publicznych, ministrowi właściwemu do spraw wewnętrznych, Ministrowi Sprawiedliwości, Szefowi Urzędu do Spraw Cudzoziemców, Prezesowi Zakładu Ubezpieczeń Społecznych, Prezesowi Kasy Rolniczego Ubezpieczenia Społecznego, Prezesowi Narodowego Funduszu Zdrowia, Głównemu Geodecie Kraju, Prezesowi Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych, marszałkom województw, starostom, wójtom, burmistrzom, prezydentom miast, zarządcom zasobów mieszkaniowych, przedsiębiorcom prowadzącym działalność gospodarczą w zakresie sprzedaży energii elektrycznej oraz dostawcom publicznie dostępnych usług telekomunikacyjnych¹²⁵ - przekazanie Prezesowi Głównego Urzędu Statystycznego prowadzonych przez te podmioty całych baz danych (art. 5 ust. 1 pkt 1

¹²³ Wersja z 06.04.2009 r.

¹²⁴ DOLiS-033-207/08.

¹²⁵ Załącznik nr 1 do projektu.

projektu), skutkowałoby powstaniem w Głównym Urzędzie Statystycznym zbioru danych nieporównywalnego pod względem obszerności i szczegółowości z jakimkolwiek innym istniejącym w chwili obecnej w Rzeczypospolitej Polskiej. Organ do spraw ochrony danych osobowych, jako podmiot stojący na straży przestrzegania przez administratorów danych wymogu legalności przetwarzania danych i ich adekwatności do celów przetwarzania,¹²⁶ konsekwentnie występuje przeciwko projektom tworzenia megabaz danych.

Generalny Inspektor zauważył, że chociaż dane pozyskane w ramach narodowego spisu powszechnego ludności i mieszkań w 2011 r. chronione będą tajemnicą statystyczną (art. 10 ustawy z dnia 29 czerwca 1995 roku o statystyce publicznej – Dz. U. Nr 88, poz. 439 z późn. zm. w zw. z art. 10 ust. 1 projektu ustawy), nie wyłącza to jednak możliwości bezprawnego wejścia w ich posiadanie. Zwłaszcza że planowany czas pozostawiania tych danych w postaci niezanonimizowanej ma być długi – od spisu próbnego w kwietniu i maju 2010 roku (art. 13 ust. 1 i ust. 2 pkt 1 projektu ustawy) do upływu dwóch lat od dnia zakończenia spisu, czyli do 30 czerwca 2013 roku (art. 10 ust. 2 w zw. z art. 1 ust. 2 projektu ustawy). Co więcej – mimo iż obowiązujące unormowania ustawy o statystyce publicznej (art. 10) wyłączają możliwość wykorzystywania danych osobowych zebranych podczas spisu powszechnego dla celów innych niż statystyczne, zdaniem Generalnego Inspektora Ochrony Danych Osobowych nie można wykluczyć takiej ewentualności wskutek zmiany przepisów w przyszłości. Ponadto Generalny Inspektor Ochrony Danych Osobowych zakwestionował propozycję przekazywania Głównemu Urzędowi Statystycznemu na potrzeby narodowego spisu powszechnego ludności i mieszkań w 2011 r. danych zgromadzonych w systemach informacyjnych w tak szerokim zakresie, jak przewiduje to załącznik nr 1 do projektu ustawy. Organ do spraw ochrony danych osobowych powołał się na zasadę adekwatności, uregulowaną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. W ocenie organu zakres danych pozyskiwanych z systemów informacyjnych wskazanych w załączniku nr 1 do tego projektu jest znacznie szerszy, aniżeli tematyka spisu określona w załączniku nr 2 do projektu oraz w załączniku do rozporządzenia nr 763/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie spisów powszechnych ludności i mieszkań, które to dokumenty – zgodnie z art. 6 ust. 1 i 2 projektu ustawy – miały wyznaczać granice zbierania danych w ramach narodowego spisu powszechnego ludności i mieszkań w 2011 r. Co więcej, przyjęta w załączniku nr 1 do projektu ustawy koncepcja przekazywania danych z systemów informacyjnych wielu podmiotów prowadzić będzie do kilkukrotnego pozyskiwania przez Główny Urząd Statystyczny w istocie tych samych danych.

Od początku prac nad projektem *ustawy o narodowym spisie powszechnym ludności i mieszkań w 2011 r.* Generalny Inspektor podtrzymał prezentowane stanowisko w kwestii

¹²⁶ Art. 12 pkt 1 w zw. z art. 26 ust. 1 pkt 1 i 3 ustawy o ochronie danych osobowych.

niedopuszczalności zbierania w ramach spisu na zasadzie obowiązku danych o istnieniu (nieistnieniu) niepełnosprawności i jej stopniu, czyli danych o stanie zdrowia podlegających szczególnej ochronie na podstawie art. 27 ustawy o ochronie danych osobowych. Jednocześnie zwrócił uwagę na wewnętrzną sprzeczność aktualnej wersji projektu ustawy w kwestii zbierania danych o istnieniu (nieistnieniu) niepełnosprawności i jej stopniu. Z jednej strony bowiem – art. 6 ust. 3 pkt 2 projektu proklamujący dobrowolność zbierania danych dotyczących posiadania orzeczenia o niepełnosprawności oraz jej stopniu i rodzaju, z drugiej zaś – ust. 6 pkt 1 lit. k; ust. 7 pkt 15 lit. b; ust. 9 pkt 1 lit. i oraz pkt 2 lit. d; ust. 11 pkt 3, pkt 4 lit. a tiret dwadzieścia jeden i dwadzieścia dwa oraz lit. b tiret osiemnaście i dziewiętnaście; ust. 12 pkt 3 lit. z, za i zb, i lit. zd tiret czternaście, piętnaście i szesnaście oraz pkt 4 lit. b tiret dwa załącznika nr 1 do projektu ustawy nakazujące odpowiednio: Prezesowi Kasy Rolniczego Ubezpieczenia Społecznego, Prezesowi Narodowego Funduszu Zdrowia, Prezesowi Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych, starostom; wójtom, burmistrzom, prezydentom miast przekazywanie takich danych Prezesowi Głównego Urzędu Statystycznego pod rygorem odpowiedzialności za wykroczenie z art. 23 pkt 1 projektu ustawy. W istocie zatem dobrowolność respondentów w zakresie podawania danych o niepełnosprawności i jej stopniu ma w projekcie ustawy charakter zupełnie fikcyjny, gdyż organy spisowe i tak posiadać będą informacje w tej kwestii z systemów informacyjnych, o których mowa była wyżej. Organ do spraw ochrony danych osobowych zaakceptował przewidziane w ust. 1 pkt 1 lit. p załącznika nr 1 do projektu ustawy unormowanie dotyczące przekazywania przez ministra właściwego do spraw finansów publicznych Prezesowi Głównego Urzędu Statystycznego z systemu informacyjnego prowadzonego przez organy podatkowe informacji o kosztach uzyskania przychodów i źródłach przychodów osób fizycznych.

W trakcie opiniowania projektu *ustawy o udostępnianiu informacji gospodarczych*,¹²⁷ zastrzeżenia Generalnego Inspektora wzbudziły zawarte w tym projekcie zapisy dotyczące gromadzenia przez biura informacji gospodarczej informacji o numerze PESEL¹²⁸ oraz o adresie zamieszkania osoby fizycznej prowadzącej działalność gospodarczą, o ile nie jest on tożsamy z miejscem wykonywania tej działalności.¹²⁹ Organ do spraw ochrony danych osobowych wskazał, że zakres przekazywanych do biur informacji gospodarczej,¹³⁰ a w konsekwencji ujawnianych¹³¹ informacji o osobach fizycznych prowadzących działalność gospodarczą, powinien być ściśle związany z prowadzoną przez te osoby działalnością. W ocenie Generalnego Inspektora Ochrony Danych Osobowych nie znajduje uzasadnienia przetwarzanie danych o numerze PESEL i adresie zamieszkania (o ile nie jest on taki sam jak miejsce wykonywania działalności gospodarczej) osoby fizycznej

¹²⁷ DOLiS-033-168/09

¹²⁸ Art. 2 ust. 1 pkt 3 lit. b *in principio* projektu.

¹²⁹ Art. 2 ust. 1 pkt 3 lit. e *in principio*.

¹³⁰ Art. 10 ust. 2 pkt 2.

¹³¹ Art. 1 ust. 1 pkt 1 i art. 17 ust. 2.

prowadzącej działalność gospodarczą, w związku z zaciągniętymi przez tę osobę zobowiązaniami z tytułu prowadzonej działalności. Nie można bowiem pominąć, iż ustawa o ochronie danych osobowych wymaga, aby dane osobowe były przetwarzane (w tym ujawniane) wyłącznie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu, jakiemu przetwarzanie (ujawnianie) danych ma służyć (art. 26 ust. 1 pkt 3). Wobec powyższego Generalny Inspektor zwrócił uwagę, iż dla identyfikacji osoby fizycznej prowadzącej działalność gospodarczą i powiązania jej z istniejącym zobowiązaniem z tytułu tej działalności, informacje o numerze PESEL i adresie zamieszkania (o ile nie jest on tożsamy z miejscem wykonywania działalności) są zbędne, tak więc ich gromadzenie przez biura informacji gospodarczej naruszać będzie – wskazaną wyżej – zasadę adekwatności.

W odniesieniu do projektu *ustawy o racjonalizacji zatrudnienia w państwowych jednostkach budżetowych i niektórych innych jednostkach sektora finansów publicznych*,¹³² Generalny Inspektor Ochrony Danych Osobowych wyraził obawy, iż zawarta w jego treści propozycja objęcia przepisami niniejszego projektu Generalnego Inspektora Ochrony Danych Osobowych, godzi w niezależność organu do spraw ochrony danych osobowych i tym samym pozostaje w sprzeczności z europejskimi standardami ochrony tych danych.

Generalny Inspektor wskazał, iż konieczność zapewnienia organowi do spraw ochrony danych osobowych całkowitej niezależności wynika wprost z wiążących Rzeczpospolitą Polską norm prawa europejskiego – w szczególności pkt 62 preambuły i art. 28 ust. 1 Dyrektywy nr 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. Zgodnie bowiem z pkt. 62 preambuły, cyt.: „(...) utworzenie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny jest zasadniczym elementem ochrony jednostek w zakresie przetwarzania danych osobowych (...)”. W myśl zaś art. 28 ust. 1 dyrektywy 95/46/WE, każde państwo członkowskie zapewnia, że jeden lub kilka organów publicznych będzie odpowiedzialnych za kontrolę stosowania na jego terytorium postanowień przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy. Organy te będą postępować w sposób całkowicie niezależny wykonując powierzone im funkcje. Podobnie do niezależności organu do spraw ochrony danych osobowych w sposób bezpośredni odnosi się Karta Praw Podstawowych Unii Europejskiej. Oto bowiem jej art. 8, stanowiąc, że każdy ma prawo do ochrony danych osobowych, które go dotyczą, a które muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej podstawie prawnej przewidzianej ustawą, jak i przewidując prawo dostępu osoby do dotyczących jej danych i prawo ich sprostowania, podkreśla, że przestrzeganie tych zasad podlega kontroli niezależnego organu.

¹³² DOLiS-033-280/09.

Ponadto Generalny Inspektor wskazał, iż także ustawodawca polski, implementując do krajowego porządku prawnego normy prawa europejskiego, respektował niezawisłość Generalnego Inspektora Ochrony Danych Osobowych, przyjmując, że w zakresie wykonywania swoich zadań podlega on jedynie ustawie (art. 8 ust. 4 ustawy o ochronie danych osobowych).

Generalny Inspektor wskazał, iż przedłożony projekt ustawy może pozbawić organ do spraw ochrony danych osobowych istotnego atrybutu niezależności – gwarantowanego mu tak przez wskazaną dyrektywę nr 95/46/WE, Kartę Praw Podstawowych, jak i ustawę o ochronie danych osobowych – poprzez odebranie mu możliwości kształtowania zatrudnienia na poziomie odpowiednim do rzeczywistych potrzeb związanych z ilością wykonywanych obowiązków oraz poddanie organu do spraw ochrony danych osobowych kontroli Prezesa Rady Ministrów (np. art. 10 ust. 1,¹³³ art. 13 ust. 1,¹³⁴ i art. 15¹³⁵ projektu). Nie można zaś pominąć, iż do zadań organu do spraw ochrony danych osobowych należy m.in. kontrola zgodności przetwarzania danych przez organy państwowe, w tym również Prezesa Rady Ministrów (art. 12 pkt 1 w zw. z art. 3 ust. 1 ustawy o ochronie danych osobowych¹³⁶). Dlatego mając na uwadze powyższe, konieczność wyłączenia organu do spraw ochrony danych osobowych spod obowiązywania aktu prawnego o charakterze takim, jak ustawa o racjonalizacji zatrudnienia w państwowych jednostkach budżetowych i niektórych innych jednostkach sektora finansów publicznych, nie powinna budzić wątpliwości. Bowiem, jak wskazał Generalny Inspektor, w projekcie zamieszczony został przepis stanowiący podstawę do ewentualnego wydania przez Prezesa Rady Ministrów rozporządzenia określającego jednostki zwolnione z obowiązku racjonalizacji zatrudnienia (art. 17 ust. 3 pkt 1¹³⁷), chociaż delegacja ta – w zaproponowanym kształcie – ma charakter fakultatywny. Oznacza to, iż stosownej treści rozporządzenie (które – pomijając kwestie niezależności – mogłoby ewentualnie uwzględniać Generalnego Inspektora Ochrony Danych Osobowych), w ogóle nie musi zostać wydane. Ponadto Generalny Inspektor zauważył, że zadania które wykonuje, tak w zakresie ich wagi, jak i ilości,

¹³³ Art. 10 ust. 1. Kierownik jednostki, w terminie do dnia 1 lutego 2010 r. przedstawi Prezesowi Rady Ministrów informacje o stanie zatrudnienia w tej jednostce, według stanu na dzień 30 czerwca 2009 r., zwane dalej „raportem początkowym”.

¹³⁴ Art. 13 ust. 1. Kierownik jednostki, w terminie do dnia 15 lipca 2010 r., przedstawi Prezesowi Rady Ministrów informację o przeprowadzonej racjonalizacji zatrudnienia w tej jednostce, zwaną dalej „raportem z realizacji”. Przepisy art. 10 ust. 2 i 4 stosuje się odpowiednio.

¹³⁵ Art. 15. Kierownik jednostki, w terminie do dnia 15 stycznia 2012 r., przedstawi Prezesowi Rady Ministrów informację o wynikach racjonalizacji zatrudnienia według stanu zatrudnienia pracowników na dzień 31 grudnia 2011 r. w podziale na rodzaj stanowisk, według wykonywanych zadań, zwaną dalej „raportem końcowym”. Przepisy art. 10 ust. 2 i 4 stosuje się odpowiednio.

¹³⁶ Zgodnie z treścią art. 12 pkt 1 ustawy o ochronie danych osobowych, do zadań Generalnego Inspektora w szczególności należy: 1) kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zgodnie zaś z treścią art. 3 ust. 1, ustawę o ochronie danych osobowych stosuje się do organów państwowych, organów samorządu terytorialnego oraz do państwowych jednostek organizacyjnych.

¹³⁷ Zgodnie z treścią tego przepisu, Prezes Rady Ministrów może określić, w drodze rozporządzeń jednostki zwolnione z obowiązku utrzymania zatrudnienia na poziomie, o którym mowa w art. 3 ust. 1 – mając na względzie konieczność zapewnienia bezpieczeństwa państwa, porządku publicznego, ochrony zdrowia lub środowiska bądź szczególne znaczenia wykonywanych przez jednostkę zadań dla funkcjonowania państwa, a także efektywność wykonywanych zadań.

zdecydowanie wypełniałyby wytyczną zawartą w art. 17 ust. 3 projektu. Zgodnie z jej treścią, Prezes Rady Ministrów, wydając rozporządzenie, ma bowiem uwzględnić, cyt.: „(...) szczególne znaczenie wykonywanych przez jednostkę zadań dla funkcjonowania państwa, a także efektywność wykonywanych zadań (...)”.

Odnosząc się natomiast do konkretnych rozwiązań projektu, Generalny Inspektor Ochrony Danych Osobowych zaproponował, aby w art. 3 projektu ustawy,¹³⁸ zamiast przepisu odnoszącego się do stanu zatrudnienia na dzień 30 czerwca 2009 r. jako podstawy, od której następuje racjonalizacja zatrudnienia (art. 3), wprowadzić przepis, w którym podstawą racjonalizacji zatrudnienia jest planowana w budżecie liczba etatów na rok 2009, bądź też zatrudnienie średnioroczne w jednostce za okres pierwszych 6 miesięcy 2009 r. Wskazał także, iż proponowana data zdaje się być datą przypadkową, nieoddającą faktycznego stanu zatrudnienia w jednostce organizacyjnej. Liczba etatów wykorzystywanych w ciągu roku jest zmienna i związana z „ruchem kadrowym” i polityką kadrową instytucji. Dla przykładu bowiem, w Biurze Generalnego Inspektora Ochrony Danych Osobowych stan etatów na 30 czerwca 2009 r. jest w istocie wynikiem przypadku, nie zaś wielkością oddającą właściwe zapotrzebowanie na obsadę kadrową. Przeprowadzenie w Biurze racjonalizacji w oparciu o tę datę doprowadziłoby do zmniejszenia zatrudnienia o 20 %, co właściwie uniemożliwiłoby wykonywanie ustawowych zadań Generalnego Inspektora.

Opiniując z kolei projekt *założeń projektu ustawy o systemie informacji oświatowej*,¹³⁹ organ do spraw ochrony danych osobowych stanowczo sprzeciwił się planowanej mocą ww. projektu zmianie zasad funkcjonowania systemu informacji oświatowej [SIO] w zakresie przetwarzania danych osobowych o uczniach i nauczycielach (część I 3.1. projektu zatytułowana „Zmiana zasad działania SIO”). Generalny Inspektor zwrócił uwagę, że nie można zgodzić się z zasadnością rozwiązania, zgodnie z którym, cyt.: „(...) Nowy SIO będzie obejmował centralną bazę danych, zawierającą dane gromadzone już w systemie oświaty (...)”, z uwagi m.in. na okoliczność, iż, cyt.: „(...) Takie rozwiązanie nie tylko uporządkuje obszar gromadzenia w systemie oświaty danych o uczniach i nauczycielach, ale przede wszystkim spowoduje efektywne wykorzystywanie tych danych do celów wykonywania określonych zadań oświatowych, w tym w sferze finansowej i administracyjnej,

¹³⁸ Zgodnie z treścią tego przepisu, racjonalizacja zatrudnienia polega na zmniejszeniu zatrudnienia w jednostkach co najmniej o 10% pracowników zatrudnionych w ramach stosunku pracy, zwanych dalej „pracownikami”, w przeliczeniu na pełne etaty, w odniesieniu do stanu zatrudnienia tych pracowników na dzień 30 czerwca 2009 r. Ust. 2. Racjonalizacja zatrudnienia może nastąpić w szczególności przez: 1) niezawarcie z pracownikiem kolejnej umowy o pracę, w przypadku umowy zawartej na okres próbny, umowy zawartej na czas określony i umowy zawartej na czas wykonania określonej pracy; 2) rozwiązanie z pracownikiem stosunku pracy; 3) obniżenie wymiaru czasu pracy pracownika z jednoczesnym proporcjonalnym zmniejszeniem wynagrodzenia za pracę. Ust. 3. Do stanu zatrudnienia, o którym mowa w ust. 1, nie wlicza się pracowników objętych szczególną ochroną przed wypowiedzeniem lub rozwiązaniem stosunku pracy wynikającą z art. 39 oraz przepisów działu ósmego ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94, z późn. zm.), pod warunkiem, że ochroną tą byli objęci w dniu 30 czerwca 2009 r. i są nią objęci w dniu wejścia w życie ustawy.

¹³⁹ DOLiS-033-414/09.

zarządzania oświatą na wszystkich poziomach oraz kreowania polityki oświatowej (...). Generalny Inspektor podkreślił, iż głównym celem funkcjonowania systemu informacji oświatowej jest dostarczanie „wiedzy statystycznej”, na co wskazuje chociażby uzasadnienie rządowego projektu ustawy o systemie informacji oświatowej.¹⁴⁰ Jako że powodem takich zmian nie może być – lakonicznie ujęta – chęć „zapewnienia efektywnego wykorzystywania tych danych do celów wykonywania określonych zadań oświatowych”, Generalny Inspektor Ochrony Danych Osobowych w wystąpieniu w tej sprawie wskazał, że nie ma podstaw do zmiany aktualnego stanu prawnego w zakresie systemu informacji oświatowej, który pozwala na uczynienie zadość zadaniom, jakie spoczywają na poszczególnych podmiotach zaangażowanych w proces edukacji, wynikających ze szczególnych przepisów prawa obowiązujących w tym sektorze. Generalny Inspektor nie zgodził się z wnioskiem, który wysnuć można z treści projektu założeń, jakoby bez stworzenia centralnej bazy danych o uczniach, i dostępu do jej zawartości „z jednego źródła” nie istniała możliwość organizowania i przeprowadzania egzaminów zewnętrznych oraz wydawanie świadectw i innych druków szkolnych. W chwili obecnej – pomimo braku takiej scentralizowanej megabazy danych, nie wydaje się, aby występowały problemy powyższej natury.

Wypowiadając się natomiast w kwestii zgodności z przepisami o ochronie danych osobowych ww. projektu, Generalny Inspektor wskazał, że nie można tym bardziej wprowadzać podstaw do istnienia bazy zawierającej olbrzymią liczbę informacji będących danymi osobowymi w rozumieniu art. 6 ustawy¹⁴¹ o ochronie danych osobowych, jako „recepty” na – przywoływane w projekcie założenia do projektu ustawy – niedoskonałości aktualnego Systemu Informacji Oświatowej przejawiające się m.in. w „wielokrotnym uwzględnianiu tych samych osób w różnych zestawieniach zbiorczych”.

Generalny Inspektor podniósł także, że nie do zaakceptowania z punktu widzenia zasad ochrony danych osobowych jest zamieszczanie w scentralizowanej megabazie danych również informacji szczególnie chronionych, o których stanowi art. 27 ust. 1 ustawy o ochronie danych osobowych, w tym m.in. danych dotyczących stanu zdrowia konkretnej osoby fizycznej czy orzeczeń wydanych wobec niej w postępowaniu sądowym lub administracyjnym. Tworzenie zintegrowanych megabaz danych zawierających wskazane informacje, niekiedy wręcz o charakterze intymnym, jest przedsięwzięciem budzącym wiele wątpliwości. Dostęp do tego rodzaju baz z założenia przysługuje olbrzymiej grupie podmiotów, co naraża zawarte w nich dane osobowe na ryzyko bezprawnej ingerencji (w tym w szczególności ryzyko ich ujawnienia). Dane takie posiadają także wysoką wartość rynkową, co dodatkowo zwiększa ryzyko ich bezprawnego wykorzystania.

¹⁴⁰ W jego treści czytamy, cyt.: „(...) System informacji oświatowej (SIO) w docelowym kształcie ma zastąpić dotychczasowy, podzielony system badań statystycznych oświaty. W szczególności ma zastąpić dane zbierane przy pomocy różnych sprawozdań statystycznych (...)”.

¹⁴¹ Zgodnie z treścią tego przepisu, w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Generalny Inspektor Ochrony Danych Osobowych wskazał również na konieczność głębokiego zastanowienia się nad niezbędną władania informacjami o konkretnych uczniach czy nauczycielach danej szkoły przez organ prowadzący inną placówkę tego typu. Zasadność niemalże automatycznego udostępniania tych danych w ramach systemu oświaty wspomnianym podmiotom – bez względu na faktyczną potrzebę władania tymi danymi – budzi poważne zastrzeżenia nie tylko pod kątem celowości tego typu działania, ale także adekwatności pozyskiwanych danych w stosunku do celów ich przetwarzania. Rozwiązania ww. projektu – jak wskazał Generalny Inspektor Ochrony Danych Osobowych – naruszają zasadę adekwatności danych i wskazał, że jak stanowi ugruntowane orzecznictwo sądów administracyjnych,¹⁴² administrator danych za każdym razem powinien pozyskiwać czy udostępniać jedynie tyle danych, ile jest niezbędne z punktu widzenia osiągnięcia zamierzonego celu.

W trakcie opiniowania *projektu ustawy o zmianie ustawy o cudzoziemcach oraz niektórych innych ustaw*,¹⁴³ Generalny Inspektor Ochrony Danych Osobowych wyraził obawy w kwestii niedookreślenia w jego treści okoliczności, w jakich dopuszczalne jest pobranie odcisków linii papilarnych. Z brzmienia art. 87a projektu wynika, iż funkcjonariusz Straży Granicznej, Policji lub Służby Celnej oraz pracownik Urzędu do Spraw Cudzoziemców lub urzędu wojewódzkiego w toku kontroli legalności pobytu może pobrać od cudzoziemca odciski linii papilarnych w celu weryfikacji tożsamości posiadacza wizy Schengen lub w celu stwierdzenia jej autentyczności. Z treści tego przepisu nie wynika jednakże, w jakich okolicznościach pobranie odcisków linii papilarnych jest dopuszczalne, co może implikować wniosek, że zawsze – w celu weryfikacji tożsamości posiadacza wizy Schengen lub w celu stwierdzenia jej autentyczności – będzie możliwość pobierania od cudzoziemca odcisków linii papilarnych.¹⁴⁴

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wskazał, iż w celu zapobieżenia nadmiernemu pobieraniu odcisków palców, a zatem wbrew zasadzie adekwatności danych w stosunku do celów ich przetwarzania,¹⁴⁵ należałoby doprecyzować powyższy przepis o sytuacji (np. budzące wątpliwość co do tożsamości cudzoziemca lub autentyczności jego wizy Schengen), w których żądanie udostępnienia linii papilarnych w celu uzyskania ich odcisków jest dopuszczalne. Generalny Inspektor, opiniując przedmiotowy projekt, wskazał także, iż w ust. 1 projektowanego art. 87a wprowadzono warunek, w jakim pozyskiwanie przedmiotowych informacji

¹⁴² Np. w glosie do wyroku Naczelnego Sądu Administracyjnego z 19 grudnia 2001 r. (II SA 2869/00) A. Drozd podniósł, iż zbieranie danych osobowych na zapas, co do zasady narusza zasadę adekwatności, ponieważ takie postępowanie nie mieści się w ramach celu przetwarzania.

¹⁴³ DOLiS-033-398/09.

¹⁴⁴ Zgodnie z brzmieniem art. 1 pkt 15 projektu, po art. 87 ustawy o cudzoziemcach dodaje się art. 87a, którego ustęp drugi otrzymuje brzmienie: funkcjonariusz Straży Granicznej, Policji lub Służby Celnej oraz pracownik Urzędu do Spraw Cudzoziemców lub urzędu wojewódzkiego w toku kontroli legalności pobytu może pobrać od cudzoziemca odciski linii papilarnych w celu weryfikacji tożsamości posiadacza wizy Schengen lub w celu stwierdzenia jej autentyczności.

¹⁴⁵ Co naruszałoby art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

o osobie fizycznej staje się możliwe.¹⁴⁶ Stąd też, co podkreślono w treści opinii skierowanej do Ministerstwa Spraw Wewnętrznych i Administracji w tej sprawie, prawidłowe rozwiązania w tej kwestii zastosowano w ust. 1, nie zastosowano natomiast w ust. 2 tego samego artykułu przedmiotowego projektu. Wskazano więc, iż rozważyć należałoby doprecyzowanie powyższego przepisu tak, aby wyeliminować wątpliwości interpretacyjne i ryzyko uznaniowości podmiotów wskazanych w analizowanym przepisie w kwestii pobierania od cudzoziemców odcisków linii papilarnych.

Opiniując z kolei projekt *rozporządzenia Ministra Zdrowia w sprawie tworzenia niepowtarzalnego oznakowania umożliwiającego identyfikację dawcy komórek, tkanek i narządów, sposobu oznaczania komórek, tkanek i narządów za pomocą tego oznakowania oraz wymagań w zakresie monitorowania komórek, tkanek i narządów*,¹⁴⁷ Generalny Inspektor wskazał na zapis, stosownie do treści którego do przetwarzania danych osobowych stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym w rozumieniu przepisów w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.¹⁴⁸

W pierwszej kolejności organ do spraw ochrony danych osobowych zaznaczył, iż właściwe byłoby odwołanie się w treści projektu do całej nazwy aktu prawnego¹⁴⁹ określającego wymagania odnośnie do zabezpieczeń danych. Adresaci normy nie mieliby wówczas wątpliwości co do tego, w jakim akcie prawnym znajdują się przepisy, które muszą w opisywanym przypadku być przez nich respektowane. Jednakże wysoki poziom bezpieczeństwa odnosi się wyłącznie do zabezpieczenia danych osobowych przetwarzanych w systemach informatycznych. Generalny Inspektor wskazał więc, iż trudno mówić o możliwości zastosowania przez administratora danych zabezpieczeń obejmujących m.in. kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną i kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych w sytuacji, gdy przetwarza on dane osobowe w tzw. postaci manualnej, poza systemem informatycznym. Brzmienie projektowanego przepisu implikuje wniosek, iż do wszelkich form przetwarzania danych osobowych przewidzianych w treści projektu należy stosować te środki. W związku z powyższym, Generalny Inspektor zasugerował autorom projektu stworzenie takiej regulacji, która odnosić będzie poziom wysoki zabezpieczeń do przetwarzania danych wyłącznie

¹⁴⁶ Wskazano bowiem, iż pobranie od cudzoziemca odcisków, linii papilarnych następuje, cyt.: „(...) jeżeli w toku kontroli legalności pobytu cudzoziemiec nie okaże dokumentu, na podstawie którego można ustalić jego tożsamość lub w przypadku, gdy zachodzi uzasadnione podejrzenie co do autentyczności dokumentu okazanego przez cudzoziemca (...)”.

¹⁴⁷ DOLiS-033-433/09.

¹⁴⁸ § 9 projektu.

w systemie informatycznym. Powyższe możliwe byłoby poprzez zastosowania w odpowiednim przepisie projektu sformułowania: „Do przetwarzania danych osobowych w formie elektronicznej stosuje się wysoki poziom bezpieczeństwa (...)”.

Analogiczną, jak powyżej wskazaną, uwagę Generalny Inspektor Ochrony Danych Osobowych odniósł do projektu *rozporządzenia w sprawie szczegółowych warunków wywozu ludzkich komórek, tkanek i narządów z terytorium Rzeczypospolitej Polskiej i przywozu tych komórek, tkanek i narządów na to terytorium oraz monitorowania stanu wywożonych i przywożonych ludzkich komórek, tkanek i narządów w drodze między dawcą a biorcą*.¹⁵⁰ Wskazał także, iż podważenia wymaga przewidziana w nim¹⁵¹ forma dokonywania zgłoszeń istotnych zdarzeń niepożądanych w czasie wywozu lub przywozu narządów. Zgodnie z projektem ma się to odbywać za pomocą listu poleconego. W opinii Generalnego Inspektora wzgląd na bezpieczeństwo danych osobowych przemawia raczej za unikaniem tej formy dostarczania korespondencji.¹⁵² Prawdopodobna jest bowiem jej utrata, a w konsekwencji - dostęp osób nieupoważnionych do danych osobowych zawartych w treści korespondencji – w tym przypadku także danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych.

Opiniując ww. projekt, Generalny Inspektor wyraził aprobatę w kwestii wprowadzenia do projektowanych przepisów bardziej restrykcyjnych, niż wynika to z przepisów o ochronie danych osobowych, uregulowań odnoszących się do zabezpieczenia danych osobowych przetwarzanych w postaci tradycyjnej.

Opiniując z kolei projekt *rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych*,¹⁵³ zastrzeżenia Generalnego Inspektora wzbudziło brzmienie § 1 pkt 5b tego projektu. Przepis ten znacznie rozszerzył zakres danych przekazywanych przez świadczeniodawców podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych. W opinii Generalnego Inspektora, gromadzenie danych osobowych w nadmiarze narusza zasadę adekwatności danych osobowych w stosunku do celów ich przetwarzania.¹⁵⁴

¹⁴⁹ 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.

¹⁵⁰ DOLiS-033-433/09, do § 2 ust. 8 projektu.

¹⁵¹ § 2 ust. 4 projektu przewiduje, iż zgłoszeń, o których mowa w ust. 2 i 3 (tj.: Każde zdarzenie niepożądane w czasie wywozu lub przywozu komórek lub tkanek należy niezwłocznie zgłosić do Krajowego Centrum Bankowania Tkanek i Komórek (ust. 2); Każde istotne zdarzenie niepożądane w czasie wywozu lub przywozu narządów należy niezwłocznie zgłosić do Centrum Organizacyjno-Koordynacyjnego do Spraw Transplantacji „Poltransplant” (ust. 3).

¹⁵² Obowiązek właściwego zabezpieczenia przez administratora danych przetwarzanych przez niego danych osobowych wynika z art. 36 ustawy o ochronie danych osobowych.

¹⁵³ DOLiS-033-436/09.

¹⁵⁴ Wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Weryfikacji wymaga też rzeczywista potrzeba przekazywania danych osobowych osób, którym udzielono określonego świadczenia, wskazanym w piśmie podmiotom. Z zasady adekwatności wynika bowiem, iż administrator danych może przetwarzać (w tym udostępniać czy gromadzić) jedynie takie dane, które są niezbędne z punktu widzenia osiągnięcia zamierzonego celu przetwarzania danych. Wątpliwości organu do spraw ochrony danych osobowych wzbudza zatem konieczność władania przez Narodowy Fundusz Zdrowia szczegółowymi informacjami dotyczącymi porady udzielonej osobie, której dane dotyczą. Ponadto z uzasadnienia do tego projektu¹⁵⁵ wynika, że dane osobowe przekazywane będą wyłącznie w stosunku do osób cierpiących na cukrzycę lub choroby układu krążenia. Powyższe nie wynika natomiast wprost z przepisów samego projektu.

Podobne wątpliwości Generalnego Inspektora wzbudziła obligatoryjność przekazywania do NFZ danych osobowych w sytuacji wskazanej w projektowanym § 6 ust. 2 pkt 2 rozporządzenia. W chwili obecnej w przypadku świadczeń innych niż porada przekazywane są wyłącznie informacje zbiorcze.¹⁵⁶ Dlatego też Generalny Inspektor wskazał, iż każdorazowe rozszerzanie zakresu przetwarzanych (przekazywanych przez jeden podmiot i – w następstwie tego gromadzonych przez inny) danych osobowych, zwłaszcza w odniesieniu do danych podlegających szczególnej ochronie, powinno następować jedynie w zakresie niezbędnym w stosunku do rzeczywistej potrzeby władania nimi przez podmiot, który je otrzymuje, implikowanej kompetencjami takiego podmiotu stosownie do obowiązujących przepisów prawa.

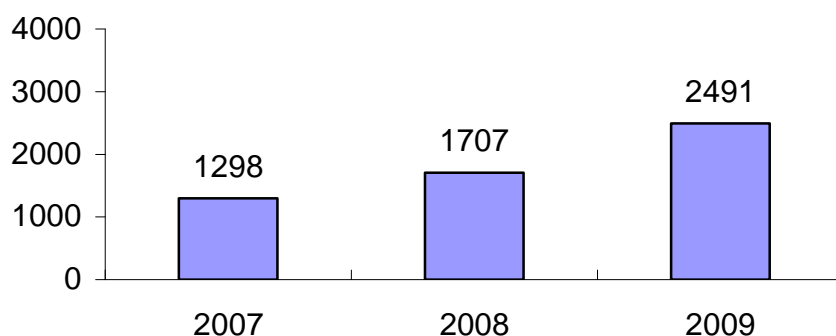
Podsumowując uchybienia najczęściej popełniane przez projektodawców w procesie tworzenia prawa należy zaznaczyć, iż mają one charakter bardzo różnorodny. Niektóre z nich w niewielkim stopniu naruszają przepisy ustawy o ochronie danych osobowych, inne zaś burzą wręcz porządek konstytucyjny, a nawet obowiązujące 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

W celu kształtowania właściwych standardów ochrony danych osobowych w życiu publicznym, Generalny Inspektor Ochrony Danych Osobowych, wychodząc naprzeciw potrzebom obywateli, prowadzi działalność w zakresie odpowiadania na kierowanie do niego pytania dotyczące legalności przetwarzania danych osobowych, zarówno przez podmioty przetwarzające dane osobowe, jak i osób,

¹⁵⁵ W zakresie projektowanego brzmienia § 6 ust. 2 pkt 1.

których dane dotyczą. Udzielanie odpowiedzi na pytania stanowi więc istotny element działalności edukacyjnej Generalnego Inspektora. W roku 2009 do GIODO wpłynęło **2491 pytań** z prośbą o interpretację przepisów prawa dotyczących ochrony danych osobowych lub sygnalizujących różnego rodzaju problemy związane z przestrzeganiem przepisów dotyczących ochrony danych osobowych. Porównanie liczby pytań skierowanych do Generalnego Inspektora w latach 2007–2009 przedstawia Wykres 24.



Wykres 24: Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GIODO w latach 2007–2009.

W porównaniu z ubiegłym rokiem, w okresie objętym sprawozdaniem o 784 zwiększyła się liczba pytań wpływających do organu do spraw ochrony danych osobowych. Należy to uznać za konsekwencję intensywnych działań informacyjno-edukacyjnych Generalnego Inspektora. Najważniejsze z nich opisane zostały 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. Zagadnienia poruszane przez pytających oraz rozstrzygane przez organ do spraw ochrony danych osobowych w roku 2009 – podobnie jak w latach ubiegłych – dotyczyły sfery działalności zarówno podmiotów prywatnych, jak i publicznych.

6.1. Interpretacja przepisów

Problemy, jakie wynikają ze stosowania przepisów o ochronie danych osobowych, pojawiają się co roku i wiążą się z podejmowaniem przez Generalnego Inspektora Ochrony Danych Osobowych takich form aktywności, jak wystąpienia do jednostek przetwarzających dane oraz udzielanie

¹⁵⁶ § 6 ust. 3 rozporządzenia Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych – Dz. U. Nr 123, poz. 801.

odpowiedzi na kierowane do niego pytania. Wystąpienia te sygnalizują konieczność zmiany dotychczasowej praktyki stosowanej przez podmioty zarówno sektora publicznego, jak i prywatnego, celem dostosowania procesu przetwarzania danych do wymogów wynikających z przepisów regulujących kwestie ich ochrony. **W 2009 r. wśród indywidualnych pytań kierowanych do GODO znalazły się zarówno te kierowane przez osoby fizyczne, jak i przez podmioty ze sfery prywatnej i publicznej.**

Wśród tego rodzaju sygnalizacji kierowanych m.in. do **podmiotów z sektora publicznego** znalazła się sprawa, w której Generalny Inspektor Ochrony Danych Osobowych pozyskał informację dotyczącą procesu doręczania przez jednego z powiatowych inspektorów nadzoru budowlanego stronom postępowania administracyjnego „Zawiadomień o złożeniu listu poleconego w postępowaniu administracyjnym”. Podmiot ten umieszczał zawiadomienia w taki sposób, że informacje o toczącym się postępowaniu i stronach tego postępowania mogły uzyskać osoby trzecie, co naruszało przepisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. 2000 r. Nr 98, poz. 1071 z późn. zm.), oraz art. 26 ustawy o ochronie danych osobowych. Z informacji wynikało, iż jedno z zawiadomień znalezione zostało na wycieraczce przy drzwiach mieszkania, chociaż w bloku mieszkalnym znajdowała się skrzynka pocztowa. Generalny Inspektor wystąpił do tego organu o zaprzestanie tego rodzaju praktyki.¹⁵⁷ W treści swego wystąpienia zwrócił uwagę, iż przepisy ustawy z dnia 7 lipca 1994 r. Prawo budowlane (Dz. U. 2006 r. Nr 156, poz. 1118 z późn. zm.), zobowiązują organy nadzoru budowlanego do stosowania przepisów K.p.a. w toku badania prawidłowości postępowania administracyjnego przed organami administracji architektoniczno – budowlanej oraz wydawanych w jego toku decyzji i postanowień. Przepisy wskazują sposób doręczania stronom pism w toku postępowania,¹⁵⁸ a także określają sposób, w jaki dostarcza się zawiadomienie o pozostawieniu pisma z możliwością jego odbioru w określonym czasie i miejscu.¹⁵⁹ Wskazał również na właściwy dla tej materii wyrok Wojewódzkiego Sądu Administracyjnego stanowiący o kolejności, w jakiej należy postępować, doręczając przedmiotowe zawiadomienie.¹⁶⁰ Generalny Inspektor skonstatował, iż analiza przepisów wskazuje jednoznacznie na hierarchizację sposobu doręczania pism w postępowaniu administracyjnym i podkreślił, że wybór sposobu doręczenia pism jest narzucony

¹⁵⁷ Wystąpienie GODO z 9 kwietnia 2009 r. DOLiS-035-278/09.

¹⁵⁸ W myśl art. 42 ust. 1 K.p.a. pisma doręcza się osobom fizycznym w ich mieszkaniu lub miejscu pracy.

¹⁵⁹ Zgodnie z art. 44 ust. 2 Kpa, zawiadomienie o pozostawieniu pisma wraz z informacją o możliwości jego odbioru w terminie siedmiu dni, licząc od dnia pozostawienia zawiadomienia w miejscu określonym w ust. 1, umieszcza się w oddawczej skrzynce pocztowej lub, gdy nie jest to możliwe, na drzwiach mieszkania adresata, jego biura lub innego pomieszczenia, w którym adresat wykonuje swoje czynności zawodowe, bądź w widocznym miejscu przy wejściu na posesję adresata.

¹⁶⁰ W wyroku z dnia 18 stycznia 2008 r., Wojewódzki Sąd Administracyjny w Gliwicach (sygn. IV SA/Gl 674/2007) orzekł, iż „Przepis art. 44 K.p.a. ustanawia wiążącą doręczającego kolejność miejsc, w których należy umieścić zawiadomienie. Oznacza to, że podmiot doręczający powinien umieścić zawiadomienie w skrzynce na korespondencję, a gdy umieszczenie zawiadomienia w ten sposób nie jest możliwe, to może to uczynić w ten sposób, że umieści zawiadomienie w drzwiach

przez ustawodawcę. Zwrócił jednocześnie uwagę na przepisy określające wymogi, jakie powinna spełniać skrzynka pocztowa umieszczona w budynkach wielorodzinnych, zwłaszcza w zakresie poufności.¹⁶¹

W związku z ukazaniem się publikacji prasowej¹⁶² pod tytułem: „Adresy i PESEL-e polityków całkiem jawne w Internecie” GIODO pozyskał informację, iż Państwowa Komisja Wyborcza od lat udostępnia na swoich stronach internetowych dane osobowe zawarte w sprawozdaniach finansowych partii politycznych. Jak ustalił Generalny Inspektor Ochrony Danych Osobowych, na stronie internetowej Państwowej Komisji Wyborczej opublikowane zostały informacje finansowe o otrzymanej subwencji oraz o poniesionych z tej subwencji wydatkach, zawierające dane osobowe osób wchodzących w skład organu statutowego partii politycznej, uprawnionego do jej reprezentowania, w zakresie imion, nazwisk, adresów zamieszkania oraz numerów ewidencyjnych PESEL. Biorąc pod uwagę przepisy ustawy z dnia 27 czerwca 1997 r. o partiach politycznych (tekst jednolity: Dz. U. z 2001 r. Nr 79, poz. 857 z późn. zm.), z których wynika, iż informacje finansowe o otrzymanej subwencji oraz o poniesionych z subwencji wydatkach Państwowa Komisja Wyborcza [PKW] ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”,¹⁶³ brak jest podstaw uprawniających PKW do udostępniania danych w innej formie niż publikacja w Monitorze Polskim. Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych wystąpił do Przewodniczącego Państwowej Komisji Wyborczej o usunięcie opublikowanych danych ze strony internetowej Państwowej Komisji Wyborczej.¹⁶⁴ W odpowiedzi Przewodniczący PKW poinformował, że dokumenty zawierające dane osobowe osób wchodzących w skład organów statutowych partii, uprawnionych do jej reprezentowania na zewnątrz zostały usunięte ze strony PKW. Udostępnianie tych dokumentów na stronie internetowej będzie wznowione po usunięciu z nich adresów zamieszkania i numerów PESEL osób wymienionych. Jednocześnie Przewodniczący Państwowej Komisji Wyborczej zwrócił uwagę na konieczność zmiany obowiązujących przepisów prawa w zakresie zapewnienia ochrony prywatności osób wchodzących w skład organów statutowych partii.¹⁶⁵

mieszkania adresata, albo w drzwiach pomieszczenia, w którym adresat wykonuje swoje obowiązki zawodowe (pracuje), lub w miejscu widocznym tej nieruchomości, np. na bramie. (...)”.

¹⁶¹ Rozporządzenie Ministra Infrastruktury z dnia 24 września 2003 r. w sprawie oddawczych skrzynek pocztowych (Dz. U. 2003 r. Nr 177, poz. 1731 z późn. zm.).

¹⁶² „Dziennik” – wydanie z dnia 5 maja 2009 r.

¹⁶³ Informację finansową o otrzymanej subwencji oraz o poniesionych z subwencji wydatkach, zgodnie z art. 34 ust. 5 ustawy z dnia 27 czerwca 1997 r. o partiach politycznych (tekst jednolity: Dz. U. z 2001 r. Nr 79, poz. 857 z późn. zm.), Państwowa Komisja Wyborcza ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, w terminie 14 dni od dnia złożenia jej Państwowej Komisji Wyborczej. Stosownie do art. 38 ust. 4 ustawy o partiach politycznych, Państwowa Komisja Wyborcza ogłasza sprawozdanie wraz z opinią i raportem, o którym mowa w ust. 3, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, w terminie 14 dni od dnia złożenia go Państwowej Komisji Wyborczej.

¹⁶⁴ DOLiS-035-677/09.

¹⁶⁵ Pismo Prezesa Państwowej Komisji Wyborczej z 11 maja 2009 r. znak: ZKF-066-10/09.

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wystąpił do Marszałka Sejmu Rzeczypospolitej Polskiej, Ministra Finansów oraz Przewodniczących Klubów Parlamentarnych i Poselskich Sejmu RP o podjęcie prac legislacyjnych mających na celu zmianę aktualnie obowiązującego porządku prawnego. Generalny Inspektor zaproponował, aby podjęte działania zmierzały albo w kierunku pozyskiwania informacji w zakresie numeru PESEL oraz adresu zamieszkania wskazanych osób wyłącznie na potrzeby PKW, tj. zmiany aktualnie obowiązującego wzoru sprawozdania (stanowiącego załącznik do rozporządzenia Ministra Finansów z dnia 18 lutego 2003 r. sprawie sprawozdania o źródłach pozyskania środków finansowych – Dz. U. Nr 33, poz. 269), poprzez wykreślenie z jego treści powołanych danych, albo też zmiany przepisów ustawy z o partiach politycznych, stanowiących o publikacji sprawozdania, w ten sposób, ażeby z ich treści wynikało, że kwestionowane wyżej informacje nie są objęte publikacją.

W związku z inną publikacją prasową, tym razem odnoszącą się do ochrony zdrowia, pod tytułem: „Jak ochronić wrażliwe dane pacjentów,”¹⁶⁶ GODO pozyskał informację, iż listy oczekujących na udzielenie świadczenia opieki zdrowotnej zawierające dane osobowe pacjentów są publikowane przez Oddziały Wojewódzkie Narodowego Funduszu Zdrowia. Powszechny dostęp do listy oczekujących może prowadzić do ujawnienia danych wrażliwych, np. listy osób oczekujących na leczenie w zakładzie psychiatrycznym. Prezes Narodowego Funduszu Zdrowia poinformował Generalnego Inspektora,¹⁶⁷ że na stronach internetowych NFZ nie były publikowane dane osobowe pacjentów oczekujących na udzielenie świadczenia opieki zdrowotnej. Zgodnie z art. 23 ust. 6 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2008 r. Nr 164, poz. 1027 z późn. zm.), Fundusz tworzył natomiast centralny wykaz informacji o liczbie oczekujących na udzielenie świadczenia opieki zdrowotnej i średnim czasie oczekiwania w poszczególnych oddziałach wojewódzkich Funduszu. Źródłem wykazu były informacje o liczbie oczekujących i średnich czasach oczekiwania do komórek organizacyjnych oraz na wybrane procedury medyczne, terapeutyczne programy zdrowotne i świadczenia z zakresu chemioterapii przekazywane co miesiąc przez świadczeniodawców za pośrednictwem szczegółowych komunikatów sprawozdawczych XML dotyczących list oczekujących do właściwych ze względów na miejsce udzielania świadczeń oddziałów wojewódzkich Funduszu, które następnie przesyłają powyższe dane do Centrali Funduszu. W ten sposób zasilany jest internetowy serwis Kolejki oczekujących, dostęp do którego zapewniony jest ze stron www zarówno oddziałów wojewódzkich, jak i Centrali Funduszu. Z serwisu mogą korzystać wszystkie zainteresowane osoby, dostęp jest powszechny, a zawiera on informacje o liczbie oczekujących, bez danych osobowych. W internetowym serwisie Kolejki oczekujących publikowany jest miesiąc i rok aktualizacji danych przez świadczeniodawcę np. 08/2009,

¹⁶⁶ „Rzeczpospolita” – wydanie z 21 sierpnia 2009 r.

¹⁶⁷ DOLiS-035-1538/09.

co oznacza, że dane o liczbie oczekujących i średnim czasie oczekiwania prezentują stan kolejki oczekujących u świadczeniodawcy na ostatni dzień sierpnia 2009 r. Listy oczekujących wykorzystuje się także do oceny prawidłowości prowadzenia przez świadczeniodawców list oczekujących, przestrzegania przez nich obowiązujących w tym zakresie przepisów prawa, a także weryfikacji wielokrotnych wpisów pacjentów na listy oczekujących na to samo świadczenie u różnych świadczeniodawców. Zgodnie bowiem z art. 20 ust. 10 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w celu otrzymania jednego świadczenia opieki zdrowotnej na podstawie skierowania, świadczeniobiorca może wpisać się na jedną listę oczekujących u jednego świadczeniodawcy.¹⁶⁸ Na podstawie powyższych wyjaśnień Generalny Inspektor uznał, iż prezentowana argumentacja w ww. piśmie przyczyniła się do rozstrzygnięcia zaistniałych wątpliwości.

W opisywanym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych pozyskał od Obywatelskiego Biura Interwencji z siedzibą w Sopocie informacje, że dane osobowe członków zarządu fundacji, w zakresie ich prywatnych adresów zamieszkania ujawniane są w sprawozdaniach finansowych fundacji. W tej sprawie Generalny Inspektor wystąpił do Ministra Sprawiedliwości¹⁶⁹ z prośbą o podjęcie prac legislacyjnych mających na celu zmianę aktualnie obowiązującego stanu prawnego zezwalającego na ujawnianie danych członków zarządu fundacji w ww. zakresie i dostosowanie do przepisów ustawy o ochronie danych osobowych. W swoim wystąpieniu Generalny Inspektor powołał § 2 pkt 1 rozporządzenia Ministra Sprawiedliwości z dnia 8 maja 2001 r. w sprawie ramowego zakresu sprawozdania z działalności fundacji (Dz. U. Nr 50, poz. 529 z późn. zm.), z którego wynika, że sprawozdanie powinno zawierać m.in. dane dotyczące członków zarządu fundacji (imię i nazwisko według wpisu w rejestrze sądowym i adres zamieszkania). Jak stanowi art. 12 ust. 2 ustawy z dnia 6 kwietnia 1984 r. o fundacjach (tj. Dz. U. z 1991 r. Nr 46, poz. 203 z późn. zm.), fundacja składa corocznie właściwemu ministrowi sprawozdanie ze swojej działalności. Sprawozdanie, o którym mowa w ust. 2, jest przez fundację udostępnione do publicznej wiadomości (ust. 3 art. 12 ustawy). Generalny Inspektor zwrócił uwagę, iż nie negując konieczności zapewnienia transparentności działania fundacji, w demokratycznym państwie prawnym konieczne jest także respektowanie prawa do prywatności i ochrony danych osobowych. Obowiązek poszanowania prawa do prywatności wynika również z faktu, iż Rzeczpospolita Polska, jako państwo członkowskie Unii Europejskiej, jest stroną europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie w 4 listopada 1950 r. [Europejska Konwencja], która w swym art. 8 ustanawia prawo do poszanowania życia prywatnego i rodzinnego, swojego mieszkania i tajemnicy korespondencji. Organ do spraw

¹⁶⁸ Pismo Prezesa NFZ z 22 września 2009 r. znak: NFZ/CF/DSS/MSZ/2009/075/0027/W/17591.

¹⁶⁹ DOLiS-035-698/09.

ochrony danych osobowych zwrócił przy tym uwagę na wyrażoną w ustawie o ochronie danych osobowych zasadę adekwatności danych osobowych, zgodnie z którą administrator danych powinien przetwarzać dane wyłącznie takiego rodzaju i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Generalny Inspektor zaproponował w tej sprawie zmiany, które powinny zmierzać albo do pozyskiwania informacji w węższym zakresie, tj. zmiany aktualnie obowiązującego rozporządzenia, albo do zmiany przepisów ustawy o fundacjach.

W kolejnej sprawie Generalny Inspektor pozyskał informację, że jeden z urzędów miejskich w postępowaniach w sprawach o wykroczenia w ruchu drogowym stosuje wzory formularzy mandatu karnego przewidujące pozyskiwanie danych w szerszym zakresie niż wynika to z przepisów prawa. Organ do spraw ochrony danych osobowych w tej sprawie wystąpił do prezydenta miasta z prośbą o podjęcie stosownych działań w tej kwestii.¹⁷⁰ Wzór formularza mandatu karnego został określony w rozporządzeniu Prezesa Rady Ministrów z dnia 22 lutego 2002 r. w sprawie nakładania grzywnien w drodze mandatu karnego (Dz. U. Nr 20, poz. 201), a także szczegółowo w załączniku do ww. rozporządzenia, określającym wzór formularza karnego. Generalny Inspektor wskazał, iż w sytuacji umieszczenia danych w szerszym zakresie niż wynika to z cytowanych wyżej przepisów, dalsze posługiwanie się tym formularzem prowadzi do ujawnienia danych osobowych sprawców podmiotom i/lub osobom nieupoważnionym. Organ do spraw ochrony danych osobowych zwrócił przy tym uwagę, iż przetwarzanie danych dotyczących orzeczeń o ukaraniu i mandatów karnych, stosownie do art. 27 ust. 1 ustawy, jest – co do zasady – zakazane. Wyjątki od ogólnego zakazu ich przetwarzania zostały określone w ust. 2 powołanego przepisu (art. 27 ust. 2 pkt. 1–10). Podkreślił, iż przy przetwarzaniu danych należy mieć na uwadze zasadę legalności i adekwatności, wyrażoną w art. 26 ust. 1 i 3 ustawy o ochronie danych osobowych, powołując wyrok Wojewódzkiego Sądu Administracyjnego w tej kwestii.¹⁷¹

W omawianym okresie organ do spraw ochrony danych osobowych wystąpił do Ministra Nauki i Szkolnictwa Wyższego o podjęcie działań, mających na celu wskazanie rektorom uczelni wyższych na konieczność legitymowania się przesłanką zgody osoby, której dane dotyczą, w sytuacji przetwarzania przez nich danych osobowych studentów, w celach marketingowych po ustaniu procesu kształcenia.¹⁷² Impulsem do tego wystąpienia stała się coraz większa liczba pytań w sprawie legalności przetwarzania danych osobowych absolwentów uczelni wyższych w celach marketingowych, a także informacje prasowe dotyczące planów Ministerstwa Nauki i Szkolnictwa Wyższego co do zobowiązania uczelni do gromadzenia danych o swoich absolwentach, w celu monitorowania ich karier, po zakończeniu procesu kształcenia.

¹⁷⁰ DOLiS-035-674/09.

¹⁷¹ Wyrok z 1 grudnia 2005 r. sygn. akt II S.A./Wa 917/2005. Zob. też przypis 197.

¹⁷² Wystąpienie GIODO z 1 czerwca 2009 r. DOLiS-035-634/09.

GIODO zwrócił uwagę na wynikający z ustawy o ochronie danych osobowych zakaz przetwarzania danych w celach innych, niż ten, dla którego zostały one zebrane. Zaznaczył również, iż wymienione w tym przepisie warunki dopuszczalności przetwarzania danych osobowych w „innych celach”, muszą być spełnione łącznie, co podkreślił w jednym ze swych wyroków Naczelny Sąd Administracyjny,¹⁷³ oraz na co wskazuje literatura przedmiotu.¹⁷⁴ Generalny Inspektor wskazał, iż na administratorze danych (w tym przypadku na uczelni), spoczywa obowiązek ochrony danych osobowych zarówno studentów, jak i absolwentów oraz przetwarzania tych danych zgodnie z zasadą celowości przewidzianą przez przepisy ustawy o ochronie danych osobowych. Pierwotnym celem, dla którego uczelnia pozyskuje dane osobowe studentów, jest przeprowadzenie procesu kształcenia. Po jego zakończeniu wszelkie działania mające na celu, czy to promocję uczelni, czy też zachęcenie absolwentów do uczestnictwa w innych przedsięwzięciach realizowanych przez uczelnię, powinno opierać się na przesłance zgody (art. 23 ust. 1 pkt 1 ustawy). Zgoda absolwenta powinna być zaś pozyskana jeszcze w toku jego kształcenia, gdyż istotne jest, aby osoba, której dane dotyczą, miała świadomość, w jakich celach dane będą przetwarzane. Jednocześnie uczelnia powinna wypełnić w tym zakresie tzw. obowiązek informacyjny, wskazany w art. 24 ustawy o ochronie danych osobowych. Generalny Inspektor zwrócił także uwagę na brzmienie prawidłowo skonstruowanej klauzuli zgody.

Kolejne warte omówienia zagadnienie związane było również z działalnością uczelni wyższej i dotyczyło ujawniania imion i nazwisk, nazwy wydziału, roku nauki i numeru grupy studentów w celu informowania ich o organizacji roku akademickiego.¹⁷⁵ Wypowiadając się w powyższej kwestii, Generalny Inspektor wyjaśnił, iż zgodnie z ustawą o ochronie danych osobowych, przetwarzanie danych osobowych tzw. zwykłych (jak np. imię, nazwisko), w tym ich udostępnianie, jest procesem legalnym, gdy ich administrator legitymuje się jedną z przesłanek dopuszczalności przetwarzania danych wymienionych w jej art. 23 ust. 1. Dlatego też sygnalizowaną sprawę należy rozpatrywać w oparciu o przepisy ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. Nr 164, poz. 1365 z późn. zm.) i wydanych na jej podstawie aktów wykonawczych, a także wewnętrznych aktów obowiązujących w danej uczelni, np. regulaminu studiów. Analiza przepisów ustawy o szkolnictwie wyższym wyraźnie wskazuje, że jawne są jedynie wyniki postępowania rekrutacyjnego.¹⁷⁶ Żaden przepis tej ustawy nie upoważnia natomiast wprost do upublicznienia informacji dotyczących organizacji roku akademickiego z wykorzystaniem danych osobowych studentów, a jedynie stanowi, iż organizację i tok studiów oraz związane z nimi prawa i obowiązki

¹⁷³ Wyrok z 5 lutego 2003 r., sygn. akt II SA 3505/2001 („Gazeta Prawna” 2002, nr 27, s. 16).

¹⁷⁴ A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, Wyd. Prawnicze (wyd. I) ss. 166.

¹⁷⁵ DOLiS-035-1910/09.

¹⁷⁶ Zgodnie z treścią art. 169 ust. 9 wyniki postępowania rekrutacyjnego są jawne.

studenta określa regulamin studiów.¹⁷⁷ W postanowieniach regulaminu powinny się zatem znaleźć takie rozwiązania organizacyjne, które pozwolą na prawidłową organizację studiów i ustalenie ich przebiegu. Zdaniem organu do spraw ochrony danych osobowych, postanowienia regulaminu nie mogą być kształtowane w oderwaniu od innych obowiązujących przepisów prawa, w tym ustawy o ochronie danych osobowych, która nakazuje administratorowi danych przetwarzanie danych wyłącznie w celu, dla którego zostały pozyskane, i z należytą starannością, tj. z uwzględnieniem potrzeby ochrony danych przed udostępnieniem ich osobom nieupoważnionym. Opublikowanie danych na stronie internetowej powoduje bowiem udostępnienie ich nie tylko zainteresowanym studentom, ale także nieograniczonej liczbie użytkowników tej strony. Powstaje zatem wątpliwość, czy dla realizacji celu, jakim jest zapewnienie właściwej organizacji przebiegu studiów, niezbędne jest udostępnianie osobom trzecim takich informacji, jak imię i nazwisko studenta, wydział, rok nauki i numer grupy. Zdaniem Generalnego Inspektora, kształtowanie treści regulaminu powinno się odbywać z uwzględnieniem zasad określonych w ustawie o ochronie danych osobowych,¹⁷⁸ gdyż skutek publikacji w Internecie powyższych informacji krąg osób, które będą miały do nich dostęp, zostaje rozszerzony. W przypadku, gdy regulamin uczelni wyraźnie nie określa warunków informowania studentów, konieczne jest spełnienie innej przesłanki legalizującej takie przetwarzanie (udostępnianie) danych osobowych, tj. pozyskanie zgody osoby, której dane dotyczą.¹⁷⁹ Generalny Inspektor Ochrony Danych Osobowych wyjaśnił też, że zasadne wydaje się rozważenie utworzenia specjalnej strony internetowej, do której dostęp posiadaliby wyłącznie studenci, bądź osoby bezpośrednio zainteresowane, posługujące się specjalnym kodem lub hasłem.

W analizowanym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych zwrócił się również do prezydenta jednego z miast o podjęcie działań mających na celu wskazanie osobom odpowiedzialnym za przetwarzanie danych osobowych w przedszkolach publicznych, iż upublicznianie danych osobowych dzieci, poprzez wywieszenie list zawierających ich dane na drzwiach wejściowych przedszkoli, prowadzi do naruszenia przepisów ustawy o ochronie danych osobowych.¹⁸⁰ Informacje o tego rodzaju praktyce Generalny Inspektor pozyskał z materiału prasowego. Podkreślił, iż w sytuacji, gdy podmiot gromadzący dane nie legitymuje się żadną z przesłanek określonych w art. 23 ust. 1 pkt. 2–5 ustawy o ochronie danych osobowych, upublicznienie danych jest możliwe wyłącznie po uzyskaniu zgody osoby, której dane dotyczą.¹⁸¹ W przypadku danych dzieci konieczna jest zgoda ich rodziców lub opiekunów prawnych. Brak spełnienia którejkolwiek z przesłanek uniemożliwia przetwarzanie danych osobowych, a w szczególności ich udostępnianie osobom nieuprawnionym.

¹⁷⁷ Art. 160 ust. 1 powołanej ustawy stanowi: organizację i tok studiów oraz związane z nimi prawa i obowiązki studenta określa regulamin studiów.

¹⁷⁸ Tj. art. 26 ust. 1 pkt. 2 i 3 oraz art. 36.

¹⁷⁹ Art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

¹⁸⁰ Wystąpienie GIODO z 1 czerwca 2009 r. DOLiS-035-807/09.

Istotną kwestią poruszoną przez jednego z senatorów w piśmie przekazanym Generalnemu Inspektorowi przez Marszałka Senatu Rzeczypospolitej Polskiej¹⁸² było podawanie do publicznej wiadomości danych osobowych, w tym nazwisk, osób skazanych przez sądy powszechne za prowadzenie pojazdów pod wpływem alkoholu. Odnosząc się do tej kwestii, Generalny Inspektor Ochrony Danych Osobowych wskazał,¹⁸³ iż obowiązujące w polskim porządku prawnym przepisy prawa regulują w sposób wyczerpujący kwestie podawania wyroków do publicznej wiadomości. Zgodnie bowiem z art. 39 pkt 8 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.), środkiem karnym jest m.in. podanie wyroku do publicznej wiadomości. Dalsze przepisy ww. kodeksu precyzują, iż sąd może orzec podanie wyroku do publicznej wiadomości w określony sposób, jeżeli uzna to za celowe, w szczególności ze względu na społeczne oddziaływanie skazania, o ile nie narusza to interesu pokrzywdzonego (art. 50 Kodeksu karnego). Jak wynika z wyroku Sądu Apelacyjnego w Katowicach z 28 czerwca 2007 r. (sygn. akt II AKa 190/2007), podanie wyroku do publicznej wiadomości powinno mieć miejsce przede wszystkim w takich przypadkach, które wzbudziły szczególne zainteresowanie społeczne, wywołały powszechne oburzenie czy też niepokój. Celowe jest również sięganie do tego środka w przypadku przestępstw nagminnie popełnianych na danym terenie lub w określonym środowisku. W każdym przypadku to sąd podejmuje decyzję o podawaniu wyroku do publicznej wiadomości, kierując się wskazanymi wyżej kryteriami. Natomiast brak jest podstaw do zmiany aktualnie obowiązującego stanu prawnego i wprowadzenia generalnej zasady podawania przez różnorakie podmioty do wiadomości publicznej danych osobowych osób skazanych przez sąd w związku z prowadzeniem przez nie pojazdów pod wpływem alkoholu, choćby podczas, jak określił to zainteresowany sprawą senator, cyt.: „(...) odczytywania ogłoszeń parafialnych czy też w postaci ogłoszeń gminnych (...)”.

Stosowanie powyższych form piętnowania osób skazanych za tego rodzaju czyn, zdaniem Generalnego Inspektora, byłoby sprzeczne z ustawą o ochronie danych osobowych. Ustawa ta w art. 27 ust. 1 wprowadza bowiem ogólny zakaz przetwarzania danych określanych powszechnie w piśmiennictwie jako dane wrażliwe albo szczególnie chronione. Katalog tych danych ma charakter zamknięty i obejmuje dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Natomiast zakaz przetwarzania omawianej kategorii danych osobowych zostaje uchylony wyłącznie w sytuacji spełnienia przez administratora danych

¹⁸¹ Art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

¹⁸² Pismo Marszałka Senatu Rzeczypospolitej Polskiej z 21 maja 2009 r. o sygn. BPS/DSK-043-1710/09.

¹⁸³ DOLiS-035-895-09.

jednej z przesłanek określonych w ust. 2 art. 27. W piśmie skierowanym do zainteresowanego w sprawie wskazano także, iż stosownie do treści pkt. 2 powołanego wyżej przepisu, wykonywanie jakichkolwiek operacji na wrażliwych danych osobowych jest dopuszczalne, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony. Omawiany wyjątek dotyczy jedynie takich przepisów, których, po pierwsze, brzmienie nie pozostawia wątpliwości w kwestii uchylenia zakazu przetwarzania danych, po drugie wskazujących, iż przetwarzanie danych osobowych jest dopuszczalne bez zgody osoby, której dane dotyczą i po trzecie, które stwarzają pełne gwarancje ochrony, przez co rozumieć należy gwarancje ochrony wrażliwych danych osobowych. Dopiero wówczas, gdy określony przepis spełnia wszystkie powyższe warunki łącznie, można uznać go za podstawę do przetwarzania, w tym ujawniania przez administratora, danych konkretnej osoby.

Istotna sprawa, którą Generalny Inspektor Ochrony Danych Osobowych podjął w 2009 r., związana była z planowanym zaprzestaniem wydawania przez Zakład Ubezpieczeń Społecznych legitymacji ubezpieczeniowych od 1 stycznia 2010 r. oraz wydaniem przez Narodowy Fundusz Zdrowia wytycznych dotyczących dokumentów, jakie osoba zamierzająca skorzystać ze świadczeń opieki zdrowotnej w ramach ubezpieczenia w NFZ zobowiązana jest przedstawić na potwierdzenie prawa do ich uzyskania. Generalny Inspektor Ochrony Danych Osobowych wystąpił do Ministra Zdrowia oraz Prezesa Narodowego Funduszu Zdrowia¹⁸⁴ w tej sprawie, bowiem propozycje przyjętych przez ww. podmioty rozwiązań budziły istotne zagrożenia dla gwarantowanych Konstytucją Rzeczypospolitej Polskiej praw osób fizycznych do ochrony dotyczących ich danych osobowych. Generalny Inspektor dostrzegł zagrożenia związane z ujawnianiem instytucjom realizującym świadczenia zdrowotne wszystkich informacji zawartych w dokumentach, jakie osoba zamierzająca skorzystać ze świadczeń opieki zdrowotnej w ramach ubezpieczenia w NFZ zobowiązana jest przedstawić na potwierdzenie prawa do ich uzyskania. Wskazał też, iż treść wytycznych NFZ w tym zakresie, nie sprzyja ochronie danych osobowych pacjentów, mimo że precyzuje jedynie obowiązujący art. 240 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (tj. Dz. U. z 2008 r. Nr 164, poz. 1027 z późn. zm.).¹⁸⁵ Wskazał także, że bez znaczenia jest w analizowanej sytuacji fakt, iż pacjentowi pozostawiono możliwość wyboru dokumentu, jaki może on przedstawić w celu uzyskania przysługującego

¹⁸⁴ DOLiS-035-2228/09.

¹⁸⁵ Zgodnie z jego brzmieniem, do czasu wydania ubezpieczonemu karty ubezpieczenia zdrowotnego dowodem ubezpieczenia zdrowotnego jest każdy dokument, który potwierdza uprawnienia do świadczeń opieki zdrowotnej, w szczególności dokument potwierdzający opłacanie składek na ubezpieczenie zdrowotne (ust. 1). W przypadku emerytów i rencistów dokumentem potwierdzającym opłacanie składek na ubezpieczenie zdrowotne, o którym mowa w ust. 1, jest dokument potwierdzający kwotę przekazanej emerytury lub renty, w tym w szczególności odcinek przekazu lub wyciąg (ust. 2). W przypadku emerytów i rencistów dokumentem potwierdzającym fakt objęcia ubezpieczeniem zdrowotnym może być legitymacja emeryta (rencisty) wydawana na podstawie odrębnych przepisów (ust. 3).

mu świadczenia. Oczywiście jest, że w chwili nagłej konieczności związanej z ochroną własnego zdrowia, może on być pozbawiony możliwości dokonania czynności jak najmniej dotkliwej dla jego prywatności i korzystać będzie z dokumentu, którym akurat będzie dysponował. Wymaganie natomiast (i oczekiwanie) od obywatela, aby gromadził dotyczące go dokumenty niejako „na zapas”, w sposób oczywisty nie sprzyja budowaniu jego zaufania do obowiązującego porządku prawnego, co więcej, może stać w sprzeczności z art. 31 ust. 2 zdanie drugie Konstytucji, zgodnie z treścią którego: „Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje.” Ujawnianie wszystkich informacji zawartych w dokumentach uzasadniających prawo do przysługującego pacjentowi świadczenia, w sposób oczywisty narusza zasady zawarte w ustawie o ochronie danych osobowych, tj. zasady adekwatności i związania celem. Wskazać należy, że powinna być zachowana równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych, co następuje jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane, gdyż swym rodzajem i swą treścią dane nie powinny również wykraczać poza potrzeby wynikające z celu ich zbierania. Administrator danych może zatem przetwarzać jedynie takie dane, które są niezbędne do osiągnięcia zamierzonego celu. Jednocześnie zasada celowości przetwarzania danych sprzeciwia się przetwarzaniu danych osobowych osoby ubezpieczonej w zakresie np. jego wynagrodzenia - przez zakład opieki zdrowotnej, bowiem przetwarzanie takich informacji jest zupełnie zbędne dla stwierdzenia praw pacjenta wynikających z ubezpieczenia społecznego.

W opinii Generalnego Inspektora Ochrony Danych Osobowych, podmioty świadczące usługi w zakresie świadczeń zdrowotnych co do zasady należą do, tj. zgodnie z przepisami o ochronie danych osobowych, chronią przetwarzane przez siebie dane. Jednakże dopuszczenie do informacji stanowiących dobra osobiste pacjentów (np. w zakresie wynagrodzeń) bliżej nieokreślonej grupy pracowników służby zdrowia każdorazowo będzie rodziło zagrożenie naruszenia tych przepisów. Stosownie do treści art. 7 Konstytucji Rzeczypospolitej Polskiej, organy władzy publicznej działają na podstawie i w granicach prawa. Przedmiotowa zasada nakazuje, by wszelkie działania organów władzy publicznej były oparte na wyraźnie określonych normach kompetencyjnych. Obowiązująca ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w swym art. 49 wyraźnie wskazuje, iż dokumentem potwierdzającym prawo ubezpieczonego do świadczeń opieki zdrowotnej oraz umożliwiającym potwierdzenie wykonania świadczeń opieki zdrowotnej jest karta ubezpieczenia zdrowotnego. Ustęp drugi tego artykułu stanowi natomiast, iż karta ta jest kartą typu elektronicznego. Generalny Inspektor zauważył, że przepisem prawa, który aktualnie stanowi, jaki dokument ma rangę potwierdzającego prawo ubezpieczonego do świadczeń opieki zdrowotnej oraz umożliwiającym potwierdzenie wykonania świadczeń opieki zdrowotnej, jest ww. art. 49 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Niemniej jednak, mimo

obowiązki niniejszego przepisu od dnia 1 października 2004 r., tj. od dnia wejścia w życie ww. ustawy, nie jest on realizowany. Omawiana sprawa dodatkowo dotyczy kwestii wytycznych, jakie NFZ sformułował, a które miałyby być „podpowiedzią” dla ubezpieczonych, w jaki sposób udokumentować przysługujące im prawo do ubezpieczenia, gdy odmówiono im wydania legitymacji ubezpieczeniowej. Generalny Inspektor zauważył przy tym, że dokumenty, które miałyby być udostępniane stosownie do wytycznych NFZ (np. RMUA), zawierają szerszy katalog informacji, w tym danych osobowych, aniżeli niezbędne podmiotom świadczącym usługi medyczne dla realizacji ich zadań. Może zatem w ten sposób dochodzić do pozyskania danych w zakresie szerszym i nieproporcjonalnym dla realizacji tych zadań.

Konkludując Generalny Inspektor Ochrony Danych Osobowych wskazał, iż jedynym rozwiązaniem dla zaistniałej sytuacji wydaje się podjęcie w możliwie szybkim terminie prac legislacyjnych nad – określoną w art. 49 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych - kartą ubezpieczenia zdrowotnego, przy jednoczesnej kontynuacji wydawania legitymacji ubezpieczeniowych, do czasu wejścia w życie rozporządzenia, o którym mowa w art. 49 ust. 9 ww. ustawy.¹⁸⁶

Na uwagę zasługuje sprawa, z którą do Generalnego Inspektora zwrócił się komendant straży miejskiej jednego z miast z prośbą o stanowisko w zakresie możliwości udostępnienia prezydentowi miasta, na obszarze którego straż miejska działa, informacji dotyczących konkretnych strażników miejskich. W sprawie tej chodziło w szczególności o udostępnienie wyników testów sprawnościowych funkcjonariuszy lub wskazanie przyczyn nieprzystąpienia ich do tych testów w kontekście ewentualnego zakwalifikowania ww. informacji do kategorii danych „szczególnie chronionych.” W odpowiedzi¹⁸⁷ Generalny Inspektor Ochrony Danych Osobowych wskazał na art. 7 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym organy władzy publicznej działają na podstawie i w granicach prawa, i – co za tym idzie – uznał, iż uprawnienie prezydenta miasta do pozyskania wymienionych danych powinno wynikać bezpośrednio z przepisu obowiązującego prawa. Ponadto zwrócił uwagę, że art. 27 ustawy o ochronie danych osobowych określa, które informacje o osobie fizycznej mają charakter danych osobowych szczególnie chronionych i wskazał, że przetwarzanie

¹⁸⁶ Zgodnie z jego treścią, Rada Ministrów określi w drodze rozporządzenia:

- 1) wzór karty ubezpieczenia zdrowotnego oraz sposób jej wykonania, uwzględniając przepisy Unii Europejskiej w sprawie wzoru Europejskiej Karty Ubezpieczenia Zdrowotnego,
- 2) wzór wniosku o wydanie karty ubezpieczenia zdrowotnego,
- 3) szczegółowy zakres danych zawartych na karcie ubezpieczenia zdrowotnego oraz ich format,
- 4) tryb wydawania i anulowania karty ubezpieczenia zdrowotnego - uwzględniając konieczność identyfikacji ubezpieczonych, potwierdzania prawa ubezpieczonych do świadczeń opieki zdrowotnej i elektronicznego potwierdzania wykonanych świadczeń, konieczność zapewnienia przejrzystości danych zawartych na karcie ubezpieczenia zdrowotnego oraz sprawność postępowania w sprawie wydawania i anulowania karty ubezpieczenia zdrowotnego.

Rozporządzenie, o którym mowa w ust. 9, może także określać dokumenty mogące pełnić funkcję karty ubezpieczenia zdrowotnego, uwzględniając możliwość potwierdzenia przez te dokumenty prawa do świadczeń opieki zdrowotnej oraz funkcję potwierdzenia udzielenia tych świadczeń (ust. 10).

danych, o których mowa w ust. 1 tego artykułu, jest dopuszczalne m.in. wtedy, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony¹⁸⁸ lub – względnie – osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,¹⁸⁹ ewentualnie po spełnieniu innego z warunków określonych w art. 27 ust. 2. Organ do spraw ochrony danych osobowych wskazał także, iż kwalifikowanie określonej informacji jako danej o stanie zdrowia powinno odbywać się zawsze w kontekście jej uzyskiwania. Uznał, że wyniki testów sprawnościowych, którym poddawani byli strażnicy miejscy, a zwłaszcza przyczyny nieprzystąpienia do testów (np. z powodu schorzenia, przebytej choroby itp.) mogą być danymi podlegającymi szczególnej ochronie, jeżeli pośrednio ujawniają informację o osobie mającą charakter medyczno-zdrowotny. Zwrócił w tym miejscu m.in. uwagę na stanowisko Europejskiego Trybunału Sprawiedliwości [ETC], który dość szeroko rozumie pojęcie „danych o stanie zdrowia”.¹⁹⁰ Ponadto Generalny Inspektor odniósł się także do przepisu art. 9 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779 z późn. zm.), który wprowadza wskazuje, iż nadzór nad działalnością straży sprawuje wójt, burmistrz (prezydent miasta), a w zakresie fachowym – Komendant Główny Policji poprzez właściwego terytorialnie komendanta wojewódzkiego Policji, jednakże – jak zaznaczył – wydaje się, że nadzór prezydenta miasta nad strażą miejską powinien być prowadzony zasadniczo nad jej kwestiami organizacyjnymi. Organ do spraw ochrony danych osobowych wskazał także na koniec, iż administrator, udostępniając dane bez stosownej podstawy (którą może być m.in. przepis prawa albo pisemna zgoda osoby, której dane dotyczą), może narazić się na zarzut działania niezgodnego z przepisami o ochronie danych osobowych.

W okresie objętym sprawozdaniem Generalny Inspektor udzielił odpowiedzi na pytanie skierowane przez Ministerstwo Spraw Wewnętrznych i Administracji, które zwróciło się z prośbą o zajęcie stanowiska w kwestii wpływu jednego z orzeczeń Trybunału Sprawiedliwości Wspólnot Europejskich¹⁹¹ na stan polskiego ustawodawstwa.¹⁹²

W przedmiotowym orzeczeniu Trybunał Sprawiedliwości Wspólnot Europejskich [TSWE] stwierdził, iż art. 12 lit. a tiret 1 dyrektywy nr 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, nakłada na państwa członkowskie obowiązek stanowienia prawa

¹⁸⁷ DOLiS-035-311/09.

¹⁸⁸ Art. 27 ust. 2 pkt 2.

¹⁸⁹ Art. 27 ust. 2 pkt 1.

¹⁹⁰ ETS uznał np., że informacja o zranieniu się osoby fizycznej w stopę i przebywaniu na zwolnieniu lekarskim jest informacją o stanie zdrowia w rozumieniu art. 8 ust. 1 Dyrektywy 95/46/WE (Wyrok ETS z 20 listopada 2003 r. w sprawie Bodil Lindqvist, Zb. Orz. 2003, nr 11A, s. I-12971).

¹⁹¹ Orzeczenie TSWE z 7 maja 2009 r. w sprawie prejudycjalnej C-553/07 College van burgemeester en wethouders van Rotterdam przeciwko M.E.E. Rijkeboer.

¹⁹² DOLiS-072-10/09.

dostępu do informacji o odbiorcach lub kategoriach odbiorców dotyczących jej danych osobowych oraz treści przekazanych danych nie tylko w odniesieniu do teraźniejszości, lecz również w odniesieniu do przeszłości.¹⁹³ Dalej TSWE wskazał, że to do państw członkowskich należy określenie okresu przechowywania tych informacji oraz odpowiedniego do nich dostępu, który stanowiłby rezultat właściwego wyważenia między, z jednej strony, interesem osoby, której dane dotyczą, w ochronie jej życia prywatnego, w szczególności za pośrednictwem prawa interwencji oraz prawa do wniesienia środka prawnego, przewidzianych przez dyrektywę nr 95/46/WE, a z drugiej strony – obciążeniem, jakie obowiązek przechowywania tej informacji stanowi dla administratora danych. Uregulowanie ograniczające przechowywanie informacji o odbiorcach lub kategoriach odbiorców danych podstawowych oraz treści przekazanych danych do okresu jednego roku i ograniczające odpowiednio dostęp do tej informacji, podczas gdy dane podstawowe są przechowywane znacznie dłużej, nie stanowi właściwego wyważenia interesów i obowiązków występujących w sprawie, chyba, żeby zostało wykazane, że dłuższe przechowywanie tej informacji stanowiłoby nadmierne obciążenie dla administratora danych.

Generalny Inspektor, zajmując stanowisko w zasygnalizowanej kwestii wskazał, iż analiza tez ww. orzeczenia prowadzi do konstatacji, iż dokonana przez Trybunał interpretacja prawa wspólnotowego nie rodzi konieczności podjęcia kroków celem zmian legislacyjnych w polskim porządku prawnym. Podkreślił, że obowiązująca na obszarze Rzeczypospolitej Polskiej ustawa o ochronie danych osobowych jest w pełni dostosowana do wymogów dyrektywy 95/46/WE. Ustawa ta przewiduje w art. 33 ust. 1 uprawnienie dla osoby, której dane dotyczą, do uzyskania od administratora jej danych m.in. informacji o tym, jakie dane osobowe zawiera prowadzony przez niego zbiór, w jaki sposób zebrano dane, w jakim celu i zakresie dane są przetwarzane i w jakim zakresie oraz komu dane zostały udostępnione. Nie zawęży więc w tak radykalny sposób (poprzez posługiwanie się konkretnym terminem), jak ma to miejsce w przypadku przywoływanych w orzeczeniu przepisów niderlandzkich, możliwości skorzystania przez osobę, której dane dotyczą, z jednego z podstawowych uprawnień wynikających z ustawy o ochronie danych osobowych. Zdaniem GODO, uznać należy, że wykonanie uprawnienia konkretnych osób, których dane są przetwarzane, wyznacza moment ich pozyskania oraz zaprzestania ich przetwarzania. Generalny Inspektor przytoczył w treści swej opinii brzmienie art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych, statuującego tzw. zasadę ograniczenia czasowego.¹⁹⁴ Uznał, iż po osiągnięciu celu przetwarzania danych

¹⁹³ Zgodnie z art. 12 lit. a tiret 1 dyrektywy, państwa członkowskie zapewniają każdej osobie, której dane dotyczą prawo do uzyskania od administratora danych bez ograniczeń, w odpowiednich odstępach czasu oraz bez nadmiernego opóźnienia lub kosztów, potwierdzenia, czy dotyczące jej dane osobowe są przetwarzane oraz co najmniej o celach przetwarzania danych, kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane.

¹⁹⁴ Na podstawie art. 26 ust. 1 pkt 4 ustawy, 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

(np. po ustaniu określonej umowy łączącej administratora danych i podmiot tych danych) – z uwzględnieniem terminów wynikających ze szczególnych przepisów prawa – dane powinny być usuwane.

Zatem w polskim porządku prawnym istnieje podkreślana w tezach orzeczenia Trybunału Sprawiedliwości Wspólnot Europejskich równowaga pomiędzy interesem osoby, której dane dotyczą, w ochronie jej życia prywatnego a z drugiej strony – obciążeniem, jakie obowiązek przechowywania tej informacji niesie dla administratora danych. Wyważenie powyższych praw następuje poprzez powołaną zasadę ograniczenia czasowego oraz przepisy innych aktów prawnych wprowadzających obowiązek przechowywania danych osobowych – w zależności od zadań podmiotu znajdującego się w ich posiadaniu – przez odpowiednio długi okres. Generalny Inspektor stwierdził, iż o prawidłowym stosowaniu tez zawartych w orzeczeniu będzie zatem można mówić w szczególności wtedy, gdy administratorzy danych będą - na żądanie osoby, której dane dotyczą - dopełniać obowiązek informacyjny wynikający z art. 33 ust. 1 ustawy o ochronie danych osobowych, w całym okresie przetwarzania przez nich jej danych osobowych.

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**. W jednej z takich spraw do organu ds. ochrony danych dotarły sygnały, że w kilku centrach handlowych ma miejsce praktyka polegająca na zatrzymywaniu dowodu tożsamości klienta w sytuacji wypożyczania wózka – koszyka (samochodzika) służącego do przewozu dziecka na terenie centrum handlowego.

W kolejnej sprawie Generalny Inspektor uzyskał informację o stosowaniu przez jeden z banków telefonicznego potwierdzania prawdziwości podanych przez kredytobiorców danych osobowych u ich pracodawców. W związku z powyższym zwrócił się do jego prezesa o odstąpienie od wskazanej praktyki jako mogącej prowadzić do naruszenia przepisów zarówno ustawy o ochronie danych osobowych, jak i ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.).¹⁹⁵ Z treści pozyskanej przez GIODO informacji wynikało, iż pracownik banku zwrócił się telefonicznie do pracodawcy przyszłego kredytobiorcy w celu „potwierdzenia prawdziwości podanych przez potencjalnego kredytobiorcę danych”, pomimo tego, iż wcześniej osoba wnioskująca o kredyt złożyła w banku podpisane stosowne zaświadczenie o zarobkach z imiennymi pieczętkami oraz pieczętką firmową pracodawcy. Z uwagi na to, że pracownik pracodawcy nie miał możliwości zidentyfikowania, kto do niego dzwoni i odmówił udzielenia informacji, to w konsekwencji bank odmówił wydania wnioskodawcy karty kredytowej.

były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania.

¹⁹⁵ Wystąpienie GIODO z dnia 18 czerwca 2009 r. DOLiS-035-305/09.

Generalny Inspektor zaznaczył, iż w przypadku telefonicznej weryfikacji danych osoby występującej z wnioskiem o przyznanie kredytu u pracodawcy tej osoby może dojść do udostępnienia danych osobowych pracownika osobie nieupoważnionej. Pracodawca potencjalnego kredytobiorcy, w trakcie rozmowy telefonicznej, nie może zidentyfikować osoby telefonującej do niego w celu zweryfikowania danych, a zatem ustalić, czy rzeczywiście osoba ta jest przedstawicielem banku upoważnionym do pozyskania informacji na temat pracownika. Nie można wszak wykluczyć sytuacji, w której za przedstawiciela banku podawać się będzie osoba trzecia, nieupoważniona do uzyskania tego rodzaju danych osobowych. Generalny Inspektor zwrócił przy tym uwagę na konieczność każdorazowego dopełniania przez administratora danych ciążącego na nim obowiązku zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym.¹⁹⁶ Podkreślił również, iż brak wywiązywania się z tego obowiązku może w konsekwencji prowadzić do naruszenia przepisów karnych ustawy o ochronie danych osobowych.¹⁹⁷

Generalny Inspektor podkreślił także, iż kwestia telefonicznego potwierdzania prawdziwości podanych przez kredytobiorcę danych, w analizowany sposób, jako działania naruszającego przepisy prawa, była przedmiotem wystąpienia tego organu do Przewodniczącego Komisji Nadzoru Bankowego. W związku z powyższym, Generalny Inspektor Nadzoru Bankowego skierował do prezesów banków pismo,¹⁹⁸ w którym wskazał, iż art. 70 ust. 1 Prawa bankowego zobowiązuje do przedłożenia w banku dokumentów i informacji określonych przez bank jako niezbędne do oceny zdolności kredytowej, zaś kierowanie przez bank pytań do osoby lub osób niebędących kredytobiorcą, wykracza poza dyspozycję tego przepisu i traktowane jest jako naruszenie prawa. Przewodniczący Komisji Nadzoru Bankowego wskazał, iż przepisy Prawa bankowego i ustawy o ochronie danych osobowych nie przewidują telefonicznej formy pozyskiwania informacji. Banki nie mogą więc uzależniać przyznania kredytu od udzielenia informacji w tej formie. Udzielanie drogą telefoniczną informacji stanowiących źródło oceny zdolności kredytowej kredytobiorcy wiąże się z dodatkowym niebezpieczeństwem przekazania informacji osobie nieuprawnionej. Nie ma bowiem możliwości potwierdzenia tożsamości rozmówcy.

Warto przytoczyć przykład pytania, które do GIODO przesłane zostało w związku z wątpliwościami, czy portal internetowy może publikować zdjęcia samochodów z widoczną tablicą rejestracyjną.¹⁹⁹ Powyższe zagadnienie nabiera ostatnio szczególnego znaczenia nie tylko wobec coraz częściej stosowanego monitoringu za pomocą kamer, ale także wobec działalności wielu podmiotów, np. portali internetowych, które publikują na stronach www, których są administratorami, zapisy

¹⁹⁶ Art. 36 ust. 1 ustawy o ochronie danych osobowych.

¹⁹⁷ Art. 51 ustawy o ochronie danych osobowych.

¹⁹⁸ Pismo GINB z 6 kwietnia 2001 r. znak: NB/BPN/I/214/01.

z kamer w celu propagowania pewnych miejsc na mapie kraju. W tej sprawie Generalny Inspektor Ochrony Danych Osobowych wskazał, iż zdjęcia samochodów z widoczną tablicą rejestracyjną, bez żadnych dodatkowych informacji, nie w każdym przypadku, niemniej jednak mogą prowadzić do identyfikacji osoby fizycznej. W związku z tym, w określonych okolicznościach posługiwanie się taką informacją, jak numer rejestracyjny samochodu, może prowadzić do naruszenia prywatności, a to z kolei skutkować naruszeniem dóbr osobistych na gruncie przepisów ustawy Kodeks cywilny. Zgodnie natomiast z definicją zawartą w art. 6 ustawy o ochronie danych osobowych, za dane osobowe uznaje się zarówno takie informacje, które pozwalają bezpośrednio na określenie tożsamości konkretnej osoby, jak również takie, które nie pozwalają na jej natychmiastową identyfikację, są jednakże przy pewnym nakładzie kosztów, czasu lub działań wystarczające do jej ustalenia. Poza zakresem przedmiotowej definicji znajdują się natomiast takie informacje, na podstawie których nie można ustalić tożsamości osoby oraz takie, na podstawie których wprawdzie można byłoby ją zidentyfikować, lecz wymagałoby to nadmiernych kosztów, czasu lub działań. Dlatego na administratorze danych spoczywa obowiązek²⁰⁰ każdorazowego wyważania, czy przetwarzane przez niego informacje, np. w postaci zdjęć samochodów, mogą w określonych okolicznościach stać się informacjami, którym należałoby nadać przymiot danych osobowych, bowiem to on odpowiada za legalność przetwarzania danych.

Wśród nadawców pytań odnoszących się do legalności stosowania rozwiązań ustawy o ochronie danych osobowych były też podmioty mające swoją siedzibę poza granicami Polski. Na uwagę zasługuje wątpliwość podmiotu gospodarczego, który będąc polskim oddziałem podmiotu mającego siedzibę poza granicami Rzeczypospolitej Polskiej, przechowuje swoje zasoby informatyczne w kraju trzecim, niebędącym członkiem Unii Europejskiej.²⁰¹ Generalny Inspektor Ochrony Danych Osobowych wyjaśnił, iż przepisy ustawy o ochronie danych osobowych znajdują zastosowanie zarówno do osób fizycznych, jak i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych – które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej. Dodatkowo podkreślił, że zgodnie z art. 85 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (tekst jednolity: Dz. U. z 2007 r. Nr 155, poz. 1095) dla wykonywania działalności gospodarczej na terytorium Rzeczypospolitej Polskiej przedsiębiorcy zagraniczni mogą, na zasadzie wzajemności, o ile ratyfikowane umowy międzynarodowe nie stanowią inaczej, tworzyć oddziały

¹⁹⁹ DOLiS-1505/09.

²⁰⁰ Zgodnie z treścią art. 7 pkt 4 ustawy o ochronie danych osobowych – jest nim organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.

z siedzibą na terytorium Rzeczypospolitej Polskiej. W konsekwencji, do przetwarzania danych w tej sytuacji zastosowanie znajdują przepisy polskiej ustawy o ochronie danych osobowych.

Jako że działalność podmiotu pytającego ma mieć formę portalu społecznościowego, Generalny Inspektor wskazał także, narodowość użytkowników projektowanego portalu nie ma żadnego znaczenia z uwagi na fakt, że ustawa przyznaje ochronę danym osobowym każdej osoby (art. 1 ustawy). Z pisma zainteresowanego podmiotu wynikało także, iż będzie on przeprowadzał konkursy dla użytkowników, a w związku z tym ma wątpliwości odnośnie do podstawy prawnej przetwarzania danych osobowych w trakcie ich przeprowadzania. Wskazano pytającemu, iż za podstawę legalizującą przetwarzanie danych osób biorących udział w konkursie należy uznać zgodę osób, których dane dotyczą, tj. przesłankę, o której mowa w pkt 1 art. 23 powołanego powyżej artykułu. Zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści i musi z jej treści wynikać (w sposób niebudzący wątpliwości), w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane.

Kolejny aspekt omawianego pytania dotyczył kwestii „doraźności” powstałego w trakcie działalności tego podmiotu zbioru danych osobowych.²⁰² Odnośnie do oceny tego, czy prowadzony zbiór można uznać za zbiór doraźny, Generalny Inspektor wskazał pytającemu, iż mimo że pojęcie „doraźności” nie zostało zdefiniowane w ustawie o ochronie danych osobowych, to jednak poprzez odwołanie się do konkretnych okoliczności faktycznych towarzyszących przetwarzaniu danych, przez konkretnego administratora, dla określonych, precyzyjnie wskazanych celów, można przypisać określonemu zbiorowi tę właśnie cechę. Przy ocenie tego faktu istotną rolę będzie odgrywał czynnik czasu, w ciągu którego są przetwarzane dane osobowe. Poza tym konieczne jest rozważenie celu (zadań), któremu służyć ma przetwarzanie danych w określonej strukturze. O ile pierwszy z tych czynników (czas) nie jest z oczywistych powodów ściśle, ustawowo określony (tzn. trudno o wskazanie ścisłych czasowych granic zbioru doraźnego), o tyle pojęcie doraźności musi być uzależnione od celu przetwarzania danych w zbiorze. Jeżeli dane tworzące określoną strukturę służą realizacji zasadniczego, głównego celu przetwarzania, trudno uznać tę strukturę za zbiór doraźny. Nie zmienia tego okoliczność, iż okres jej przetwarzania jest relatywnie krótki.

W związku z pozyskaniem informacji, iż spośród kilku warunków skorzystania ze zbiorów znajdujących się w czytelni jednej z bibliotek było pozostawienie dyżurnemu bibliotekarzowi dowodu tożsamości, Generalny Inspektor Ochrony Danych Osobowych wystąpił do tej biblioteki, o podjęcie działań mających na celu zmianę dotychczasowej praktyki. Wskazał przy tym warunki legalności

²⁰¹ DOLiS-035-1778-09.

²⁰² Ma to znaczenie o tyle, że zgodnie z treścią art. 2 ust. 3 ustawy o ochronie danych osobowych, w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 (Zabezpieczenie danych osobowych) tej ustawy.

przetwarzania danych osobowych, zaznaczając, że w odniesieniu do danych zwykłych zależą one od spełnienia przez podmiot przetwarzający te dane, jednej z przesłanek określonych w art. 23 ust. 1 ustawy. Natomiast w sytuacji, gdy podmiot przetwarzający dane nie legitymuje się żadną z przesłanek określonych w pkt. 2–5 ww. przepisu, pozyskanie danych jest możliwe wyłącznie po uzyskaniu zgody osoby, której dane dotyczą (art. 23 ust. 1 pkt 1 ustawy). Odnosząc się do tej sprawy, GODO zwrócił uwagę, iż wprawdzie ustawa z dnia 27 czerwca 1997 r. o bibliotekach (Dz. U. z 1997 r. Nr 85, poz. 539 z późn. zm.) określa, iż zadania, organizację oraz szczegółowy zakres działania biblioteki wchodzącej w skład innej jednostki organizacyjnej określa regulamin nadany przez kierownika tej jednostki, zaś zgodnie z pkt. 3 lit. e regulaminu korzystania ze zbiorów tej biblioteki w czytelni obowiązani są pozostawić dyżurnemu bibliotekarzowi dowód tożsamości (legitymację ze zdjęciem, dowód osobisty, paszport, prawo jazdy itp.), to jednak należy mieć na względzie, iż wskazany regulamin nie może stać w opozycji do obowiązujących przepisów z zakresu ochrony danych osobowych. Generalny Inspektor wskazał na zasadę adekwatności wynikającą z art. 26 ust. 1 pkt 3 ustawy i wyjaśnił, że administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Relewantność (adekwatność) danych powinna być oceniana najpóźniej w momencie ich zbierania. Zatem administrator ma obowiązek dokonania w tym względzie oceny. Zakres danych osobowych adekwatnych do celu przetwarzania oceniać trzeba każdorazowo z uwzględnieniem określonego stosunku prawnego, w związku z którym administrator przetwarza dane osobowe.²⁰³ Ponadto Generalny Inspektor zwrócił uwagę, iż art. 33 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.) stanowi, że dowodu osobistego nie wolno zatrzymywać, z wyjątkiem przypadków określonych w ustawie. Zatrzymanie zaś cudzego dowodu osobistego stanowi wykroczenie stypizowane w art. 55 pkt 2 wyżej powołanej ustawy, zgodnie z którym, kto zatrzymuje cudzy dowód osobisty, podlega karze ograniczenia wolności do 1 miesiąca albo karze grzywny. Odpowiadając na powyższe zastrzeżenia organu do spraw ochrony danych osobowych, administrator danych poinformował wstępnie o podjętych w tym zakresie działaniach (wydanych „decyzjach i zarządzeniach”), w efekcie czego został zobligowany przez Generalnego Inspektora do podania szczegółów zastosowanych rozwiązań.

6.2. Działalność informacyjna

W celu podnoszenia wiedzy z zakresu ochrony danych osobowych, Generalny Inspektor, stawiający edukację jako jeden z priorytetów swojej działalności, tak jak w latach ubiegłych, również w 2009 r. korzystał z pośrednictwa mediów (prasa, radio, telewizja, agencje informacyjne i portale

²⁰³ Wyrok NSA z 27 listopada 2003 r. II SA 209/2003.

internetowe) oraz wszelkich innych form propagowania wiedzy o ochronie danych osobowych. Organizował konferencje prasowe i akcje informacyjne, udzielał wywiadów, odpowiadał na indywidualne pytania dziennikarzy, jak też z własnej inicjatywy przekazywał najistotniejsze informacje wymagające nagłośnienia. Na bieżąco zamieszczał też i aktualizował informacje zawarte na stronie internetowej (www.giodo.gov.pl) będącej jednocześnie Biuletynem Informacji Publicznej. 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. Duży krąg odbiorców informacji zapewniły również publikacje książkowe, szkolenia oraz konferencje naukowe.

Upowszechniane i udostępniane przez GIODO materiały edukacyjne i informacyjne obejmowały m.in. interpretacje 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. Zainteresowani mogli zapoznać się również z podejmowanymi w indywidualnych sprawach rozstrzygnięciami oraz z informacjami dotyczącymi działalności GIODO na arenie międzynarodowej.

6.2.1 Współpraca ze środkami masowego przekazu

1. Stałe kontakty z mediami

W celu upowszechniania wiedzy o ochronie danych osobowych GIODO – wzorem lat ubiegłych – w roku 2009 kontynuował stałą współpracę z prasą o zasięgu ogólnopolskim, przede wszystkim zaś z „Rzeczpospolitą”, „Gazetą Prawną”, „Gazetą Samorządu i Administracji” („GSiA”), „Bezpieczeństwem w Szkole”, „Tiną” oraz „Twoim Imperium”, a także nawiązał stałe kontakty z takimi pismami, jak „Przyjaciółka”, „Kadry w Urzędzie”, „Serwis Prawno-Pracowniczy”, „Przegląd Komunalny” czy „Computerworld”. Regularnie współpracował też z takimi redakcjami portali internetowych, jak Dziennik Internautów (di.com.pl) czy należący do Wydawnictwa Wiedza i Praktyka portal kadrowy (www.portalkadrowy.pl).

W 2009 r. rozszerzona została współpraca z „Gazetą Prawną”, dzięki czemu decyzje, wyjaśnienia i interpretacje organu ds. ochrony danych osobowych były częściej publikowane na łamach tego dziennika.

Z kolei w „Gazecie Samorządu i Administracji” w 2009 r. zamieszczane były nie tylko wyjaśnienia GIODO dotyczące ochrony danych osobowych w jednostkach samorządu terytorialnego, lecz także informacje o działalności Generalnego Inspektora w formie oddzielnych ogłoszeń. Ponadto współpraca z „GSiA” dotyczyła upowszechniania informacji i wyjaśnień przekazywanych podczas prowadzonych przez GIODO szkoleń dla jednostek samorządu terytorialnego.

Dzięki stałej współpracy z tak wieloma, różnorodnymi, wymienionymi wyżej mediami, na ich łamach cyklicznie ukazywały się artykuły poświęcone ochronie danych osobowych. W 2009 r. łącznie opublikowano ich ponad **160**.

Żeby upowszechnić efekty tej współpracy odzwierciedlającej najistotniejsze problemy związane z ochroną danych osobowych, Generalny Inspektor zamieszczał na swojej stronie internetowej – po uzgodnieniu z redakcjami – wszystkie powstałe w ten sposób doniesienia medialne.

Upowszechnianiu informacji dotyczących ochrony danych osobowych służyło też nagrywanie przez Generalnego Inspektora Ochrony Danych Osobowych kolejnych audycji radiowych z cyklu „Chroń swoje dane osobowe!”. Rozgłoszenie zainteresowane ich emisją mogły bezpłatnie pobierać ze strony internetowej GODO.

2. Odpowiedzi na indywidualne pytania dziennikarzy

Stałą formą kontaktów GODO z dziennikarzami było udzielanie im odpowiedzi na przesłane pytania dotyczące ochrony danych osobowych.

W 2009 r. GODO udzielił – pisemnie lub telefonicznie – około **320** takich odpowiedzi.

Wśród problemów, z którymi najczęściej zgłaszali się przedstawiciele mediów, były m.in.:

- funkcjonowanie portali społecznościowych,
- zasady przetwarzania danych osobowych dłużników,
- zakres danych pozyskiwanych przez przewoźników, zwłaszcza na potrzeby wystawienia biletów elektronicznych lub internetowej rezerwacji biletów,
- upublicznianie zdjęć złodziei lub osób źle parkujących pojazdy,
- ochrona danych osobowych w procesie rekrutacji i w zatrudnienia,
- odpowiedzialność za wyciek danych osobowych,
- dopuszczalność pozyskiwania danych biometrycznych,
- zasady przetwarzania danych osobowych przez placówki medyczne,
- zabezpieczanie danych osobowych,
- zasady wykorzystywania danych osobowych na potrzeby marketingu,
- upubliczniania danych przez jednostki samorządu terytorialnego zarówno w BIP, jak i w podejmowanych uchwałach czy decyzjach.

3. Wywiady i wystąpienia

W celu popularyzacji zagadnień z zakresu ochrony danych osobowych GODO udzielał wywiadów i brał udział w programach radiowych i telewizyjnych. GODO w 2009 r. udzielił blisko **150** wywiadów. Ich tematyka dotyczyła zarówno ogólnych zasad ochrony danych osobowych określonych w ustawie o ochronie danych osobowych, jak i rozwiązań ustanowionych przepisami branżowymi.

Szczególne zainteresowanie mediów budziło m.in. przetwarzanie danych osobowych na potrzeby zatrudnienia, w sektorze ubezpieczeniowym, bankowym, marketingowym, mieszkalnictwa, oświaty i służby zdrowia. Wiele wywiadów i wystąpień odnosiło się też do kwestii ochrony danych osobowych w kontekście rozwoju nowoczesnych technologii. Częstymi tematami dla przykładu można wymienić, dopuszczalność tworzenia profili behawioralnych, cyberprzestępczość, zatrzymywanie i przetwarzanie przez operatorów publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych danych pozyskanych w związku ze świadczeniem ww. usług łączności. Częstym tematem wywiadów było też przetwarzanie danych osobowych przez pracodawców, w tym wykorzystywanie informacji zamieszczanych na portalach społecznościowych, pobieranie odcisków palców na potrzeby rejestracji czasu pracy, przeprowadzanie testów psychologicznych czy monitorowanie poczty e – mailowej pracowników. Tworzenia przez GUS megabazy na potrzeby spisu powszechnego ludności i mieszkań w 2011 r. w kontekście właściwej ochrony danych osobowych to kolejny częsty temat wystąpień medialnych GIODO. Pod koniec 2009r. duże zainteresowanie mediów budziła kwestia zapowiadanego zaprzestania wydawania legitymacji ubezpieczeniowych i potwierdzania prawa do bezpłatnej opieki zdrowotnej m.i. poprzez przedłożenie druku RMUA.

Media interesowały się również dopuszczalnością świadczenia przez firmę Google usługi Street View, zbyt szerokim zakresem danych pozyskiwanych od pasażerów przez Zarząd Transportu Miejskiego w Warszawie oraz propozycją sejmowej Komisji „Przyjazne Państwo”, by w punktach sprzedaży alkoholu montować kamery nagrywające osoby kupujące alkohol. Duże zainteresowanie dziennikarzy wywołała też sprawa umieszczenia na stronie internetowej Państwowej Komisji Wyborczej danych osobowych polityków, m.in. w zakresie imienia, adresu zamieszkania i numeru PESEL.

4. Konferencje prasowe

W związku z potrzebą nagłośnienia ważnych wydarzeń lub koniecznością publicznego zajęcia stanowiska w określonych sprawach, GIODO w 2009 r. zorganizował 4 konferencje prasowe, które poświęcone były:

- obchodom III Dnia Ochrony Danych Osobowych i podpisaniem Porozumienia pomiędzy GIODO a Związkiem Banków Polskich (28 stycznia 2009 r.).
- z planowanemu pozyskiwaniu przez GUS danych osobowych na potrzeby spisu powszechnego ludności i mieszkań w 2011 r. (10 marca 2009 r.).
- nieprawidłowościom w procesie przetwarzania danych osobowych pasażerów stwierdzonym podczas kontroli GIODO w Zarządzie Transportu Miejskiego w Warszawie (8 lipca 2009 r.),

- omówieniu opracowanej wspólnie z Sekretariatem Konferencji Episkopatu Polski Instrukcji „Ochrona danych osobowych w działalności Kościoła Katolickiego w Polsce” (23 września 2009 r.).

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

5. Akcje informacyjno – promocyjne

Szczególne wydarzenia czy informacje związane z tematyką ochrony danych osobowych są nagłaśnianie przez Generalnego Inspektora w formie specjalnych akcji informacyjno - promocyjnych. W 2009 r. dwa zagadnienia zostały rozpropagowane w ten właśnie sposób.

- W związku z przypadającym 28 stycznia Dniem Ochrony Danych Osobowych GIODO podjął działania związane z nagłośnieniem europejskich i polskich obchodów tego dnia, zwłaszcza tych związanych z tematem przewodnim uroczystości – tj. bezpieczeństwem danych osobowych w kontekście rozwoju nowoczesnych technologii. Podobnie jak w latach ubiegłych obchodom tego święta towarzyszyły liczne wydarzenia, jak spotkanie GIODO z eurodeputowanymi w Brukseli i uroczystości w siedzibie Stałego Przedstawicielstwa Rzeczypospolitej Polskiej przy Unii Europejskiej oraz Dzień Otwarty w Biurze GIODO, w czasie którego podpisane zostało Porozumienie pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych a Związkiem Banków Polskich w sprawie współpracy na rzecz poprawy poziomu ochrony danych osobowych. Obchody Dnia Ochrony Danych Osobowych były też okazją do organizacji przez GIODO oraz redakcję „Gazety Prawnej” debaty „Ochrona danych osobowych klientów banków, ze szczególnym uwzględnieniem bankowości elektronicznej”. Otrzymała się ona 14 stycznia 2009 r. w siedzibie redakcji „Gazety Prawnej”. Akcja informacyjna dotycząca Dnia Ochrony Danych Osobowych zaowocowała publikacją licznych artykułów prasowych i internetowych związanych z tematyką ochrony danych osobowych.

- W związku z obchodzonym od 11 do 18 października 2009 r. Tygodniem Zapobiegania Kradzieży Tożsamości w Biurze GIODO 14 października 2009 r. zorganizowany został Dzień Otwarty, podczas którego odbyły się wykłady ekspertów, a pracownicy Biura GIODO udzielali porad prawnych. Ponadto przeprowadzono konkursy z nagrodami. Z kolei w specjalnych wykładach eksperci wyjaśniali m.in.: jakie cyfrowe ślady, ułatwiające kradzież tożsamości, zostawiamy w sieci, jak zapewnić dzieciom bezpieczne korzystanie z Internetu oraz to, jak dane osobowe powinni chronić przedsiębiorcy.

Dodatkowo rozdane zostały opracowane przez GIODO materiały edukacyjno-informacyjne, w tym zestaw broszur z serii ABC ochrony danych osobowych.

Celem akcji było zwrócenie uwagi na problem kradzieży tożsamości, a zwłaszcza na jej przyczyny i konsekwencje, a dzięki temu podnoszenie wiedzy i świadomości w tym zakresie.

Dodatkowemu wzmocnieniu przekazu służyło zorganizowanie konferencji prasowej oraz rozesłanie do mediów specjalnych materiałów informacyjnych, co zaowocowało licznymi publikacjami prasowymi oraz wystąpieniami GIODO w radiu i telewizji.

- W 2009 r. GIODO wziął udział w europejskim konkursie na najlepsze praktyki w zakresie ochrony danych osobowych stosowane przez podmioty administracji publicznej, zorganizowanym przez Agencję Ochrony Danych Osobowych Regionu Madryt. Podjęte więc zostały działania mające na celu nagłośnienie nominacji GIODO do tej nagrody, a dzięki temu promowanie platformy eduGIODO, która była projektem zgłoszonym do udziału w tym konkursie.

6.2.2 Publikacje

Innowacyjną formą edukacji było wydawanie broszur z serii ABC ochrony danych osobowych. W 2008 roku Generalny Inspektor Ochrony Danych Osobowych ich druk rozpoczął we współpracy z Wydawnictwem Sejmowym, zaś w 2009 r. kontynuował realizację tego projektu z udziałem instytucji reprezentujących podmioty z określonych sektorów. Dzięki temu seria ABC ochrony danych osobowych została wzbogacona o nowe pozycje i na koniec 2009 r. obejmowała:

- „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 przetwarzania danych osobowych w sektorze bankowym”,
- „ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych”

(która dodatkowo została wytłoczona na płycie CD na potrzeby konferencji pt. „Bezpieczeństwo w Internecie”, zorganizowanej 16 czerwca 2009 r. przez Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie).

Ponadto w analizowanym roku sprawozdawczym trwały prace nad przygotowaniem do publikacji broszur poświęconych przetwarzania danych osobowych w sektorze marketingu i w sektorze oświaty.

6.2.3 Szkolenia, staże, wymiana pracowników

a) Szkolenia podmiotów zewnętrznych

W ramach działalności edukacyjnej organizowane były nieodpłatne **szkolenia** skierowane głównie do instytucji publicznych zgłaszających zainteresowanie problematyką z zakresu ochrony danych osobowych. Generalny Inspektor Ochrony Danych Osobowych przeprowadził szkolenia m.in.: kadry urzędniczej Sądu Apelacyjnego w Łodzi, pracowników Sądu Okręgowego w Częstochowie, kuratorów zawodowych Sądu Rejonowego i Sądu Okręgowego w Łodzi oraz Sądu Okręgowego w Nowym Sączu, dyrektorów oddziałów wojewódzkich Narodowego Funduszu Zdrowia, Rzeczników Praw Pacjentów, kadry kierowniczej i pracowników centrali NFZ, funkcjonariuszy celnych, przedstawicieli jednostek i komórek organizacyjnych Komendy Stołecznej Policji, naczelników w biurach i delegaturach dla dzielnic m. st. Warszawy, Administratorów Bezpieczeństwa Zbiorów Kancelarii Prezesa Rady Ministrów, dyrektorów departamentów Urzędu Komisji Nadzoru Finansowego i Urzędu Marszałkowskiego Województwa Małopolskiego, a także pracowników spółdzielni mieszkaniowych regionu toruńskiego.

W jednym ze szkoleń GIODO udział wzięli uczestnicy Forum Sekretarzy Samorządów Polski Południowej - liderzy reprezentujący Samorządowy Ośrodek Doradztwa Metodycznego i Doskonalenia Nauczycieli w Kielcach oraz Gliwicki Ośrodek Metodyczny w Gliwicach, w ramach programu pilotażowego *„Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”*.

Wśród podmiotów szkolonych przez Generalnego Inspektora Ochrony Danych Osobowych znaleźli się też pracownicy Ministerstwa Spraw Zagranicznych, Ministerstwa Infrastruktury, Ministerstwa Finansów, kadra kierownicza Kancelarii Sejmu RP i pracownicy Działu Stenogramów oraz Biura Prac Senackich Kancelarii Senatu RP.

W sumie w 2009 r. odbyło się 56 takich szkoleń, których wykaz znajduje się w załączniku nr 6. Ponadto Generalny Inspektor Ochrony Danych Osobowych przygotował specjalną ofertę bezpłatnych szkoleń z udziałem ekspertów Biura dla jednostek samorządu terytorialnego. Do skorzystania z niej zaproszone zostały wszystkie urzędy zainteresowane podnoszeniem kwalifikacji swoich pracowników w zakresie ochrony danych osobowych.

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych nawiązał współpracę z Biurem Edukacji m. st. Warszawy w zakresie przygotowania szkoleń dla dyrektorów placówek edukacyjnych i współpracy z nimi przy przygotowaniu materiałów edukacyjnych dla uczniów.

b) Szkolenia wewnętrzne pracowników Biura GIODO

Wzorem poprzednich lat, w roku 2009 organizowane były szkolenia wewnętrzne dla pracowników Biura GIODO, którymi objęto osoby nowo zatrudnione oraz tych pracowników Biura, którzy prowadzą szkolenia dla instytucji zewnętrznych. Tematyka szkoleń obejmowała takie zagadnienia, jak: geneza ochrony danych osobowych, prawa osób, których dane dotyczą, bezpieczeństwo i podstawowe zasady ochrony danych, platforma e-learningowa eduGIODO, status GIODO na tle organizacji i funkcjonowania organów władzy publicznej, organizacja i techniczne środki zabezpieczania danych, rejestracja zbiorów, podstawy prawne SIS, CIS i Europolu, europejskie standardy ochrony danych osobowych oraz przekazywanie danych do państw trzecich. Spośród tematów poruszanych na szkoleniach wewnętrznych wymienić należy także bezpieczeństwo danych osobowych przetwarzanych przy użyciu systemów informatycznych oraz sieci publicznej Internet (serwisy społecznościowe, poczta elektroniczna) i problem pojawiający się na gruncie przypisów o ochronie danych osobowych w związku z usługą Google Street View.

W celu podwyższania jakości wykonywanej pracy, pracownicy Biura GIODO uczestniczyli także w cyklicznych szkoleniach z zakresu wewnętrznego obiegu dokumentów e-SOD oraz w kursach języka angielskiego zorganizowanych w ramach unijnego programu LdV dla projektu wymian (PL/09/LLP-LdV/VETPRO/140419 „Wzmocnienie umiejętności pracowników Biura GIODO”).

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych nawiązał współpracę z Biurem Edukacji m. st. Warszawy w zakresie przygotowania szkoleń dla dyrektorów placówek edukacyjnych i współpracy z nimi przy przygotowaniu materiałów edukacyjnych dla uczniów.

c) Staże

W 2009 r. w Departamencie Orzecznictwa, Legislacji i Skarg odbywał praktykę aplikant radcowski III roku z Okręgowej Izby Radców Prawnych w Warszawie. Praktykant miał okazję zapoznać się z zagadnieniami dotyczącymi ochrony danych osobowych oraz ze specyfiką pracy w Biurze GIODO. Oprócz zadań wykonywanych na potrzeby DOLiS uczestniczył także w specjalnych - prowadzonych przez kadrę kierowniczą oraz pracowników Biura - szkoleniach organizowanych cyklicznie dla wszystkich nowo zatrudnionych pracowników.

d) Udział pracowników Biura GIODO w szkoleniach organizowanych przez jednostki zewnętrzne

Pracownicy Biura GIODO korzystali ze 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 2009 pracownicy Biura GIODO uczestniczyli w 4 takich szkoleniach.

e) Projekt partnerski realizowany w ramach Programu Leonardo da Vinci

W ramach Programu Leonardo da Vinci [LdV] będącego częścią Programu „*Uczenia się przez całe życie*” (*Lifelong Learning Programme*) realizowany jest projekt partnerski pt.: „*Zwiększanie świadomości w zakresie ochrony danych wśród przedsiębiorców funkcjonujących na rynkach Unii Europejskiej*” finansowany ze środków Unii Europejskiej.

Celem projektu jest dostarczenie materiałów edukacyjnych i szkoleniowych dla podmiotów podejmujących działalność w jednym z krajów uczestniczących w konsorcjum projektowym. Wszystkie kraje partnerskie uczestniczące w realizacji projektu wskazują na brak wyczerpujących i kompleksowych informacji dotyczących praktyk stosowania prawa ochrony danych osobowych w poszczególnych obszarach życia codziennego. Brak usystematyzowanej wiedzy wskazują zarówno podmioty reprezentujące różne sektory działalności gospodarczej i publicznej, jak i osoby fizyczne. Biorąc pod uwagę powyższe zidentyfikowane potrzeby konieczne jest podejmowanie wszelkich działań mających na celu upowszechnianie wiedzy dotyczącej problematyki ochrony danych osobowych, adresowanych do różnych grup odbiorców.

W planowanej na zakończenie projektu publikacji podjęte zostaną problemy ochrony danych w kontekście prowadzenia działalności gospodarczej, przeprowadzony zostanie przegląd praktyk stosowanych w poszczególnych krajach partnerskich w zakresie stosowania przepisów prawa ochrony danych osobowych, które mogą mieć bezpośredni wpływ na legalność i zgodność z przepisami wykonywanej działalności gospodarczej. Poruszone zostaną zagadnienia związane m.in. z obowiązkami i działaniami, które należy podjąć celem rejestracji i zabezpieczenia danych osobowych pracowników oraz dysponowaniem danymi na potrzeby działalności przedsiębiorstwa.

W rezultacie projekt ukierunkowany będzie na upowszechnianie wiedzy w zakresie ochrony danych osobowych w sposób umożliwiający efektywną i samodzielną naukę przez bezpośrednich adresatów przepisów prawa w tym obszarze w krajach partnerskich.

Realizacja projektu umożliwi:

- analizę i porównanie praktyk stosowania prawa o ochronie danych osobowych w krajach partnerskich,
- dotarcie z informacjami o ochronie danych osobowych do podmiotów gospodarczych podejmujących działalność za granicą,
- uświadomienie i poinformowanie wszystkich odbiorców, do których adresowana jest publikacja, o niezbędnych działaniach, prawach i obowiązkach przy rejestracji

przedsiębiorstwa w krajach partnerskich,

- wzmocnienie roli organów ochrony danych poszczególnych państw uczestniczących w projekcie w upowszechnianiu informacji do poszczególnych grup odbiorców,
- zintensyfikowanie współpracy między organami ochrony danych w różnych krajach członkowskich UE.

W dniach 5-6 listopada 2009 r. w siedzibie Biura GODO odbyło się pierwsze spotkanie konsorcjum partnerskiego realizującego ten projekt, tj. Generalnego Inspektora Ochrony Danych Osobowych z przedstawicielami Urzędu Ochrony Danych z Czech i Węgier. Projekt realizowany będzie w latach 2009-2011.

f) Ogólnopolski program: „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”

Inicjatywa ta ma na celu zwiększenie wiedzy uczniów i nauczycieli o zagadnienia związane z ochroną danych osobowych i prawem każdego człowieka do prywatności. Program zakłada współdziałanie na zasadzie partnerstwa dwóch samorządowych ośrodków doskonalenia zawodowego nauczycieli (z Kielc i z Gliwic) i Generalnego Inspektora Ochrony Danych Osobowych. Pilotaż ogólnopolskiego programu realizowany będzie w województwach śląskim i świętokrzyskim przy wykorzystaniu „dobrych praktyk” europejskich organów ochrony danych osobowych. Pilotaż składa się z dwóch etapów. W ramach I etapu, w okresie od 1 września 2009 r. do 30 czerwca 2010 r. przeszkolona zostanie kadra nauczycielska, tj. wychowawcy, nauczyciele, pedagodzy szkolni i bibliotekarze. Na tym etapie realizacji programu zorganizowana została konferencja organizacyjno-promocyjna w Gliwicach, 28 października 2009 r. Natomiast w II etapie pilotażu nastąpi włączenie zagadnień związanych z ochroną danych osobowych do tematyki zajęć szkolnych. Powstaną konspekty zajęć dla nauczycieli i uczniów, raport ewaluacyjny podjętych działań oraz edukacyjny program o zasięgu ogólnopolskim. Nauczyciele będą mogli korzystać z bezpłatnych szkoleń, konsultacji, materiałów dydaktycznych oraz wymiany doświadczeń. Honorowy patronat nad programem objęli Rzecznik Praw Dziecka i Prezydent Miasta Gliwice.

6.2.4 Konkursy

a) V edycja konkursu na najlepsze praktyki stosowane przez organy i instytucje publiczne

Generalny Inspektor Ochrony Danych Osobowych był jednym z kandydatów do zdobycia nagrody za nowatorskie rozwiązania w zakresie ochrony danych osobowych stosowane przez podmioty administracji publicznej w krajach, które podpisały Konwencję Rady Europy z 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. W piątej edycji

konkursu organizowanego przez Agencję Ochrony Danych Osobowych Regionu Madryt wysoko została oceniona platforma e-learningowa „eduGIODO” przygotowana przez Biuro Generalnego Inspektora Ochrony Danych Osobowych. W związku z tym, w dniu 4 lutego 2009 r., wizytę w Biurze GIODO złożyła ekipa filmowa z Hiszpanii w celu nagrania filmu o zgłoszonej do konkursu platformie e-learningowej *eduGIODO*. Film został zaprezentowany 18 lutego 2009 r. w Madrycie podczas „Europejskiego seminarium poświęconego najlepszym praktykom stosowanym przez organy i instytucje administracji publicznej w zakresie ochrony danych osobowych”. Seminarium było okazją do prezentacji 17 projektów dobrych praktyk, w tym projektu polskiego. Inicjatywa Agencji Ochrony Danych Osobowych Regionu Madryt ma na celu poszerzenie świadomości społecznej na temat najlepszych praktyk w zakresie ochrony danych, zaproponowanych i wprowadzonych dla przetwarzania danych osobowych przez jakiegokolwiek organ lub instytucję administracji publicznej w krajach, które podpisały wspomnianą Konwencję. Najlepsze praktykibrane pod uwagę przez komisję oceniającą dotyczyły różnych zagadnień, jak np. poprawa jakości danych osobowych, projektowanie skutecznych systemów przekazywania obywatelom informacji o zbieraniu danych osobowych, postępowanie w związku z wyrażeniem zgody przez osobę, której dane dotyczą, na przetwarzanie jej danych osobowych, bezpieczeństwo danych czy obowiązek zachowania tajemnicy. Coroczne przyznawanie tej nagrody przez madrycką Agencję stanowi formę propagowania idei ochrony prywatności i ma znaczący wpływ na poziom "kultury ochrony danych".

Polska platforma edukacyjno-informacyjna „eduGIODO” zyskała wysokie noty zarówno u członków jury, jak i pozostałych uczestników madryckiego spotkania. Nie zdobyła jednak głównej nagrody ze względu na to, że informacje na niej zamieszczone są dostępne jedynie w języku polskim.

b) III edycja konkursu plastycznego pt. „Ochrona danych osobowych we współczesnym świecie”

Rozwijanie zainteresowań związanych z problematyką ochrony danych osobowych i podnoszenie świadomości najmłodszych członków społeczeństwa stało się celem organizacji III edycji konkursu plastycznego „Ochrona danych osobowych we współczesnym świecie”. Jego adresatami były dzieci w wieku 12-16 lat, wychowankowie warszawskich placówek opiekuńczo-wychowawczych. Na konkurs przysłanych zostało 27 prac plastycznych od 25 podopiecznych następujących placówek:

- | | |
|---|-----------|
| - Dom Dziecka Zgromadzenia Sióstr Franciszkanek
Rodziny Maryi, ul. Klasyków 52/54 | - 3 prace |
| - Dom Dziecka Nr 1 im. Maryny Falskiej, Al. Zjednoczenia 34 | - 5 prac |
| - Zespół Ognisk Wychowawczych im. Kazimierza Lisieckiego
Dziadka, Ognisko Mokotów, ul. Grottgera 25a | - 5 prac |
| - Ośrodek Wsparcia Dziecka i Rodziny, Koło ul. Dalibora 1 | - 2 prace |
| - Zespół Ognisk Wychowawczych im Kazimierza Lisieckiego | |

Dziadka, Ognisko Bielany, ul. Broniewskiego 56a	-	2 prace
- Dom Dziecka Nr 4, ul. Łukowska 25	-	1 praca
- Pogotowie Opiekuńcze Nr 2, ul. Św. Bonifacego 81	-	1 praca
- Pogotowie Opiekuńcze Nr 1, ul. Dembińskiego 1	-	6 prac

Rozstrzygnięcie konkursu nastąpi w dniu 20 stycznia 2010 r. Natomiast wystawa prac plastycznych oraz uroczyste wręczenie nagród odbędzie się podczas Dnia Otwartego z okazji obchodów IV Dnia Ochrony Danych Osobowych 28 stycznia 2010 r. „Masz prawo do prywatności w Internecie”.

c) Wyniki II edycji 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 i zwiększenie zainteresowania absolwentów szkół wyższych tą problematyką. Autorzy i promotorzy mogli zgłaszać do konkursu prace magisterskie i licencjackie obronione w latach 2004/2005, 2005/2006, 2006/2007 i 2007/2008. Laureatem najlepszej pracy magisterskiej z zakresu ochrony danych osobowych został absolwent Uniwersytetu Warszawskiego. Nagrodą był miesięczny płatny staż w Kancelarii Wierzbowski Eversheds. Uroczystość wręczenia nagród odbyła się 25 maja 2009 r. w Warszawie.

6.2.5 Konferencje, seminaria, spotkania

W roku sprawozdawczym 2009 Generalny Inspektor Ochrony Danych Osobowych zarówno organizował konferencje i seminaria, jak i brał aktywny udział w konferencjach zorganizowanych przez inne podmioty.

1. Seminarium „Tajemnica statystyczna w postępowaniu karnym. Między dobrem wymiaru sprawiedliwości a wiarygodnością danych statystycznych” (Kraków, 15 stycznia 2009 r.).

Organizatorami seminarium byli Główny Urząd Statystyczny w Krakowie oraz Katedra Prawa Karnego Uniwersytetu Jagiellońskiego.

2. III Dzień Ochrony Danych Osobowych – 28 stycznia 2009 r.

W dniu 28 stycznia 2009 r. Generalny Inspektor Ochrony Danych Osobowych już po raz trzeci obchodził Europejski Dzień Ochrony Danych Osobowych ustanowiony przez Komitet Ministrów Rady Europy, jako że w tym dniu świętowana jest rocznica otwarcia do podpisu Konwencji 108 RE

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. Tematem przewodnim tegorocznych obchodów była ochrona danych osobowych w dobie rozwoju nowoczesnych technologii. Patronat nad obchodami Dnia Ochrony Danych Osobowych objęły takie media, jak: „Gazeta Prawna”, „Computerworld”, Dziennik Internautów i TVN Warszawa.

Choć Dzień Ochrony Danych Osobowych przypada 28 stycznia, to w 2009 r. jego obchody rozpoczęły się już 26 stycznia i trwały do 2 lutego 2009 r. W ramach obchodów Dnia Ochrony Danych Osobowych miały miejsce następujące wydarzenia:

- **spotkanie Generalnego Inspektora Ochrony Danych Osobowych w siedzibie Stałego Przedstawicielstwa RP przy Unii Europejskiej** (Bruksela, 26 stycznia 2009 r.) z posłami do Parlamentu Europejskiego, przedstawicielami Komisji Europejskiej oraz innych polskich i unijnych instytucji. W spotkaniu z Generalnym Inspektorem Ochrony Danych Osobowych udział wzięli: Peter Hustinx, Europejski Inspektor Ochrony Danych, Jego Ekscelencja Ks. prof. dr hab. Piotr Mazurkiewicz, Sekretarz Generalny Komisji Episkopatów Wspólnoty Europejskiej oraz Francisco Fonseca Murillo, Dyrektor ds. Sądownictwa Cywilnego, Praw Podstawowych i Obywatelstwa, Komisja Europejska.

- **obrazy Klubu Polskiego w Parlamencie Europejskim (Bruksela, 27 stycznia 2009 r.)**, podczas których GODO miał wystąpienie poświęcone bezpieczeństwu danych osobowych w Internecie,

- **Dzień Otwarty w Biurze GODO** (Warszawa, 28 stycznia 2009 r.), w ramach którego uczestnicy mieli okazję uzyskać informacje na temat ochrony danych osobowych oraz porady prawne. Wszyscy przybyli na Dzień Otwarty otrzymali broszury z cyklu „ABC ochrony danych osobowych”, ulotki o działalności Biura i zagrożeniach w Internecie, a także mogli zapoznać się z platformą edukacyjną eduGODO i najciekawszymi artykułami prasowymi dotyczącymi ochrony danych. Dzień Otwarty był ponadto okazją do przeprowadzenia konkursów wiedzy o bezpiecznym użytkowaniu Internetu, a najlepiej poinformowani uczestnicy otrzymali atrakcyjne nagrody. Odbyły się również dwa spotkania pracowników Biura GODO z dziećmi spędzającymi zimę w mieście. Na spotkaniach tych dzieci dowiedziały się o zagrożeniach czyhających w sieci i uzyskały wskazówki, jak bezpiecznie korzystać z Internetu podczas zabawy czy nauki. Spotkanie z nimi urozmaicone zostało projekcją filmu o tematyce związanej z tymi zagrożeniami oraz konkursem wiedzy o bezpiecznym użytkowaniu Internetu. Dzieci biorące udział w dyskusji zostały nagrodzone prezentami. Podczas Dnia Otwartego odbyła się też **konferencja Związku Banków Polskich pt. „Dobre praktyki przetwarzania danych osobowych w bankach - spojrzenie praktyków”**, podczas której podpisane zostało porozumienie o wspólnym działaniu GODO i Związku Banków Polskich na rzecz podnoszenia standardów ochrony danych osobowych i prawa do prywatności w działalności bankowej. Konferencję

otworzyli GIODO i Prezes ZBP, natomiast wykład pt. *Standardy ochrony danych osobowych a bezpieczeństwo klientów banków* wygłosił Zastępca Generalnego Inspektora Ochrony Danych Osobowych. Adresatami konferencji byli Prezesi Zarządów Banków - Członków ZBP oraz przedstawiciele Ministerstwa Finansów, Narodowego Banku Polskiego i Komisji Nadzoru Finansowego.

- **spotkanie Generalnego Inspektora Ochrony Danych Osobowych z przedsiębiorcami zrzeszonymi w Amerykańskiej Izbie Handlowej w Polsce** (Warszawa, 2 lutego 2009 r.) poświęcone bezpieczeństwu danych osobowych w Internecie.

3. **Konferencja „Monitoring wydatkowania wybranych funduszy publicznych”**

(Warszawa, 28 stycznia 2009 r.).

Na konferencji tej, zorganizowanej przez Fundację im. Stefana Batorego, głównym tematem dyskusji uczestników był konflikt między przepisami dotyczącymi dostępu do informacji publicznej a ochroną danych osobowych.

4. **Konferencja „Zarządzanie w oświacie – III edycja”** (Warszawa, 26 lutego 2009 r.).

Organizatorem III edycji tej ogólnopolskiej konferencji dla dyrektorów szkół ponadgimnazjalnych była Wyższa Szkoła Zarządzania i Prawa im. Heleny Chodkowskiej. Przedstawiciele Generalnego Inspektora Ochrony Danych Osobowych przedstawili uczestnikom problematykę związaną z ochroną danych osobowych w działalności szkoły średniej.

5. **Konferencja „Problemy edukacji prawno-informatycznej”** (Warszawa, 26 lutego 2009 r.).

Podczas tej konferencji zorganizowanej na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, w dyskusji panelowej na temat problemów edukacji prawno-informatycznej uczestniczył Zastępca Generalnego Inspektora Ochrony Danych Osobowych. Inicjatywa konferencji o problemach edukacji prawno-informatycznej jest związana między innymi z planowanym poszerzeniem oferty studiów podyplomowych i szkoleń związanych z wykorzystaniem narzędzi informatycznych w administracji publicznej i w sądach. Konferencja była też okazją do sformułowania koncepcji poszerzenia udziału uczelni w budowie społeczeństwa informacyjnego.

8. **XVIII Zwyczajne Zgromadzenie Członków Polskiej Izby Informatyki i Telekomunikacji. Konferencja 3.TeraForum** (Warszawa, 11 marca 2009 r.).

Podczas Konferencji Generalny Inspektor Ochrony Danych Osobowych w swoim wystąpieniu omawiał zagadnienia dotyczące ochrony danych osobowych w kontekście działalności teleinformatycznej. Jego przemówienie skoncentrowało się na wyzwaniach, jakie dla właściwej ochrony danych osobowych stwarza rozwój nowoczesnych technologii i podkreślał, że ustawa o ochronie danych osobowych jest i powinna pozostać zbiorem ogólnych zasad gwarantujących

obywatelom prawo do ochrony ich danych osobowych. Potrzebny jest natomiast dialog z przedstawicielami środowisk poszczególnych sektorów gospodarczych, którego rezultatem może być stworzenie kodeksu dobrych praktyk. Zdaniem GODO, ochronę danych osobowych należy postrzegać jako wartość istotnie zwiększającą konkurencyjność na rynku, gdyż budowanie zaufania klientów, szczególnie w gospodarce elektronicznej, w dużym stopniu jest uzależnione od spełnienia zasad ochrony danych osobowych.

9. **Kongres „Strategiczne Forum Liderów Marketingu, Mediów i Komunikacji”**
(Warszawa, 12-13 marca 2009 r.).

ECU Marketing wraz ze Stowarzyszeniem Marketingu Bezpośredniego byli organizatorami tego pierwszego w Polsce kongresu połączonego z targami marketingu zintegrowanego. W zamierzeniach organizatorów kongres ten stał się platformą komunikacji między firmami tworzącymi rynek marketingowy w Polsce a podmiotami, które dysponują konkretną i sprawdzoną wiedzą na temat tego, na czym powinny one oprzeć swoją przewagę konkurencyjną na rynku. Podczas kongresu 12 marca 2009 r. Generalny Inspektor Ochrony Danych Osobowych, jego Zastępca oraz - na zaproszenie GODO - András Jóri, Parlamentarny Rzecznik Ochrony Danych z Węgier, wzięli udział w dyskusji panelowej Effective Protection of Personal Data in Poland – the Consequences for the Marketing Sector.

10. **V edycja seminarium „Jakość danych w systemach informatycznych zakładów ubezpieczeń”** zorganizowanego przez Polską Izbę Ubezpieczeń (Warszawa, 25 marca 2009 r.).

Na seminarium prezentowane były zagadnienia dotyczące zarządzania systemami informatycznymi oraz działania ukierunkowane na uzyskanie wysokiej jakości danych w tych systemach. Prezentowane były również prace powołanej w sektorze ubezpieczeniowym Komisji ds. Standaryzacji Informacji oraz OBD PIU. Przedstawiciel GODO w swoim wystąpieniu pt. „Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną” zwrócił uwagę na różne podejścia do problemu określania warunków, jakie powinny spełniać systemy informatyczne oraz porównał wymagania określone w przepisach o ochronie danych osobowych oraz w przepisach o informatyzacji działalności podmiotów realizujących zadania publiczne z wymaganiami określonymi w normach międzynarodowych ISO/IEC, które stosowane są również w Polsce. Wskazał w szczególności na zalecenia dotyczące stosowania tych norm. Zwrócił uwagę na zalecenia określone w normie PN-ISO/IEC 17799:2005 oraz PN-ISO/IEC 27001, które mogą być wykorzystane jako przewodnik do sposobu realizacji obowiązku administratorów danych wynikających z art. 36 ustawy o ochronie danych osobowych oraz realizacji zadań określonych Rozporządzeniem 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. z 2004 r. nr 100, poz. 1024).

11. **III Konferencja „Call Contact Center– Bądźmy w kontakcie”** (Warszawa, 1 kwietnia 2009 r.). Obrady III Konferencji „Call Contact Center – Bądźmy w kontakcie” zorganizowanej przez tygodnik „Computerworld” koncentrowały się wokół istotnych problemów firm prowadzących telefoniczną sprzedaż i obsługę klienta. Wystąpienie przedstawiciela Biura GODO pozwoliło na przybliżenie uczestnikom konferencji istoty planowanych zmian w ustawie o ochronie danych osobowych.

12. **Sesja Naukowa X Konferencji Okrągłego Stołu pt. „Polska w drodze do Społeczeństwa Informacyjnego; bezpieczeństwo w warunkach powstającego Społeczeństwa Informacyjnego”** (Warszawa, 15 maja 2009 r.).

Stowarzyszenie Elektryków Polskich i Przemysłowy Instytut Telekomunikacji w ramach obchodów Światowego Dnia Telekomunikacji i Społeczeństwa Informacyjnego²⁰⁴ zorganizowali Konferencję Okrągłego Stołu. Honorowy patronat nad Konferencją sprawował Marszałek Sejmu - Bronisław Komorowski, zaś Minister Infrastruktury – Cezary Grabarczyk - objął patronatem honorowym całość obchodów Światowego Dnia Telekomunikacji i Społeczeństwa Informacyjnego w 2009 r. Konferencja miała charakter sesji naukowej poświęconej bezpieczeństwu w warunkach powstającego Społeczeństwa Informacyjnego, w ramach której poruszane były tematy związane z komputeryzacją systemów walki, dowodzenia i logistyki w nowoczesnej armii, wojskowe techniki dla bezpieczeństwa narodowego i obrony cywilnej, bezpieczeństwo sieciowe jako fundament bezpieczeństwa infrastruktury krytycznej, a także związane z tym aspekty prawne i moralne.

13. **III Konferencja „Holistyczne zarządzanie danymi osobowymi. Praktyka marketingu a zarządzanie danymi osobowymi”** zorganizowana przez Global Information Security Sp. z o.o. (Mikołajki, 21 maja 2009 r.).

W spotkaniu tym, w którym uczestniczyli Generalny Inspektor Ochrony Danych Osobowych i jego zastępca, przedstawione zostały zagadnienia związane z prawnymi aspektami działalności marketingowej w kontekście administrowania i zarządzania danymi osobowymi.

²⁰⁴ Zgodnie z decyzją przywódców państw podjętą w listopadzie 2005 r. w Tunisie podczas Światowego Szczytu Społeczeństwa Informacyjnego i postanowieniami konferencji Międzynarodowego Związku Telekomunikacyjnego (ITU) w 2006 r. (Antalaya, Turcja) postanowiono dzień 17 maja obchodzić na całym świecie jako „Światowy Dzień Telekomunikacji i Społeczeństwa Informacyjnego”. Data 17 maja upamiętnia utworzenie 17 maja 1865 r. Międzynarodowego Związku Telekomunikacyjnego (ITU), wyspecjalizowanej organizacji Narodów Zjednoczonych. W 2009 r. obchody Światowego Dnia Telekomunikacji i Społeczeństwa Informacyjnego przebiegały pod ogłoszonym przez Międzynarodowy Związek Telekomunikacyjny hasłem „Bezpieczeństwo dzieci w cyberprzestrzeni” i odbywały się od 12 do 15 maja 2009 r.

14. **V Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych Krajowego Stowarzyszenia Ochrony Informacji Niejawnych** (Kazimierz Dolny, 3 czerwca 2009 r.).

Tematyka Kongresu obejmowała najnowsze zagadnienia dotyczące ochrony danych w kontekście prawnych i praktycznych uwarunkowań związanych z ochroną informacji niejawnych, biznesowych oraz danych osobowych. W kongresie udział wzięł Zastępca GIODO, który zabrał głos w panelu tematycznym pt. „Aktualne problemy, wyzwania i zagrożenia ochrony informacji w firmie/instytucji w aspekcie bezpieczeństwa państwa”.

15. **Konferencja naukowa „Bezpieczeństwo w Internecie”** (Warszawa, 16 czerwca 2009 r.).

Organizatorem konferencji, nad którą honorowy patronat sprawował Generalny Inspektor Ochrony Danych Osobowych, był Dziekan Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Na konferencji przedstawiony został referat na temat portali społecznościowych w kontekście ochrony danych osobowych. W trakcie spotkania Generalny Inspektor Ochrony Danych Osobowych oraz Prorektor UKSW podpisali Porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych.

16. **Letnie konwersatorium nt. ochrony danych osobowych** zorganizowane przez Krajowe Stowarzyszenie Ochrony Informacji Niejawnych [KSOIN] w porozumieniu z Generalnym Inspektorem Ochrony Danych Osobowych (Kazimierz Dolny, 21 sierpnia 2009 r.).

Adresatami konwersatorium byli administratorzy danych osobowych [ADO], administratorzy bezpieczeństwa informacji [ABI] oraz kadra kierownicza i pracownicy działów przetwarzających dane osobowe. Celem konwersatorium było ugruntowanie wiedzy w zakresie przepisów dotyczących ochrony danych osobowych, a także doskonalenie umiejętności opracowania dokumentacji dotyczącej ochrony danych osobowych, opracowania i wdrażania polityki bezpieczeństwa, instrukcji zarządzania systemem informatycznym, wprowadzania niezbędnych zmian w jednostce organizacyjnej dostosowujących jej działania do wymagań prawnych z dziedziny ochrony danych osobowych oraz wymiana doświadczeń i uwag na temat roli, zadań i kompetencji ADO i ABI. Zajęcia programowe prowadzone były przez pracowników GIODO oraz innych ekspertów zajmujących się na co dzień ochroną danych osobowych i bezpieczeństwem informacji.

17. **III Konferencja „Bezpieczeństwo dzieci i młodzieży w Internecie”** (Warszawa, 29-30 września 2009 r.) zorganizowana przez Fundację Dzieci Niczyje oraz Naukową i Akademicką Sieć Komputerową.

To już trzecia edycja tej imprezy zorganizowanej w ramach programu Komisji Europejskiej „Safer Internet Plus” współfinansowanego ze środków Unii Europejskiej. Honorowy patronat nad konferencją objął Generalny Inspektor Ochrony Danych Osobowych, który wygłosił na niej wykład pt. „Portale społecznościowe a ochrona danych osobowych”. Z myślą o najmłodszych

użytkownikach Internetu opracowana została ulotka informacyjna „Ja i mój komputer jesteśmy bezpieczni”, która w przystępny sposób przedstawia podstawowe zasady bezpiecznego korzystania z sieci w obszarze „Mój bezpieczny komputer”, „Mój bezpieczny Internet”, „Moje bezpieczne dane”. W ulotce tej wykorzystane zostały rysunki uczniów warszawskich szkół podstawowych, którzy brali udział w I edycji konkursu plastycznego pt. „Prywatność wokół mnie” zorganizowanego przez GIODO w 2007 r.

18. **Cykl wykładów poświęconych problematyce ochrony danych osobowych, Wszechnica Polska Szkoła Wyższa Towarzystwa Wiedzy Powszechnej w Warszawie** (Warszawa, w okresie od 8 października 2009 r. do 7 lutego 2010 r.).

Na mocy porozumienia zawartego w dniu 4 sierpnia 2009 r. pomiędzy GIODO a Rektorem Wszechnicy Polskiej Szkoły Wyższej TWP o współpracy w zakresie ochrony danych osobowych i prawa do prywatności, w semestrze zimowym roku akademickiego 2009/2010 dyrektorzy Biura GIODO oraz ich zastępcy przeprowadzili 50 godzin zajęć na studiach stacjonarnych, kierunku „Bezpieczeństwo wewnętrzne”, 48 godzin na studiach niestacjonarnych, kierunku „Bezpieczeństwo wewnętrzne” i 20 godzin na studiach niestacjonarnych, kierunku „Administracja”. W sumie 118 godzin. Tematyka spotkań ze słuchaczami obejmowała takie zagadnienia, jak charakterystykę podstawowych pojęć ustawy o ochronie danych osobowych, przetwarzanie danych osobowych, zadania administratora danych oraz prawa podmiotu danych, rejestracja zbiorów danych osobowych, ochrona danych osobowych na forum Unii Europejskiej: podstawy prawne, zasady i ramy współpracy, kontrola przestrzegania przepisów ustawy o ochronie danych osobowych, techniczno-organizacyjne aspekty ochrony danych osobowych w systemach informatycznych, narzędzia i systemy informatyczne służące do przetwarzania danych osobowych.

19. **Tydzień Zapobiegania Kradzieży Tożsamości. Dzień Otwarty w Biurze GIODO** (Warszawa, 14 października 2009 r.).

W związku z obchodzonym w dniach 11-18 października 2009 r. Tygodniem Zapobiegania Kradzieży Tożsamości, w dniu 14 października 2009 r. w Biurze GIODO zorganizowany został Dzień Otwarty, podczas którego odbyły się wykłady ekspertów, konkursy z nagrodami, a także udzielane były bezpłatne porady prawne. Celem akcji było zwrócenie uwagi na problem kradzieży tożsamości, a zwłaszcza na jej przyczyny i konsekwencje, a dzięki temu podnoszenie wiedzy i świadomości w tym zakresie.

20. **VI Ogólnopolska Konferencja „Pomoc dzieciom – ofiarom przestępstw”** zorganizowana przez Fundację Dzieci Niczyje (Warszawa, 27 października 2009 r.).

Tematem przewodnim tej Konferencji było stworzenie ram prawnych i organizacyjnych niesienia pomocy dzieciom, które doświadczyły różnych form przemocy, a także ochrona praw dzieci

uczestniczących w procedurach prawnych. Prezentowane były projekty i inicjatywy praktycznej pomocy dzieciom – ofiarom przestępstw i ich rodzinom oraz profesjonalne wydawnictwa dotyczące tej problematyki. Przedstawiciel GIODO wziął udział w panelu dyskusyjnym „Ochrona danych osobowych a prawne ograniczenia możliwości pomocy dzieciom”.

21. **Konferencja informacyjno-promocyjna w ramach ogólnopolskiego programu „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”** (Gliwice, 28 października 2009 r.).

Adresatami Konferencji, nad którą honorowy patronat objęli Rzecznik Praw Dziecka i Prezydent Miasta Gliwice, byli przedstawiciele placówek oświatowych zainteresowanych problematyką ochrony danych osobowych i prywatności. Na spotkaniu tym, oprócz wystąpienia GIODO, grupie złożonej z 22 gimnazjalistów została zaprezentowana lekcja pokazowa na temat ochrony danych osobowych. Zajęcia zakończone zostały procedurą omówienia i ewaluacji.

22. **III edycja FORUM IAB 2009** (Warszawa, 4-5 listopada 2009 r.).

Organizatorem Forum był Związek Pracodawców Branży Internetowej IAB Polska, zaś patronat honorowy nad tym spotkaniem objął Minister Gospodarki. Forum IAB pokazało, jakim silnym medium jest w Polsce Internet. Na spotkaniach dyskutowane były przyszłe rozwiązania prawne mające wpływ na rozwój reklamy internetowej, w tym reklamy z wykorzystaniem serwisów społecznościowych i telewizji.

23. **VII Forum ADO/ABI „Outsourcing procesów przetwarzania danych osobowych”** zorganizowane przez Centrum Promocji Informatyki Sp. z o.o. (Warszawa, 17 listopada 2009 r.).

W programie spotkania znalazły się takie tematy, jak: pojęcie danych osobowych w świetle ostatnich stanowisk zajmowanych przez właściwe organy w Polsce i w innych krajach Unii Europejskiej, status podmiotów przetwarzających dane osobowe w grupach kapitałowych, wykreślenie z rejestru zbiorów, zagadnienia prawidłowego wykonania obowiązków dotyczących struktur baz danych oraz funkcjonalności zarządzających nimi aplikacji, powierzenie przetwarzania danych, outsourcing informatyczny a przetwarzanie danych osobowych, praktyczne aspekty outsourcingu funkcji administratora bezpieczeństwa informacji i inne. Na spotkaniu tym dyrektor Departamentu Informatyki Biura GIODO wygłosił referat pt. „Prawidłowe wykonanie obowiązków dotyczących struktur baz danych oraz funkcjonalności zarządzających nimi aplikacji – odnotowanie i raportowanie czynności związanych przetwarzaniem danych osobowych w systemie informatycznym (§ 7 rozporządzenia MSWiA z dnia 29.04.2004 r.).

24. **III Kongres Prawa Oświatowego** (Warszawa, 3 grudnia 2009 r.).

Na Kongresie tym, którego organizatorem był Instytut Badań w Oświacie, przedstawiona została prezentacja Generalnego Inspektora Ochrony Danych Osobowych pt. „Ochrona danych osobowych w oświacie.”

6.2.6 Internet

W roku 2009 nastąpiła gruntowna przebudowa serwisu informacyjnego Biura GIODO. Opracowano nowy układ graficzny serwisu wraz z nowym podziałem na sekcje informacyjne.

Modyfikacje polegały na:

- zmianie układu zawartości, która miała na celu poprawę przejrzystości i dostępności treści,
- modyfikacji treści,
- uruchomieniu nowych funkcjonalności,
- uproszczeniu sposobu przekazywania informacji,
- poprawie nawigacji.

Założeniem wprowadzonych zmian było stworzenie bardziej przyjaznej dla użytkowników strony internetowej, a także ułatwienie korzystania z niej.

Realizacja tego przedsięwzięcia wymagała od strony programowej wprowadzenia szeregu zmian w istniejących już modułach programowych, jak również opracowania wielu nowych modułów, np. modułu prezentacji strony głównej i systemu nawigacji, modułu prezentacji specyficznych podstron dla określonych rodzajów zestawów informacji (np. wyroków sądowych, decyzji GIODO, sygnalizacji GIODO itd.), a także opracowanie 4 nowych podstron tematycznych dla prezentacji grup tematycznych: „Jeśli chcesz złożyć skargę”, „Elektroniczna Skrzynka Podawcza”, „Rejestracja zbiorów danych osobowych” oraz „Porady i wskazówki”. Nowy podział na sekcje informacyjne wymagał ponadto przeprowadzenia zmian w strukturze bazy danych, opisie poszczególnych materiałów informacyjnych oraz opracowania nowych modułów prezentacji. W ramach aktualizacji treści serwisu internetowego Biura GIODO w 2009 r. zamieszczono 758 nowych artykułów oraz 339 załączników w postaci plików PDF. Dodatkowo dokonano 2546 modyfikacji istniejących już artykułów. Większość modyfikacji związana była ze zmianą przyporządkowania poszczególnych materiałów do właściwych sekcji informacyjnych.

W związku z bardzo dynamiczną rozbudową serwisu internetowego Biura GIODO, który na koniec 2009 r. zawierał blisko 2700 artykułów oraz blisko 1600 załączników, rozpoczęto pracę nad zaprojektowaniem i stworzeniem nowego bardziej elastycznego i wydajnego mechanizmu do prezentacji danych. Prace te obejmowały zmiany w konstrukcji głównego kontrolera systemu,

opracowanie nowego sposobu budowania linków oraz opracowanie funkcji tworzącej nawigację. Dodatkowo opracowano nowe funkcje obiektu „strona” i funkcji decydującej o układzie podstrony.

a) Elektroniczna Skrzynka Podawcza (ESP)

Na stronie internetowej GIODO od 2007 r. funkcjonuje Elektroniczna Skrzynka Podawcza, dzięki której system informatyczny Biura GIODO dostosowany został do wymogów Rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno–technicznych doręczania dokumentów elektronicznych podmiotom publicznym (Dz. U. Nr 200, poz. 1651). Zakupione 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 6 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 wskazanej przez GIODO,
- Inne podanie (wniosek).

Elektroniczna Skrzynka Podawcza [ESP-GIODO] jest środkiem komunikacji elektronicznej służącym do składania podań, wniosków i skarg do Generalnego Inspektora Ochrony Danych Osobowych w formie elektronicznej, przy wykorzystaniu powszechnie dostępnej sieci teleinformatycznej. ESP-GIODO automatycznie wytwarza urzędowe poświadczenie odbioru dokumentów elektronicznych, zgodnie z warunkami określonymi w ww. rozporządzeniu. Korzystanie z ESP-GIODO w zakresie niektórych spraw jest możliwe tylko dla tych interesantów, którzy posiadają bezpieczny podpis elektroniczny weryfikowany przy użyciu kwalifikowanego certyfikatu, o którym mowa w art. 5 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450 z późn. zm.), wywołujący skutki prawne określone ustawą. Na stronie internetowej GIODO znajduje się wykaz wniosków, które można składać za pośrednictwem ESP bez wymogu posiadania kwalifikowanego certyfikatu (tzn. nie wymagają podpisu elektronicznego).

W Biurze GIODO opracowany też został projekt modyfikacji formularzy udostępnianych w ramach Elektronicznej Skrzynki Podawczej oraz integracji systemów e-GIODO z ESP oraz ESP z ePUAP-em, tj. elektroniczną Platformą Usług Administracji Publicznej.²⁰⁵

²⁰⁵ ePUAP stanowi część projektu elektronicznej Platformy Usług Administracji Publicznej, realizowanego w ramach Centrum Projektów Informatycznych MSWiA. Zadaniem portalu jest udostępnianie informacji na temat usług publicznych

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

W roku 2009 dokonano kilku, bardzo istotnych z punktu widzenia funkcjonalności, modyfikacji platformy e-GIODO. Najważniejsze z nich to:

1. Wprowadzenie nowej wersji interaktywnego formularza wniosku zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, zmodyfikowanego stosownie do wzoru zgłoszenia opublikowanego w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. (Dz. U. z 2008 r. Nr 229, poz. 1536).
2. Wymiana komponentu służącego do elektronicznego podpisywania wysyłanych wniosków bezpośrednio w oknie przeglądarki z wersji uzależnionej technologicznie od środowiska Net Framework firmy Microsoft na wersję otwartą.
3. Wprowadzenie funkcjonalności wysyłania do administratorów przesyłających wnioski, tzw. Urzędowego Poświadczenia Przedłożenia [UPP]. Funkcjonalność ta została zrealizowana poprzez użycie do przekazywania wniosków wysyłanych z eGIODO narzędzi zastosowanych w Elektronicznej Skrzynce Podawczej.

c) Udział GIODO w pracach Komitetu Technicznego nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych

W roku 2009, podobnie jak w latach ubiegłych, Generalny Inspektor Ochrony Danych Osobowych uczestniczył w pracach Komitetu Technicznego nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych przy Polskim Komitecie Normalizacyjnym [PKN]. Działalność GIODO była zwrócona szczególnie na prace podejmowane przez Komitet JTC/SC27 w ramach grupy roboczej WG 5 - Identity management and privacy Technologies. W roku 2009 w ramach ww. komitetu KT-182 przygotowywano między innymi dziewięć projektów norm.

Poza udziałem w dyskusjach dotyczących uzgodnienia treści ww. norm, GIODO brał udział w wypracowaniu polskiego stanowiska w głosowaniu nad projektem normy ISO/IEC CD 24745 Information Technology – Security techniques – Biometric template protection, opracowanej w ramach prac Komitetu JTC/SC27 przez grupę roboczą WG 5.

6.2.7 Inne informacje

a) Porozumienie pomiędzy GIODO a Związkiem Banków Polskich

W ramach obchodów III Dnia Ochrony Danych Osobowych 28 stycznia 2009 r. odbyła się konferencja Związku Banków Polskich pt. „Dobre praktyki przetwarzania danych osobowych

realizowanych drogą elektroniczną. Informacje zawarte na portalu odnoszą się do formy organizacyjno-prawnej, możliwości systemu, sposobu korzystania oraz innych kwestii związanych z platformą.

w bankach– spojrzenie praktyków”, podczas której podpisane zostało **porozumienie GIODO ze Związkiem Banków Polskich na rzecz podnoszenia standardów ochrony danych osobowych i prawa do prywatności w działalności bankowej**. Podpisanie dokumentu stało się podstawą do rozpoczęcia zainicjowanego przez Generalnego Inspektora Ochrony Danych Osobowych procesu współpracy z sektorem bankowym w zakresie wprowadzenia dobrych praktyk przetwarzania danych osobowych w bankach i instytucjach kredytowych. Porozumienie podpisali Michał Serzycki - GIODO oraz Prezes ZBP - Krzysztof Pietraszkiewicz.

b) Porozumienie pomiędzy GIODO a JM Prorektorem Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

W dniu 16 czerwca 2009 r. w Warszawie, podczas obrad konferencji naukowej „Bezpieczeństwo w Internecie” zorganizowanej przez Dziekana Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, Michał Serzycki, Generalny Inspektor Ochrony Danych Osobowych oraz JM Prorektor UKSW ks. prof. dr hab. Henryk Skorowski podpisali *Porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych*, w którym zobowiązali się do współpracy w zakresie ochrony prywatności i danych osobowych.

c) Porozumienie pomiędzy GIODO a JM Rektorem Wszechnicy Polskiej Szkoły Wyższej Towarzystwa Wiedzy Powszechnej w Warszawie

W dniu 4 sierpnia 2009 r. Generalny Inspektor Ochrony Danych Osobowych podpisał Porozumienie ze Szkołą Wyższą Towarzystwa Wiedzy Powszechnej w Warszawie o współpracy w zakresie ochrony danych osobowych i prawa do prywatności. Zgodnie z Porozumieniem, na uczelni będą prowadzone zajęcia z ochrony danych osobowych.

Jest to kolejna inicjatywa edukacyjna, ponieważ GIODO już od dawna współpracuje przy realizacji zajęć akademickich m.in. z Akademią Leona Koźmińskiego (studia podyplomowe *Ochrona Danych Osobowych*) oraz z Uniwersytetem Kardynała Stefana Wyszyńskiego (*Podyplomowe Studium z zakresu Ochrony Informacji Niejawnych i Danych Osobowych*).

d) Porozumienie pomiędzy GIODO a Samorządowym Ośrodkiem Doradztwa Metodycznego i Doskonalenia Nauczycieli w Kielcach

W dniu 20 października 2009 r. Generalny Inspektor Ochrony Danych Osobowych podpisał porozumienie z Samorządowym Ośrodkiem Doradztwa Metodycznego i Doskonalenia Nauczycieli w Kielcach o współpracy w zakresie działań edukacyjnych na rzecz podnoszenia poziomu świadomości w zakresie ochrony prywatności i danych osobowych. W wyniku porozumienia rozpoczęty został program pilotażowy, który ma na celu opracowanie ogólnopolskiego programu,

w ramach którego do szkół zostaną wprowadzone lekcje o tematyce dotyczącej ochrony danych osobowych.

e) Newsletter „Prywatność w świecie. Przegląd wydarzeń.”

W celu zagwarantowania systematycznego otrzymywania informacji dotyczących ochrony prywatności i danych osobowych za granicą, od września 2008 r. pracownicy Biura GIODO otrzymują tłumaczenia artykułów z Newslettera „Prywatność w świecie. Przegląd wydarzeń.” Informujących o najważniejszych i inicjatywach podejmowanych na świecie w związku z ochroną danych osobowych i przestrzeganiem prawa do prywatności. W 2009 r. dokonał tłumaczeń i przekazał **97 artykułów** o łącznej liczbie 230 stron.

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 zarówno w kraju, jak i za granicą, a także w różnych formach współpracy z innymi organami ochrony danych osobowych. Do najważniejszych zadań GIODO w ramach współpracy międzynarodowej należy:

1. udział w pracach Grupy Roboczej Art. 29 ds. ochrony danych osobowych,
2. wyznaczanie członków Wspólnego Organu Nadzorczego zajmującego się zagadnieniami ochrony danych osobowych w związku z utworzeniem tzw. Obszaru Schengen (JSA Schengen) i uczestnictwo w roli obserwatora w posiedzeniach tego organu,
3. wybór członków Wspólnego Organu Nadzorczego nad Europolem (JSB 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. uczestnictwo w pracach Komitetu Konsultacyjnego ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych,
6. wyznaczanie członków Wspólnego Organu Nadzorczego właściwego w sprawach ochrony danych osobowych w związku z wykorzystywaniem systemu informacyjnego dla odpraw celnych (JSA Customs),
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 organizowanych cyklicznie Międzynarodowych Konferencjach Rzeczników Ochrony Danych Osobowych i Prywatności, Wiosennych Konferencjach Europejskich Organów Ochrony Danych oraz w 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.²⁰⁶

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.

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.

Grupa Robocza Art. 29 w swoim Programie prac na lata 2008-2009 podkreśliła konieczność rozważenia kilku podstawowych kwestii, jak: zwiększenie oddziaływania dyrektywy 95/46/WE i roli Grupy Roboczej Art. 29, wpływu nowych technologii na kwestie ochrony danych osobowych (w szczególności zastosowanie chipów RFID czy elektronicznych systemów pobierania opłat za przejazd), transfer danych osobowych do innych krajów oraz zagadnienia dotyczące ochrony prywatności i jurysdykcji w wymiarze światowym.²⁰⁷ W roku sprawozdawczym 2009 Generalny Inspektor Ochrony Danych Osobowych uczestniczył w Brukseli w czterech posiedzeniach wspomnianej Grupy. Na 69. posiedzeniu, które odbyło się w dniach 10-11 lutego 2009 r. omawiane były zagadnienia związane z wyszukiwarkami. Grupa Robocza Art. 29 spotkała się z przedstawicielami

²⁰⁶ Najnowsze wydanie i archiwalne numery periodyka „Data Protection Review” można znaleźć w Internecie pod adresem www.dataprotectionreview.eu

²⁰⁷ 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

operatorów usług wyszukiwarek, którzy zobowiązali się do współpracy z organami ochrony danych w celu usprawnienia swoich praktyk ochrony prywatności. Dyskusja koncentrowała się na trzech głównych tematach: okresie przechowywania danych, skutecznej i nieodwracalnej anonimizacji oraz właściwym ustawodawstwie. Grupa z zadowoleniem przyjęła zobowiązanie dostawców usług wyszukiwarek do stworzenia wspólnych standardów branżowych dla wyszukiwania on-line w oparciu o europejskie ustawodawstwo w zakresie ochrony danych i prywatności. Na kolejnych dwóch posiedzeniach (7-8.04.2009 r. i 16-17.06.2009 r.) kontynuowane były prace nad Międzynarodowymi Standardami Ochrony Prywatności i Danych Osobowych oraz przyjęto opinię Grupy Roboczej Art. 29 z dnia 12 czerwca 2009 r. w sprawie portali społecznościowych. Natomiast 72. posiedzenie Grupy (12-13 października 2009 r.) poświęcone było konsultacjom w sprawie przyszłości prywatności. W ich ramach kontynuowane były prace Grupy m.in. nad definicją kluczowych terminów *administrator danych/przetwarzający dane* (artykuł 2 dyrektywy 95/46/WE), a także nad uwagami do Raportu Grupy Ekspertów ds. Historii Kredytowych w kwestii szczególnych gwarancji w odniesieniu do zasad ochrony danych. Przeprowadzona też była dyskusja na temat Programu Sztokholmskiego (*Program dla Obszaru Wolności, Bezpieczeństwa i Sprawiedliwości służący obywatelom*) oraz podjęta decyzja o współpracy z Grupą Roboczą ds. Policji i Wymiaru Sprawiedliwości na rzecz wydania wspólnej opinii na temat tego Programu. Ponadto Grupa zapoznała się z aktualnym stanem rzeczy odnośnie do nowego porozumienia między UE a USA będącego obecnie przedmiotem negocjacji, a dotyczącego przekazywania danych za pośrednictwem sieci danych finansowych SWIFT. Na posiedzeniu tym dyskutowane też były zagadnienia związane z ochroną danych pasażerów gromadzonych i przetwarzanych przez sklepy wolnocłowe na lotniskach i w innych portach. W sprawie tej praktyki opracowana zostanie opinia Grupy na ten temat. Z kolei 73. posiedzenie (30 listopada – 1 grudnia 2009 r.) poświęcone było między innymi usługom portali społecznościowych po przyjęciu Opinii 5/2009 Grupy na ten temat. Dyskusja skoncentrowała się na trzech najważniejszych tematach: ochronie niepełnoletnich, okresie zatrzymywania danych oraz dostępie do danych przez strony trzecie. Kontynuowane też były rozmowy w sprawie przyszłości prywatności i uwagi do Raportu Grupy Ekspertów ds. Historii Kredytowych. W odniesieniu do nowego tymczasowego porozumienia między UE a USA w sprawie przekazywania danych za pośrednictwem sieci danych finansowych SWIFT (podpisane 30 listopada 2009 r.) Grupa Robocza Artykułu 29 postanowiła dokładnie zbadać kwestie ochrony danych związane z tym porozumieniem. Na wniosek Komisji Europejskiej Grupa Robocza Art. 29 przyjrzała się sprawie ochrony danych pasażerów gromadzonych i przetwarzanych przez sklepy wolnocłowe na lotniskach i w portach w Unii Europejskiej i wydała zalecenia w sprawie jednolitego stosowania ogólnych zasad ochrony danych, które powinny być przestrzegane przez sklepy wolnocłowe na lotniskach i w portach.

W 2009 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. Sprawy indywidualne z zakresu przetwarzania danych osobowych przez Europol rozpatrywane są przez Komitet Rewizyjny Wspólnego Organu Nadzorczego, którego Generalny Inspektor jest członkiem. W dniach 3 – 6 marca 2009 r. zespół kontrolny WON Europolu przeprowadził coroczną kontrolę przetwarzania danych osobowych, która miała miejsce w siedzibie Europolu. Natomiast w dniu 22 czerwca 2010 r. WON zorganizował spotkanie z organami ochrony danych tych państw członkowskich i instytucji, które zawarły porozumienie operacyjne z Europolem. W spotkaniu uczestniczyli przedstawiciele chorwackich, szwajcarskich i norweskich organów ochrony danych, wspólny organ nadzorczy Eurojustu i Sekretariat Ochrony Danych Interpolu. W trakcie spotkania jego uczestnicy wymienili się doświadczeniami związanymi z nadzorem działań Europolu i podkreślili potrzebę dalszej współpracy.

Duża część prac WON była związana z przyjęciem nowych podstaw prawnych Europolu.²⁰⁸ WON przyjął nowy regulamin, który został przesłany do zatwierdzenia przez Radę, zgodnie z art. 34 ust. 7 decyzji Rady ustanawiającej Europejski Urząd Policji [Europol]. Przesłał także opinię (nr 09/13) w odniesieniu do projektu decyzji zarządu Europolu w sprawie warunków dotyczących przetwarzania danych w celu określenia ich istotności w oparciu o art. 10 ust. 4 decyzji Europolu. Ponadto WON zajmował się przyszłą strategią działania oraz różnymi aspektami wdrażania zasady dostępności. Przyjął - na przykład - opinię w sprawie poziomu ochrony danych w Kolumbii. Uznano bowiem, że z punktu widzenia ochrony danych nie ma przeszkód, by Europol rozpoczął negocjacje z tym państwem w sprawie przygotowania porozumienia dotyczącego przekazywania danych osobowych przez Europol oraz by w trakcie negocjacji uwzględnić pewne kwestie. Przyjął także opinię w sprawie poziomu ochrony danych w Byłej Jugosłowiańskiej Republice Macedonii [BJRM], w której również stwierdzono brak przeszkód, by Europol rozpoczął negocjacje z BJRM w sprawie przygotowania porozumienia dotyczącego przekazywania danych osobowych przez Europol. Przyjęto również opinię w sprawie wdrażania przepisów dotyczących otrzymywania informacji z publicznie dostępnych źródeł, od osób prywatnych i innych stron działających prywatnie. Generalny Inspektor kontynuował również współpracę na forum Wspólnego Organu Nadzorczego Schengen, który m.in. przyjął raport ze wspólnej kontroli stosowania art. 97 i 98 Konwencji Wykonawczej do Układu z Schengen, a także zajmował się dalszymi działaniami wynikającymi z Raportu z kontroli dotyczącej stosowania art. 96 i 99 Konwencji Wykonawczej do Układu z Schengen. Ponadto przygotowano uaktualniony poradnik dotyczący realizowania prawa dostępu do danych zawartych w Systemie Informacji Schengen [SIS].

²⁰⁸ Decyzja 2009/371/WSiSW Rady z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol) (Dz. Urz. UE L 121/37), która wchodzi w życie w styczniu 2010 r. zastąpiła Konwencję ustanawiającą Europejski Urząd Policji.

W omawianym okresie aktywność Wspólnego Organu Nadzorczego ds. systemu informacji celnej koncentrowała się na pracach nad przyszłą decyzją Rady, która ma zastąpić dotychczas obowiązującą Konwencję w sprawie wykorzystywania technologii informatycznych dla potrzeb celnych, a także pracami nad wdrażaniem kwestionariusza samooceny, który mógłby być stosowany przez służby celne.

W 2009 r. Generalny Inspektor Ochrony Danych Osobowych uczestniczył w pracach grupy koordynującej nadzór nad **systemem Eurodac**, w ramach których przyjęto Drugie sprawozdanie z kontroli dotyczącej sposobu spełniania obowiązku informacyjnego wobec osób, których dane są zbierane na potrzeby tego systemu oraz oceny wieku osób młodocianych ubiegających się o azyl. Raport został przygotowany na podstawie danych zebranych przez organy ochrony danych w roku poprzednim. W raporcie m.in. stwierdzono, że informacje dostarczane osobom ubiegającym się o azyl dotyczące ich praw i wykorzystywania ich danych, z reguły są niekompletne, w szczególności jeśli chodzi o konsekwencje pobierania odcisków palców oraz prawa dostępu do danych i ich korygowania. Dostarczane informacje również w szerokim stopniu różnią się w poszczególnych państwach członkowskich; duże różnice zaobserwowano w praktykach stosowanych wobec osób ubiegających się o azyl i nielegalnych imigrantów – ta druga grupa przeważnie otrzymuje mniej informacji, a w niektórych przypadkach nie otrzymuje ich wcale. Natomiast w odniesieniu do metod określania wieku osób ubiegających się o azyl (czy to w ramach systemu Eurodac, czy też w szerszym kontekście procedury azylowej), to stwierdzono, że są one wciąż tematem dyskusji w wielu państwach członkowskich – zwłaszcza jeśli chodzi o ich wiarygodność i możliwość ich zaakceptowania ze względów etycznych. Zwrócono przede wszystkim uwagę na brak harmonizacji systemów wykorzystywanych w państwach członkowskich do ustalenia wieku małoletnich osób ubiegających się o azyl, co również prowadzi do różnorodnych wyników. Dlatego w raporcie zawarte zostały odpowiednie zalecenia.

Natomiast **Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości** koncentrowała się w tym okresie na różnych kwestiach związanych z wejściem w życie przepisów decyzji ramowej 2008/977/JHA o ochronie danych osobowych w trzecim filarze UE, Traktatu Lizbońskiego i przygotowaniu Programu Sztokholmskiego. Jednocześnie zajmowano się różnymi aspektami wdrożenia Konwencji z Prüm czy dialogiem prowadzonym ze Stanami Zjednoczonymi Ameryki na forum Grupy Kontaktowej Wysokiego Szczebla ds. wymiany informacji oraz ochrony prywatności i danych osobowych. Grupa Robocza prowadziła również wspólne badania dotyczące istniejących umów dwustronnych zawieranych z państwami trzecimi w obszarze współpracy policyjnej i sądowej w sprawach karnych, a także wdrażania postanowień Konwencji o Cyberprzestępczości. Innym ważnym obszarem prac było przygotowanie katalogu dotyczącego nadzoru i współpracy.

7.1 Międzynarodowe spotkania i konferencje

Generalny Inspektor Ochrony Danych Osobowych oraz pracownicy jego Biura uczestniczyli także w konferencjach i seminariach o charakterze międzynarodowym odbywających się w kraju i za granicą. Najważniejsze z nich to:

1. Wiosenna Konferencja Europejskich Organów Ochrony Danych i Prywatności

(Edynburg, 23-24 kwietnia 2009 r.).

Organizatorem tej Wiosennej Konferencji był Rzecznik Ochrony Informacji Zjednoczonego Królestwa. Jej głównym tematem było podniesienie poziomu ochrony danych poprzez dyskusowanie kwestii dotyczących mocnych i słabych stron europejskich przepisów dotyczących ochrony danych w kontekście postępującej globalizacji, a także określenie ich pożądanych skutków dla obywateli, prawodawców i administratorów danych. Na Konferencji tej przyjęta została *Deklaracja w sprawie przewodnictwa i przyszłości ochrony danych w Europie* oraz *Rezolucja w sprawie umów dwustronnych i wielostronnych pomiędzy państwami członkowskimi UE i państwami trzecimi w obszarze współpracy policyjnej i sądowej w sprawach karnych*. Przyjęte też zostało stanowisko Europejskiej Konferencji Rzeczników Ochrony Danych Osobowych w kwestii przyszłości warsztatów rozpatrywania skarg (tzw. warsztatów skargowych - case handling workshop).

2. Konferencja dotycząca przechowywania danych „W kierunku oceny dyrektywy

o zatrzymywaniu danych - Data Retention Conference (Bruksela, 14 maja 2009 r.).

Zorganizowana przez Komisję Europejską Konferencja dotyczyła kwestii związanych z wdrażaniem i oceną dyrektywy o zatrzymywaniu danych (2006/24/WE). Ogólnym celem wydarzenia było zastanowienie się nad zaletami zatrzymywania danych w ramach mechanizmu wprowadzonego przez wskazaną dyrektywę, w szczególności zaś nad wartością dodaną dyrektywy, a także nad tym, czy dostępność zatrzymywania danych zapewnia organom egzekwowania prawa odpowiednie narzędzie do prowadzenia dochodzeń, ścigania i wykrywania sprawców poważnej przestępczości. Podczas Konferencji skupiono się także na związanych z tą kwestią skutkach dla dostawców usług komunikacyjnych oraz dla konsumentów, których dane są zatrzymywane.

3. XI. Spotkanie Grupy Organów Ochrony Danych Osobowych Europy Środkowej

i Wschodniej (Central and Eastern European Data Protection Authorities), zorganizowane w dniach 2-4 czerwca 2009 r. przez rumuński organ ochrony danych osobowych.

Głównym tematem spotkania było omówienie wyzwań, jakie napotykają organy ochrony danych osobowych w związku z rozwojem nowoczesnych technologii. Podczas dyskusji uczestnicy spotkania koncentrowali się na bezpieczeństwie danych osób korzystających z różnych narzędzi

informatycznych, takich jak fora internetowe, blogi, e-mail, wideonadzór czy portale społecznościowe. Analizowano również ochronę danych umieszczonych w różnego rodzaju bazach, na przykład w systemie informacji kredytowej. Poruszono temat ochrony danych osobowych pracowników i rozwoju biometrii, a w szczególności umieszczania danych biometrycznych na różnego rodzaju kartach identyfikacyjnych oraz kwestie związane z cyfrowymi dokumentami tożsamości. Do stałego punktu tych corocznych spotkań należy omówienie przez poszczególnych przedstawicieli organów ochrony danych osobowych najważniejszych wydarzeń, z którymi zetknęli się w swojej codziennej pracy od czasu poprzedniego spotkania.

Na spotkaniu podjęta została decyzja, aby kolejne 12. spotkanie zorganizowane zostało w 2010 r. w Polsce. 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 niezmiennie odgrywa kluczową rolę w jego pracach i podejmowanych wspólnie inicjatywach.²⁰⁹

4. 25. plenarne posiedzenie Komitetu Konsultacyjnego Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych T-PD (Strasburg, 2-4 września 2009 r.).

Jednym z głównych tematów spotkania były kwestie dotyczące projektu rekomendacji w sprawie ochrony osób w związku z przetwarzaniem danych osobowych podczas profilowania. Współpracujące w ramach forum T-PD organy ochrony danych osobowych stanęły przed zadaniem opracowania zestawu wytycznych dla projektowanej rekomendacji w celu wyeliminowania zagrożeń dla prywatności mogących pojawić się podczas tworzenia profili użytkowników wykorzystujących nowoczesne technologie w codziennym życiu. Zadanie to jest o tyle ważne, że zjawisko profilowania staje się coraz bardziej powszechne. Z profilowaniem związane jest najczęściej przetwarzanie informacji o charakterze danych osobowych, w tym między innymi danych o ruchu w sieci, danych rejestrowanych przez wyszukiwarki internetowe (co pozwala na prześledzenie aktywności użytkowników Internetu oraz ich nawyków,

²⁰⁹ Pod koniec 2001 r. polski Generalny Inspektor Ochrony Danych Osobowych zainicjował międzynarodową współpracę między organami ochrony danych osobowych z państw Europy Środkowej i Wschodniej dla wspierania rozwoju ochrony prywatności na tym obszarze. W trakcie zorganizowanego 17 grudnia 2001 r. przez Generalnego Inspektora Ochrony Danych Osobowych spotkania rzeczników z państw Europy Środkowej i Wschodniej została podpisana Deklaracja Końcowa, w której przedstawiciele organów ochrony danych osobowych z Czech, Węgier, Litwy, Słowacji, Estonii, Łotwy oraz Polski zadeklarowali chęć współpracy i wzajemnej pomocy w zakresie niezbędnym do zapewnienia odpowiedniej ochrony danych osobowych w swoich krajach. W chwili obecnej w ramach niniejszego forum, oprócz wskazanych powyżej państw, współpracuje również Bułgaria, Chorwacja, Macedonia, Rumunia oraz Słowenia, jako obserwator. Spotkania organów ochrony danych osobowych z państw Europy Środkowej i Wschodniej, których celem jest wspieranie państw kandydujących do Unii Europejskiej oraz będących nowymi członkami, dzielenie się informacjami i doświadczeniami, podnoszenie poziomu świadomości tego, jak ważną kwestią jest ochrona danych osobowych, a ponadto, co najważniejsze, dalsza harmonizacja przepisów krajowych z prawem Unii Europejskiej, przybrały postać organizowanych w poszczególnych państwach, cyklicznych konferencji i bieżącej – w zależności od aktualnych potrzeb – współpracy. Ponadto, w celu ułatwienia współpracy, Generalny Inspektor Ochrony Danych Osobowych stworzył specjalną stronę internetową (www.cecprivacy.org), stanowiącą źródło informacji na temat danych osobowych w poszczególnych państwach członkowskich Grupy oraz pozwalającą na szybką wymianę informacji pomiędzy rzecznikami ochrony danych osobowych, w tym poszukiwanie wspólnych rozwiązań dla podobnych problemów występujących w tej dziedzinie.

upodobań konsumenckich i zainteresowań), a także danych geolokalizacyjnych zgromadzonych przez operatorów sieci telefonii komórkowej, systemy wideonadzoru lub systemy identyfikacji za pomocą fal radiowych (RFID). Tego rodzaju praktyki mogą prowadzić do poważnych naruszeń w sferze prywatności i ochrony danych użytkowników. Prace nad projektem kontynuowane będą w czasie kolejnej sesji Grupy T-PD planowanej w 2010 roku.

5. **46. Spotkanie Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji**

(Berlin, 6-8 września 2009 r.).

Głównym tematem spotkania były usługi świadczone przez operatorów i ich obowiązki wobec osób, które zaprzestały korzystania z nich. Dyskusja koncentrowała się głównie wokół tematu związanego z praktyką przyznawania konta użytkownika, który zaprzestał korzystania z usługi - innej osobie. W takich sytuacjach często się zdarza, że do nowego użytkownika konta dochodzą informacje, których adresatem powinien być poprzedni użytkownik. Dzieje się tak dlatego, że osoba wysyłająca wiadomość nie została poinformowana o zmianie adresu podmiotu, do którego swoją korespondencję kieruje. W odniesieniu do tego tematu GODO zwrócił uwagę na konieczność zastosowania takich samych zasad, jak w odniesieniu do usług telefonii komórkowej, gdzie np. komunikacja SMS może być wykorzystywana do przesyłania danych poufnych typu: kod jednorazowy do wykonania operacji bankowej, hasło dostępu czy klucz do szyfrowania zakodowanej informacji. Innym ważnym tematem spotkania były kwestie związane ze stosowaniem narzędzi programowych do tzw. głębokiej analizy pakietów, które mogą być wykorzystywane do podglądania poufnych informacji przez osoby do tego nieupoważnione.

6. **Międzynarodowa Konferencja „Ponad podziałami – jak skutecznie przybić do Bezpiecznej przystani”** (Waszyngton, 16-18 listopada 2009 r.).

Organizatorami tego spotkania byli Administracja Handlu Międzynarodowego oraz Departament Handlu USA przy współpracy z Komisją Europejską i Grupą Roboczą Art. 29 ds. ochrony danych. Podczas konferencji przeanalizowane zostały postępy poczynione w zakresie programu Safe Harbor²¹⁰ oraz procedur zatwierdzania wiążących reguł korporacyjnych. Program ten - wypracowany przez Departament Handlu Stanów Zjednoczonych w porozumieniu z Komisją Europejską – ma za zadanie wspierać wymianę gospodarczą pomiędzy Unią Europejską a USA, umożliwiając amerykańskim podmiotom gospodarczym sprostać wymaganiom Dyrektywy 95/46/WE Parlamentu Europejskiego

²¹⁰ Od 2005 r. Stany Zjednoczone, Komisja Europejska oraz Grupa Robocza Artykułu 29 ds. Ochrony Danych co roku spotykają się w celu przeanalizowania postępów poczynionych w zakresie Uregulowań Safe Harbor USA-UE oraz ostatnich wydarzeń w dziedzinie zgodności, ochrony danych i prywatności, które miały miejsce na poziomie krajowym, regionalnym i globalnym. Konferencja z listopada 2009 r. stanowiła kontynuację zobowiązań podjętych przez Stany Zjednoczone i Unię Europejską w porozumieniu zawartym w 2000 r. w sprawie przekazywania danych osobowych w celach komercyjnych z Unii Europejskiej do Stanów Zjednoczonych. Dyrektywa UE o ochronie danych z 1998 r. upoważnia państwa członkowskie do blokowania tego typu przekazywania danych do krajów, których system egzekwowania przepisów o ochronie prywatności nie jest zgodny z wymogami dyrektywy 95/46/WE. Zgodnie z Uregulowaniami Safe Harbor USA-UE, Stany Zjednoczone otrzymują od Komisji Europejskiej zatwierdzenie „adekwatności” poziomu ochrony danych wyłącznie dla tych organizacji USA, które same przedstawiły deklarację o przestrzeganiu zasad Safe Harbor, co pozwala na dokonywanie transferów danych bez uprzedniego zatwierdzenia.

i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Uczestnicy konferencji zapoznali się z nowym paradygmatem przestrzegania zasad ochrony prywatności w kontekście prawa dostępu obywateli do informacji. Wśród innych tematów poruszanych na konferencji znalazły się: transgraniczna wymiana danych podczas pandemii, prywatność w fazie projektowania, strategiczne zarządzanie informacjami dla przedsiębiorstwa, dostawcy usług portali społecznościowych, reklama behawioralna w tzw. cloud computing,²¹¹ globalne standardy ochrony prywatności i in.

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 dniach 11-13 marca 2009 r. Generalny Inspektor Ochrony Danych Osobowych gościł w Warszawie delegację węgierskiego organu ochrony danych osobowych. Na spotkaniu omówiona została działalność obu Urzędów, aktualne problemy, z jakimi organy ochrony danych spotykają się w swojej codziennej pracy, oraz przedyskutowano propozycje rozwiązań dla omawianych kwestii. Spotkanie GIODO z przedstawicielami węgierskiego rzecznika ochrony danych osobowych połączone było z odbywającym się w Warszawie Kongresem „Strategiczne Forum Liderów Marketingu, Mediów i Komunikacji”. Z kolei na zaproszenie Andrása Jóri, Rzecznika Ochrony Danych i Wolności Informacji Węgier, **Generalny Inspektor Ochrony Danych Osobowych i jego zastępca, przebywał w dniach 13-14 lipca 2009 r. z dwudniową wizytą w Budapeszcie,** gdzie kontynuowane były rozpoczęte w Warszawie rozmowy na temat współpracy i wymiany doświadczeń w obszarze ochrony danych.

Natomiast **7 kwietnia 2009 r. Generalny Inspektor Ochrony Danych Osobowych złożył wizytę w Czeskim Urzędzie Ochrony Danych w Pradze,** gdzie brał udział w dyskusjach dwustronnych na temat przyszłych wspólnych działań w instytucjach UE.

²¹¹ Model sprzedaży oprogramowania oparty na pobieraniu opłaty wyłącznie za użytkowanie jego funkcjonalności.

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). **XIX warsztaty skargowe odbyły się w dniach 12-13 marca 2009 r. w Pradze.** Ich organizatorem był Rzecznik Ochrony Danych Republiki Czeskiej, który zaznajomił uczestników warsztatów z działalnością urzędu, podkreślając, że oprócz ochrony danych osobowych zajmuje się także sprawami z zakresu komunikacji elektronicznej. Na XIX warsztatach omówione zostały kwestie związane z działalnością mass mediów, które np. w Szwecji wyłączone są spod zakresu obowiązywania ustawy o ochronie danych osobowych i stąd konieczność opracowania kodeksu dobrych praktyk i kodeksu etyki. Dyskutowane też były zagadnienia związane z zamieszczaniem różnych publikacji w Internecie, wideonadzorem, korzystaniem z kamer internetowych i związanym z tym ograniczeniem czasowym przechowywania utrwalonego materiału. W odniesieniu do spraw związanych z ochroną danych medycznych w kontekście stosowania elektronicznych kart zdrowia podkreślano konieczność zapewnienia zróżnicowanego dostępu personelu do danych osobowych pacjentów, gdzie np. pracownicy administracyjni placówek służby zdrowia mieliby dostęp wyłącznie do danych demograficznych.

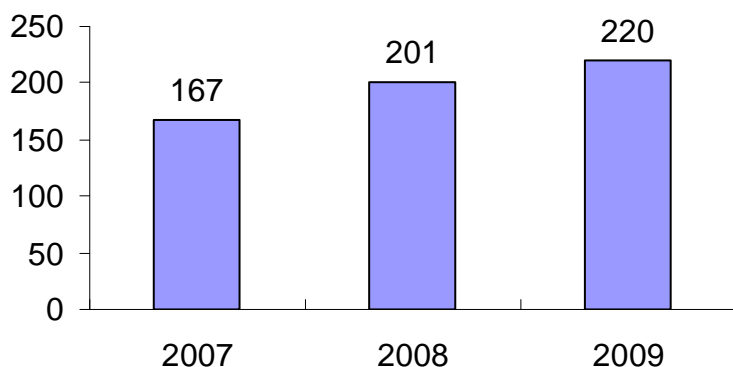
Natomiast **XX warsztaty rozpatrywania spraw** odbyły się w październiku 2009 r. w Limassol na Cyprze. Ich uczestnicy zapoznali się z działalnością cypryjskiego organu ochrony danych osobowych, poznali organizację i strukturę biura tego organu, zaznajomili się z nietypowymi rozwiązaniami z zakresu ochrony danych osobowych przyjętymi przez cypryjskiego ustawodawcę (w szczególności z instytucją połączenia). Zapoznali się też z systemem informatycznym Policji cypryjskiej. Omawiane były również zagadnienia najczęściej poruszane w skargach, jak odpowiedzialność za przetwarzanie danych na forach dyskusyjnych i na stronach umożliwiających dokonanie oceny np.: nauczycieli, lekarzy lub przedsiębiorców, system sankcji karnych za łamanie przepisów prawa o ochronie danych osobowych, a także kwestie związane z technologią street view i nadzorem wideo. Dyskutowane też były zagadnienia związane z prawem dostępu do danych przez osobę, której dane te dotyczą, w tym prawo dostępu na nagrania dźwiękowych wykonanych przez centra telefoniczne różnych instytucji (banków, dostawców usług telekomunikacyjnych itd.) czy dostępu do danych medycznych, a także prawem do wiedzy o tym, kto jest odbiorcą tych informacji. Podczas warsztatów przedstawiciele organów ochrony danych osobowych omówili ważne kwestie dotyczące między innymi korzystania z wariografów, monitoringu GPS, systemu kontroli telefonii komórkowej w sektorze zatrudnienia czy biometrii w celu identyfikacji pracowników i kontroli czasu ich pracy oraz przetwarzanie danych osobowych przez instytucje finansowe i mass media.

Część III.

Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2009 roku

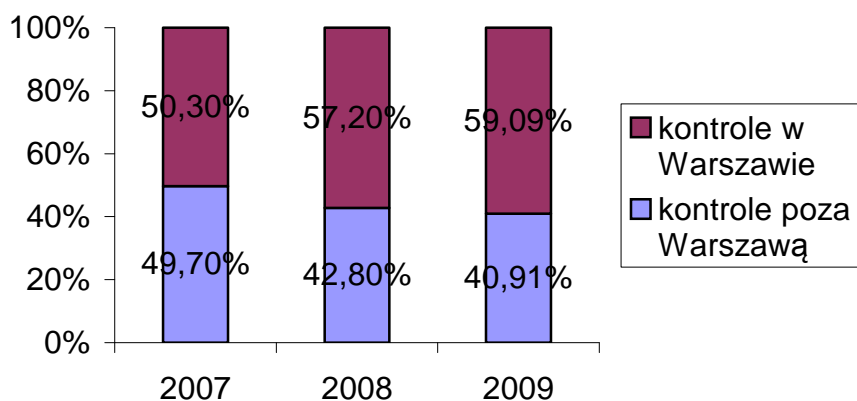
W odniesieniu do przeprowadzonych **kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych należy stwierdzić, że – podobnie jak w latach ubiegłych – znaczna część kontrolowanych podmiotów nadal miała problemy z zastosowaniem odpowiednich środków technicznych 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. Uchybienia występowały również w procesie przetwarzania danych osobowych przy użyciu **systemów informatycznych**.

W 2009 r. przeprowadzonych zostało 220 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Od 2007 r. liczba kontroli systematycznie wzrasta (zob. Wykres 25).



Wykres 25: Porównanie liczby kontroli przeprowadzonych w latach 2007–2009.

Z kolei Wykres 26 przedstawia procentowe zastawienie kontroli przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych na terenie Warszawy oraz poza nią.



Wykres 26: Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2007–2009.

Najwięcej kontroli przeprowadzonych zostało z urzędu (128). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący:

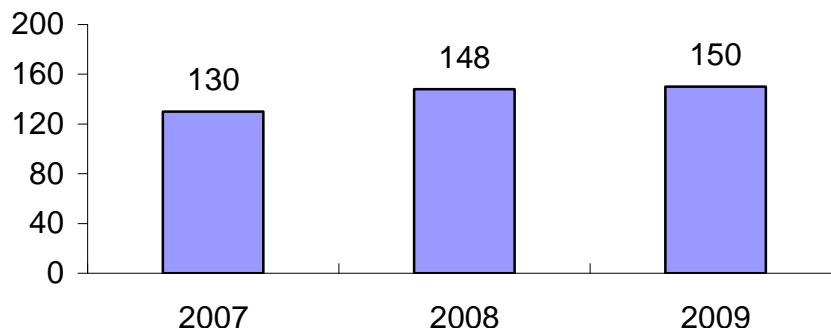
Inicjatywa kontroli	Liczba kontroli
Z urzędu	128
Departament Orzecznictwa, Legislacji i Skarg	46
Departament Rejestracji Zbiorów Danych Osobowych	16
Departament Edukacji Społecznej i Spraw Międzynarodowych	6
Prokuratura	3
Naczelna Izba Lekarska	1
Okręgowy Rzecznik Odpowiedzialności Zawodowej Izby Lekarskiej	2
Agencja Bezpieczeństwa Wewnętrznego	1
Policja	1
Starostwo Powiatowe	1
W związku z inną kontrolą	15
RAZEM	220

Czynnościom kontrolnym poddawane były między innymi biura obrotu nieruchomości, komornicy, portale internetowe oraz pracodawcy. Dużą grupę jednostek kontrolowanych stanowiły również 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 w 2009 r. objęto portale internetowe (17 kontroli), biura obrotu nieruchomościami (16 kontroli), komorników (19 kontroli), urzędy pracy (11 kontroli), podmioty zajmujące się transportem miejskim wydające spersonalizowane karty miejskie (11 kontroli) oraz pracodawców (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 2009 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 10 kontroli sprawdzających wykonanie decyzji administracyjnych. Wykazały one, że zdecydowana większość podmiotów poddanych w tym zakresie kontroli wykonała wydane wobec nich decyzje. Skutkiem jednej z tego typu kontroli²¹² było skierowanie do organu powołanego do ścigania przestępstw zawiadomienia o popełnieniu przestępstwa²¹³ z uwagi na nieprzywrócenie przez jednostkę kontrolowaną stanu zgodnego z prawem.

W 2009 r. Generalny Inspektor w związku z przeprowadzonymi kontrolami wydał łącznie 150 decyzji.



Wykres 27: Porównanie liczby decyzji wydanych w związku z kontrolami przeprowadzonymi w latach 2007–2009.

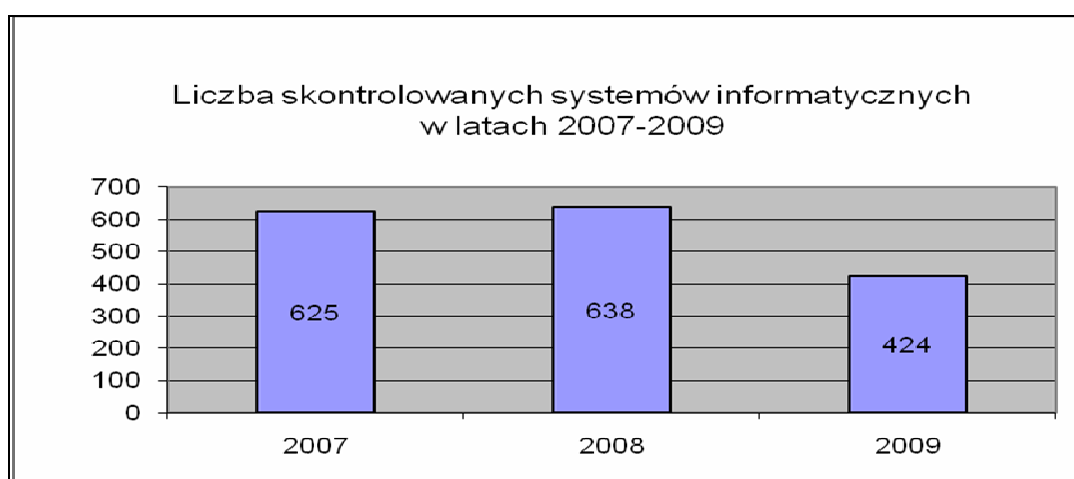
W okresie sprawozdawczym, w związku z obecnością Polski w strefie Schengen, kontynuowane były kontrole podmiotów uprawnionych do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych SIS oraz w celu wglądu do danych SIS. W 2009 r. takie kontrole przeprowadzono przede wszystkim w sądach (7 kontroli), gdzie ustalono

²¹² Kontrola DIS-K-421/30/09.

²¹³ Zawiadomienie z 15.04.2009 r., nr DIS/ZAW-7/13356/09, do Prokuratury Rejonowej Warszawa – Mokotów o popełnieniu przestępstwa określonego w art. 49 ust. 1 ustawy o ochronie danych osobowych, polegającego na

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 (Dz. U. Nr 165, poz. 1170). Do istotnych kontroli, jakie przeprowadzili w 2009 r. inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, należały także kontrole dostawców usług telekomunikacyjnych (4 kontrole), przeprowadzone w związku z prowadzonym przez Grupę Roboczą Art. 29 badaniem wdrażania przez kraje członkowskie Unii Europejskiej dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz. Urz. UE L z 2006 r., Nr 105, poz. 54).

W 2009 r. skontrolowano 424 systemy informatyczne wykorzystywane do przetwarzania danych osobowych, co obrazuje Wykres 28:



Wykres 28: Liczba skontrolowanych systemów informatycznych w latach 2007-2009.

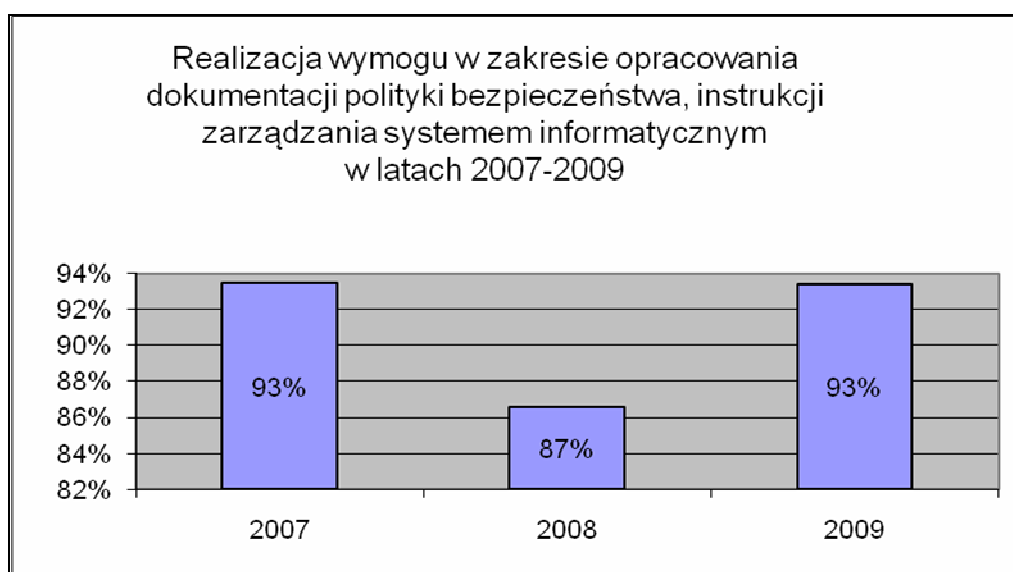
Stopień wypełnienia w poszczególnych latach (od roku 2007 do 2009) wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie o ochronie danych osobowych i rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków 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,

przetwarzaniu w zbiorze danych osobowych potencjalnych klientów (osób, z którymi nie została zawarta umowa

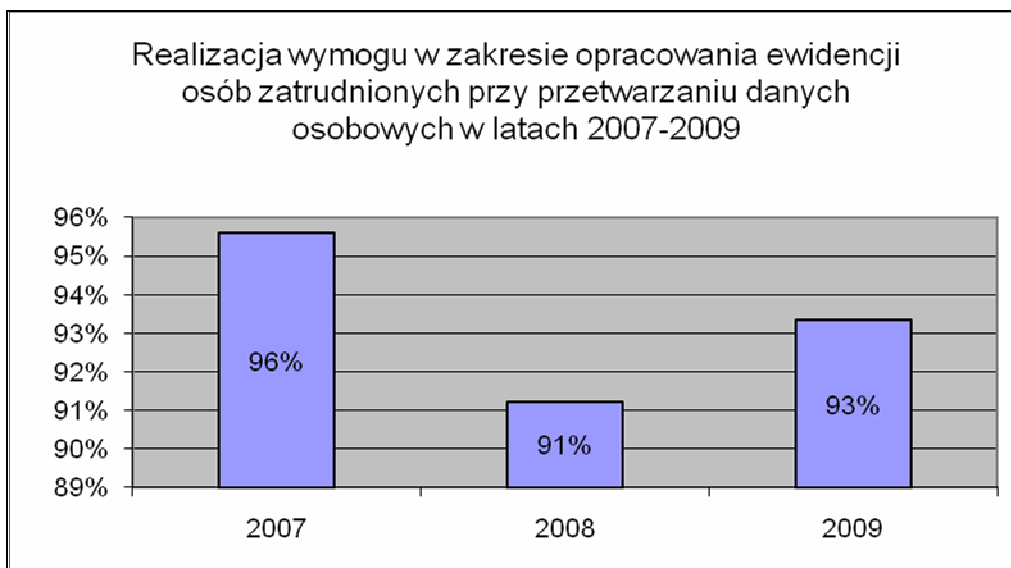
że stopień realizacji wymaganych funkcjonalności systemów informatycznych oceniany był w skali procentowej, w odniesieniu do liczby systemów objętych kontrolą. Pozostałe wymogi natomiast, odnoszące się np. do dokumentacji procesu przetwarzania czy też do obowiązku prowadzenia ewidencji osób upoważnionych 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. Ocenie poddano takie dokumenty, jak: politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz ewidencję osób upoważnionych do przetwarzaniu danych osobowych. Ponadto kontrolowano, czy w podmiocie wyznaczony został administrator bezpieczeństwa informacji.

Stopień wykonania przez kontrolowane podmioty ww. warunków w roku 2009 przedstawiono na Wykresach 29-31.



Wykres 29: Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych w latach 200 -2009.

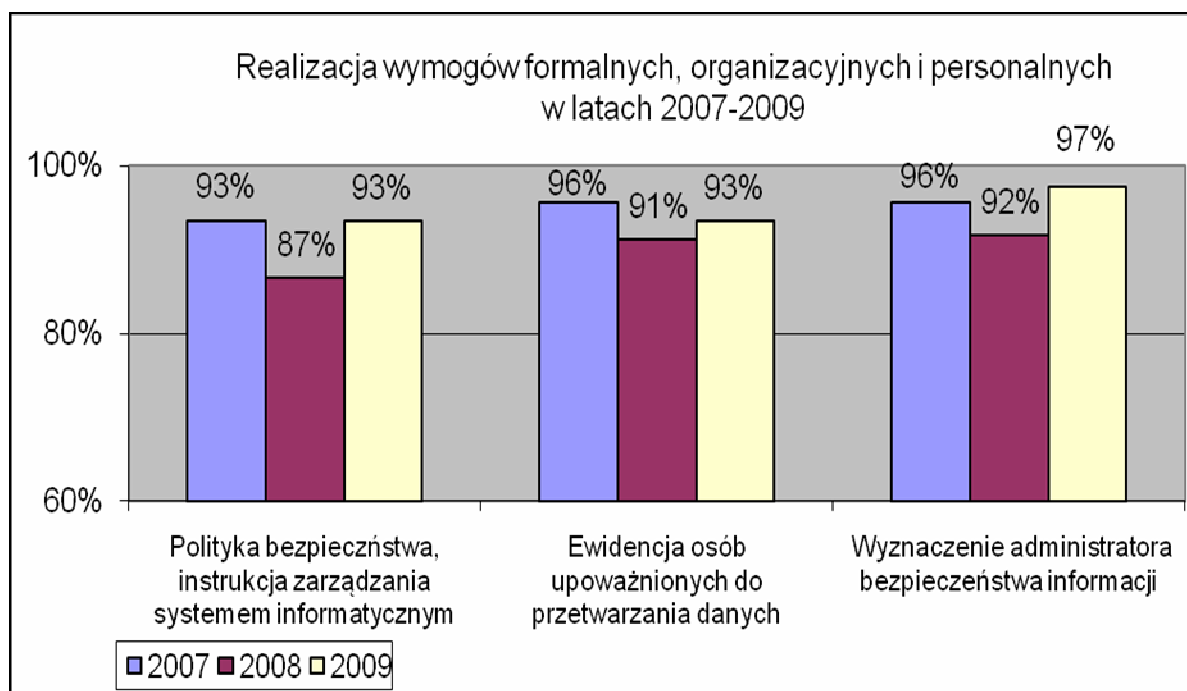


Wykres 30: Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w latach 2007-2009.



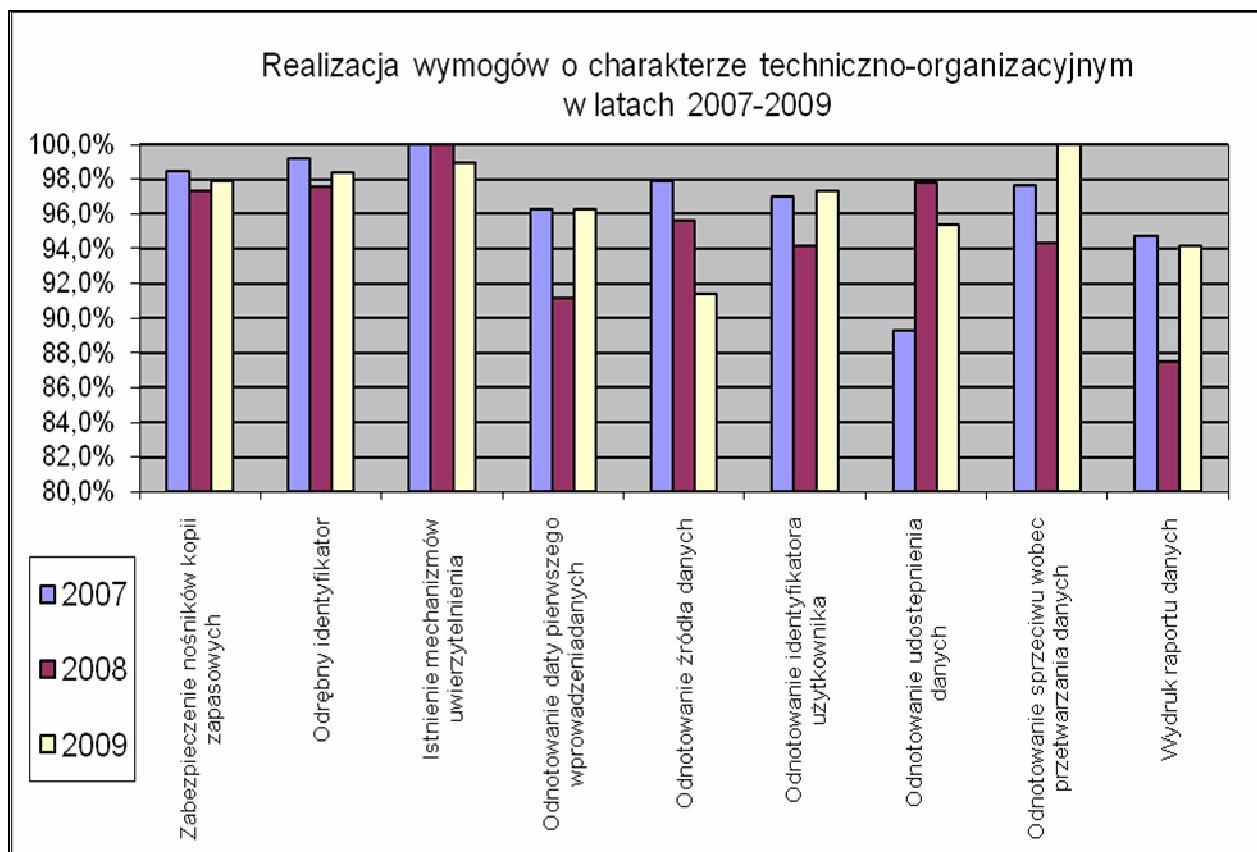
Wykres 31: Stopień realizacji obowiązku wyznaczenia osoby wykonującej zadania administratora bezpieczeństwa informacji w latach 2007–2009.

Zbiorcze zestawienie stopnia wypełnienia wymogów formalno-organizacyjnych i personalnych w zakresie dotyczącym prowadzenia dokumentacji przetwarzania danych osobowych, wdrożenia do stosowania opracowanej dokumentacji oraz wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji [ABI] w latach 2007-2009 przedstawia *Wykres 32*.



Wykres 32: 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 2007–2009.

Jednostkę statystyczną w zestawieniach odnoszących się do stopnia realizacji technicznych warunków przetwarzania danych stanowił kontrolowany system informatyczny. Poszczególne warunki uznawano dla kontrolowanego systemu jako wypełnione, 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. Stopień realizacji wymogów o charakterze techniczno-organizacyjnym dla systemów informatycznych objętych kontrolą w latach 2007-2009 przedstawiono na *Wykresie 33*.

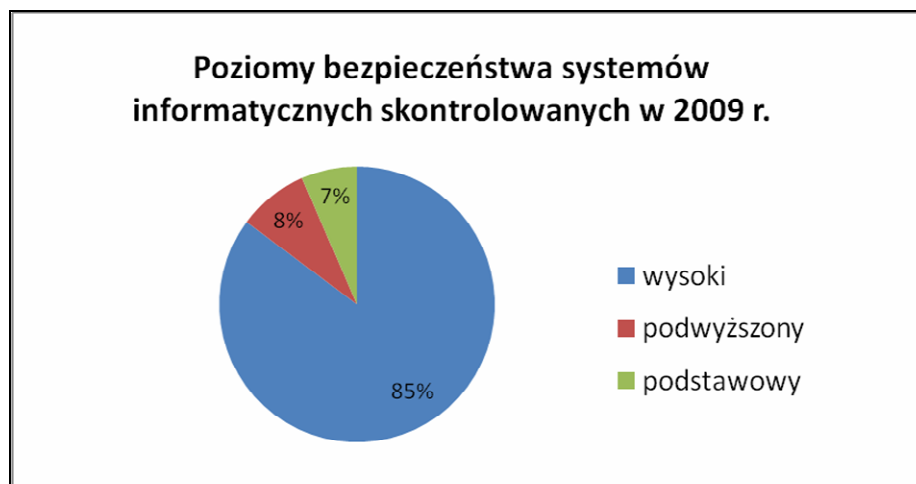


Wykres 33: Stopień realizacji wymogów technicznych i organizacyjnych w latach 2007 –2009.

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).

Jak już o tym wspomniano, w 2009 r. skontrolowano 424 systemy informatyczne służące do przetwarzania danych osobowych, tj. o 214 mniej niż w 2008 r. Główną przyczyną mniejszej liczby systemów informatycznych objętych kontrolami była większa ich integracja. Widoczne było to szczególnie na przykładzie skontrolowanego w 2009 roku sektora „Komornicy”. W sektorze tym prawie u wszystkich komorników użytkowany był jeden, wielomodułowy system informatyczny, który wspomagał zarówno prowadzenie poszczególnych spraw egzekucyjnych, jak i inne czynności wykonywane w kancelariach komorniczych, w tym rejestrację pism przychodzących i wychodzących. Daje się zauważyć, że coraz częściej administratorzy używają specjalistycznych systemów informatycznych, które często służą do przetwarzania kilku różnych zbiorów danych.

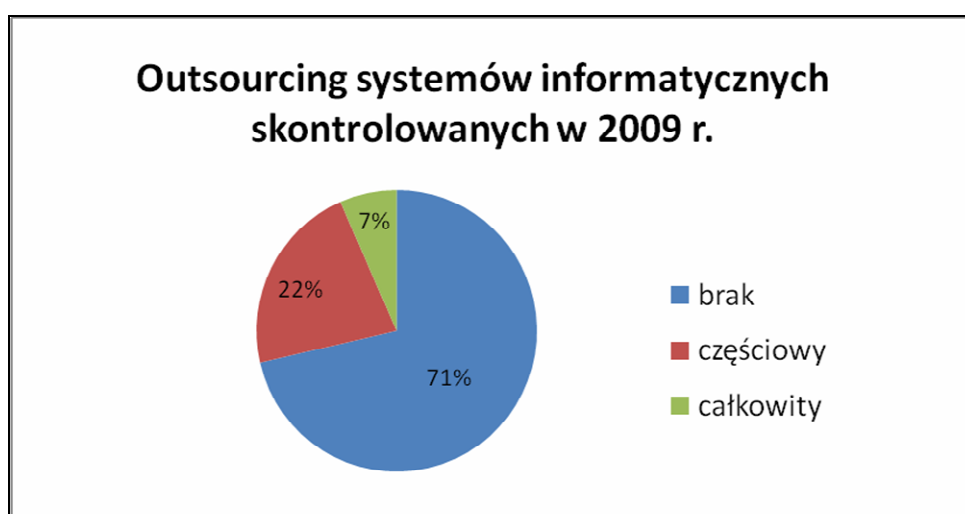
W odniesieniu do skontrolowanych w 2009 r. systemów informatycznych ustalono, że udział poszczególnych systemów, w zależności od przyjętego **poziomu bezpieczeństwa**, przedstawiał się jak na Wykresie 34.



Wykres 34: Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych skontrolowanych w 2009 r.

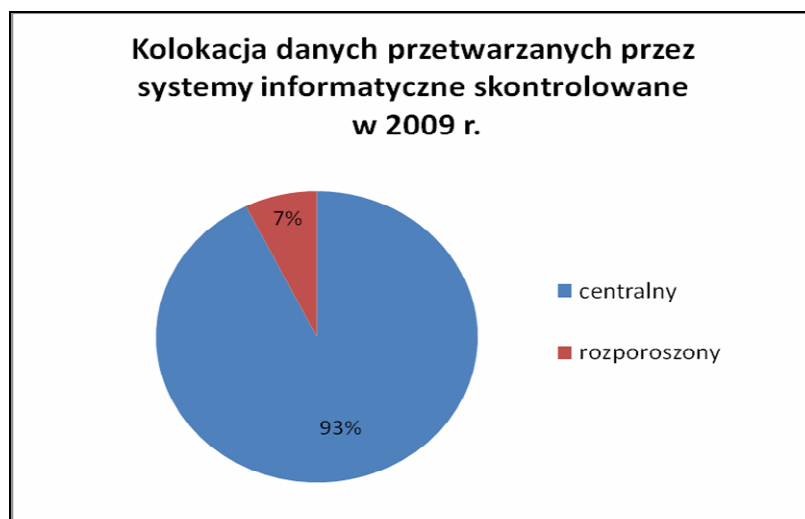
Jak wynika z zaprezentowanego wyżej podziału, znaczna część (tj. 85 %) skontrolowanych w 2009 r. systemów informatycznych służących do przetwarzania danych osobowych posiada dostęp do publicznej sieci Internet, co ma istotny wpływ na bezpieczeństwo w procesie przetwarzania danych osobowych.

Ponad 70 % systemów informatycznych poddanych kontroli w 2009 r. zarządzanych było w sposób samodzielny przez użytkujące je podmioty. Około 7 % skontrolowanych systemów informatycznych użytkowanych było na zasadzie całkowitego outsourcingu, gdzie proces przetwarzania danych osobowych (oprogramowanie oraz sprzęt teleinformatyczny) administrator danych powierzył w całości do administrowania podmiotom zewnętrznym.



Wykres 35: Procentowy udział outsourcingu systemów informatycznych objętych kontrolami w 2009 r.

Analizując systemy informatyczne pod względem kolokacji danych (fizycznej lokalizacji danych) należy zauważyć, że u większości skontrolowanych podmiotów dane osobowe zapisywane były w jednym, centralnym miejscu, np. na serwerze/serwerach znajdujących się w jednym budynku, zazwyczaj w siedzibie kontrolowanego podmiotu. Ilościowe wyniki w tym zakresie przedstawiono na poniższym wykresie.



Wykres 36: Procentowy udział centralnego przetwarzania danych w systemach informatycznych objętych kontrolami w 2009 r.

Jak ilustruje Wykres 37, w 2009 r. ustalono, że około 80% skontrolowanych systemów informatycznych stanowiły systemy wielostanowiskowe. Pozostałe systemy informatyczne były systemami jedno stanowiskowymi.



Wykres 37: Udział systemów informatycznych jedno- i wielostanowiskowych w ogólnej liczbie systemów objętych kontrolami w 2009 r.

Oceniając wyniki przeprowadzonych kontroli stwierdzić należy, że znaczna część kontrolowanych jednostek miała problemy z zastosowaniem odpowiednich środków technicznych

i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniami przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Ponad 12 % kontrolowanych podmiotów miała także problem z prawidłowym opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych. Wiele zastrzeżeń wzbudzały także stosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń i kategorii danych objętych ochroną, tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Nieprawidłowości w tym zakresie stwierdzono w szczególności w toku kontroli pracodawców. 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 z większości 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 m.in. niedopełnienia obowiązku zgłoszenia do rejestracji Generalnemu Inspektorowi prowadzonych zbiorów danych osobowych, niedopełnienia obowiązku dokonania aktualizacji zgłoszonych zbiorów danych oraz zbierania w szerszym zakresie danych osobowych niż wynika to z przepisów prawa lub w zakresie nieadekwatnym do celu przetwarzania. Z porównania stopnia realizacji w latach 2007-2009 poszczególnych wymogów ustawy i rozporządzenia wynika, że w roku 2009 odnotowano, w porównaniu do roku 2008, w większości przypadków tendencję wzrostową w zakresie realizacji wymagań formalno-organizacyjnych czy też wymagań o charakterze technicznym.

Tendencje spadkowe w porównaniu do wyników z roku 2008 dotyczą m.in.: braku lub niewłaściwego wdrożenia mechanizmów kontroli dostępu do danych przetwarzanych w systemach informatycznych, braku bądź niewłaściwego wdrożenia funkcjonalności dotyczącej zapewnienia przez system informatyczny odnotowania informacji o źródle danych, w przypadku zbierania informacji nie od osoby, której dane dotyczą oraz zapewnienia przez system informatyczny odnotowania informacji o odbiorcach danych, dacie i zakresie udostępnienia. Spadek stopnia realizacji ww. wymogów kształtował się na poziomie od 1 % do 4 %.

W 2009 r. poziom realizacji obowiązków związanych z prowadzeniem dokumentacji stanowiącej politykę bezpieczeństwa, instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, opracowaniem ewidencji osób upoważnionych do przetwarzania danych osobowych, jak również poziom realizacji obowiązku wyznaczenia osoby pełniącej zadania

administratora bezpieczeństwa informacji był wyższy niż w roku ubiegłym i kształtował się średnio na poziomie 93 %.

W odniesieniu do rozbudowanych systemów informatycznych zaobserwowano, że ich administratorzy stosowali najczęściej kompleksowe podejście do administrowania bezpieczeństwem użytkowanych systemów i ochroną przetwarzanych danych. Ustalono, że większość skontrolowanych w 2009 r. systemów informatycznych pracowało pod kontrolą systemu operacyjnego MS Windows lub w środowisku sieci komputerowej zarządzanej przez system MS Windows. Nieliczne stacje robocze pracowały pod kontrolą systemu Linux lub MacOS. Systemy operacyjne Unix, Linux, BSD użytkowane były jako systemy operacyjne na mniejszej liczbie serwerów (odpowiednio 6 %, 10 %, 1% ogółu skontrolowanych systemów informatycznych). W odniesieniu do poddanych kontroli systemów bazodanowych ustalono, że najczęściej spotykanymi bazami były: MySQL - 20 %, PostgreSQL - 28 % oraz Oracle - 11,6 %.

W 2009 r. - podobnie jak w roku 2008 - najczęściej stosowanym mechanizmem zabezpieczającym dostęp do danych był standardowy proces logowania, polegający na wprowadzaniu przy użyciu klawiatury identyfikatora użytkownika oraz hasła. Proces ten stosowany był w 98 % wszystkich systemów. Pomimo faktu, iż skontrolowane systemy informatyczne dysponowały mechanizmem uwierzytelnienia, mechanizm ten nie był we wszystkich przypadkach właściwie stosowany. Niewłaściwe w procesie logowania było m.in. wykorzystywanie jednego identyfikatora logowania przez więcej niż jedną osobę, wykorzystywanie wspólnego hasła logowania, nieodpowiednie konstruowanie hasła czy też zmiana hasła rzadziej niż raz na 30 dni. W 2009 r. zaobserwowano ponadto znaczną liczbę uchybień polegających na niezastosowaniu środków kryptograficznej ochrony dla procesu teletransmisji danych poprzez sieć publiczną Internet. Uchybienia te polegały na braku lub niewłaściwej implementacji zastosowanego mechanizmu kryptograficznego (przeważnie protokołu https).

Obowiązki określone w przepisach o ochronie danych nie były wykonywane przez jednostki kontrolowane najczęściej z powodu błędnej interpretacji tych przepisów oraz ich niekonsekwentnego stosowania. Częstą przyczyną był również, jak wskazywali administratorzy danych, brak odpowiednich środków finansowych niezbędnych do pokrycia kosztów związanych z wdrożeniem rozwiązań zapewniających prawidłowe spełnienie wymogów. W niektórych przypadkach przyczyny powyższego stanu rzeczy wynikały także z niewłaściwego podejścia osób odpowiedzialnych za przetwarzanie danych osobowych do problematyki ochrony tych danych, a nawet lekceważenia tych przepisów. Świadczy o tym, w szczególności niewykonywanie tych obowiązków, które nie pociągają za sobą nadmiernych kosztów finansowych, na przykład brak ewidencji osób upoważnionych do przetwarzania danych osobowych, czy też niewyznaczenie administratora bezpieczeństwa informacji. Jednocześnie należy wskazać, że wśród jednostek poddanych w 2009 r. kontroli były podmioty, dla których ochrona

przetwarzanych danych osobowych jest ważnym zagadnieniem. Do podmiotów tych należą głównie urzędy pracy, które w zdecydowanej większości zastosowały takie środki techniczne i organizacyjne, które w sposób odpowiedni zabezpieczyły przetwarzane dane osobowe.

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

W 2009 r. przed sądami administracyjnymi zapadło 9 orzeczeń dotyczących decyzji wydanych na skutek przeprowadzonych kontroli (w tym jedno postanowienie Naczelnego Sądu Administracyjnego o wstrzymaniu wykonania zaskarżonej decyzji) oraz jedno dotyczące udostępnienia akt kontroli.

Do najistotniejszych rozstrzygnięć dotyczących legalności przetwarzania danych osobowych należało orzeczenie Naczelnego Sądu Administracyjnego z 1 grudnia 2009 r. (sygn. akt I OSK 249/09), który oddalił skargę na decyzję Generalnego Inspektora w przedmiocie nakazu usunięcia uchybień w procesie przetwarzania danych poprzez usunięcie i zaprzestanie zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników. W toku postępowania administracyjnego ustalono, że w celu ewidencji czasu pracy pracodawca skanował linie papilarne palców dłoni pracowników. Zeskanowany obraz (charakterystyczne punkty linii papilarnych) był następnie przetwarzany na zapis cyfrowy (kod cyfrowy). Linie papilarne palca przyłożonego przez pracownika do czytnika były porównywane z zapisanym kodem w celu ewidencji wejść i wyjść z pracy. Pracownicy składali pisemne oświadczenia o wyrażeniu zgody na pobranie wzoru linii papilarnych. Sąd podzielił stanowisko Generalnego Inspektora wyrażone w zaskarżonej decyzji i wskazał w uzasadnieniu wyroku, iż wyrażona na prośbę pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie danych osobowych narusza prawa pracownika i swobodę wyrażenia przez niego woli, ze względu na zależność pracownika od pracodawcy i brak równowagi w relacji pracodawca – pracownik. Uznanie takiego oświadczenia woli za przesłankę legalizującą przetwarzanie danych osobowych pracownika stanowiło, zdaniem Sądu, obejście art. 22¹ Kodeksu pracy, ustanawiającego katalog danych osobowych, których pracodawca może żądać od pracownika. Jednocześnie rozszerzenie zakresu danych prowadzi do naruszenia zasady adekwatności wyrażonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którą dane powinny być adekwatne w stosunku do celów, w jakich są przetwarzane. Sąd stwierdził, iż przetwarzanie danych biometrycznych w celu ewidencji czasu pracy jest nieproporcjonalne do zamierzonego celu ich przetwarzania.

Naczelny Sąd Administracyjny wyrokiem z 1 grudnia 2009 r. (sygn. akt II OSK 227/09), potwierdził również zasadność dokonanego przez Generalnego Inspektora rozstrzygnięcia dotyczącego przyznania bankowi przymiotu administratora danych użytkowników przedpłaconych kart płatniczych, a także uznania, iż przesłankę przetwarzania takich danych powinna stanowić zgoda wyrażona przez użytkownika. Bank nie pozyskiwał zgody na przetwarzanie danych osobowych użytkowników kart, nie realizował również wobec nich obowiązku informacyjnego wynikającego z art. 25 ust. 1 ustawy o ochronie danych osobowych, gdyż uznawał, iż nie przysługuje mu przymiot administratora tych danych. Sąd wskazał na dokonanie przez Generalnego Inspektora prawidłowej oceny w zakresie uznania banku za administratora danych i konieczności spełniania przez bank obowiązku informacyjnego oraz uzyskania zgody na przetwarzanie danych osobowych.

Poddanie weryfikacji sądowej decyzji administracyjnej, w której nakazano zaprzestanie przetwarzania danych osobowych bez podstawy prawnej, opracowanie dokumentacji opisującej sposób przetwarzania danych osobowych oraz wyznaczenie administratora bezpieczeństwa informacji, doprowadziło do wydania 10 czerwca 2009 r. przez Wojewódzki Sąd Administracyjny w Warszawie wyroku (sygn. akt II SA/Wa 124/09) oddalającego skargę stowarzyszenia będącego stroną postępowania. Sąd stwierdził, że stowarzyszenie powinno legitymować się przynajmniej jedną przesłanką przetwarzania danych osób niebędących jego członkami. Sąd uznał, iż przesłanki legalizującej przetwarzanie danych w związku z prowadzeniem działalności nieujętej w statucie stowarzyszenia, nie może stanowić prawnie usprawiedliwiony cel administratora danych, a jedynie zgoda osób, których dane dotyczą. Jednocześnie sąd podkreślił, że nie jest wystarczające samo powiadomienie o zamiarze przetwarzania danych oraz brak sprzeciwu zainteresowanej osoby. Ponadto fakt udzielenia zgody nie może budzić wątpliwości, a co za tym idzie administrator danych powinien wykazać, że została ona faktycznie udzielona.

Do ważnych orzeczeń Naczelnego Sądu Administracyjnego należy również wyrok z 5 stycznia 2010 r. (sygn. I OSK 399/09), w którym sąd, oddalając skargę na decyzję Generalnego Inspektora, uznał, że dealer samochodowy ma obowiązek uzyskania zgody na przetwarzanie danych osobowych od potencjalnych klientów, tj. osób, które są zainteresowane kupnem samochodu, a nie brały udziału w jeździe testowej. Przetwarzanie danych na podstawie umowy dealerskiej nie mieści się bowiem w ramach marketingu własnych produktów lub usług i w związku z tym nie może odbywać się na podstawie 23 ust. 1 pkt 5 ustawy, tzn. jako prawnie usprawiedliwiony cel administratora danych.

W porównaniu z poprzednimi latami, w 2009 r. można już zauważyć niewielki wzrost liczby **skarg**, które wpłynęły do Biura GODO. W roku 2008 wpłynęło 986 skarg, zaś w 2009 – 1049, czyli o 63 skargi więcej. Niemniej jednak ich ocena pod kątem znajomości zasad ochrony danych osobowych niezmiennie prowadzi do wniosku, iż zagadnienia te w dalszym ciągu przysparzają sporo

problemów podmiotom z sektora publicznego i prywatnego. Z treści rozpatrywanych w 2009 r. skarg wynika, że podobnie jak w latach ubiegłych można zauważyć zbyt liberalne podejście przez administratorów danych do kwestii dostępu do informacji publicznych zawierających dane osobowe przetwarzane przez konkretny organ administracji. Realizując obowiązek ujawniania informacji o sprawach publicznych, administratorzy danych często pomijali fakt istnienia prawa z ustawy o ochronie danych osobowych i publikowali informacje zawierające dane osobowe w zbyt szerokim zakresie. Wspomniane przypadki dotyczyły np. ujawniania oświadczeń majątkowych funkcjonariuszy publicznych wraz z zawartymi w nich informacjami o współmałżonku, adresie zamieszkania, ewentualnie adresach nieruchomości stanowiących własność osoby, której oświadczenie dotyczyło, albo publikacji oświadczeń majątkowych za ubiegłe lata w sytuacji zaprzestania pełnienia przez skarżącego funkcji, w związku z którą oświadczenia te złożył. W opinii GODO podmioty sektora administracji publicznej nadal mają problemy z przyznawaniem danej informacji miana informacji publicznej i jej ewentualnym udostępnianiem zgodnie/niezgodnie z przepisami prawa. W takich sytuacjach organ ds. ochrony danych osobowych wskazywał, że decyzja w tej materii każdorazowo leży po stronie podmiotu, który tą informacją dysponuje oraz podlega weryfikacji sądowej. Dodać również 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.

Znaczna liczba skarg dotyczyła również kwestii niewłaściwego zabezpieczenia danych osobowych. W większości przypadków, podobnie jak w poprzednich okresach sprawozdawczych, przyczyną naruszeń przepisów w tym zakresie było zarówno niedostateczne techniczne zabezpieczenie przetwarzania danych, jak i 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. Przykładem tego rodzaju spraw były skargi na działania komorników sądowych i naczelników urzędów skarbowych przesyłających wezwania pozbawione koperty, a także na operatorów telekomunikacyjnych czy na pracowników urzędów miejskich, którzy dostarczając niezabezpieczoną korespondencję wobec nieobecności adresata zastawiali ją sąsiadowi bądź w drzwiach mieszkań. Zdarzały się też skargi na przypadki znakowania kopert z korespondencją, tak jak to było w przypadku jednej z firm ubezpieczeniowych, która zamieściła na kopercie listu skierowanego do skarżącego, oznaczenie – „opiekun nieletniego sprawcy”. W takich przypadkach organ korzystał ze swojej ustawowej kompetencji i występował do administratorów danych z wnioskami o wszczęcie postępowań dyscyplinarnych wobec osób odpowiedzialnych za sprzeczne z przepisami prawa

przetwarzanie danych osobowych, a także wysyłał sygnalizacje, których celem było zapewnienie należytego poziomu ochrony danych osobowych przez administratora.

Spośród skarg kierowanych pod adresem banków i innych instytucji finansowych najczęściej odnosiło się do przetwarzania danych osobowych przez Biuro Informacji Kredytowej, do którego skarżący zwracali się o nakazanie zaktualizowania danych osobowych bądź ich usunięcie, a także spełnienia przez podmioty z tego sektora obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych i większą dbałość o należyte zabezpieczenie danych osobowych przed dostępem do nich osób nieuprawnionych. W odniesieniu do tego ostatniego zaznaczyć należy, że w 2009 r. pojawiła się nowa praktyka stosowana przez banki – telefoniczna weryfikacja danych kredytobiorcy u jego pracodawcy. Generalny Inspektor Ochrony Danych Osobowych informował, że zgodnie z art. 36 ust. 1 ustawy o ochronie danych osobowych, na pracodawcy – jako administratorze danych osobowych - spoczywa obowiązek zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym. W przypadku telefonicznej weryfikacji danych dotyczących osoby występującej z wnioskiem o przyznanie kredytu, np. w zakresie wysokości jej wynagrodzenia, pracodawca nie może z całą pewnością stwierdzić, iż osoba telefonująca do niego w celu zweryfikowania danych rzeczywiście jest przedstawicielem banku, a więc osobą upoważnioną do pozyskania tego typu informacji. W opinii GODO taka praktyka stosowana przez banki jest niedopuszczalna z punktu widzenia ochrony danych osobowych i wskazał również na pismo Narodowego Banku Polskiego - Generalnego Inspektora Nadzoru Bankowego z dnia 6 kwietnia 2001 r. (NB/BPN/I/214/01) skierowane do osób kierujących bankami, które zawiera stwierdzenie, iż „przepisy ustawy - Prawo bankowe i ustawy o ochronie danych osobowych nie przewidują telefonicznej formy pozyskiwania żądanych informacji. Banki nie mogą więc uzależniać przyznania kredytu od udzielenia informacji w tej formie”.

Podobnie jak w poprzednich okresach sprawozdawczych, tak i w 2009 r. nadal napływały skargi na administratorów przetwarzających dane osobowe w celach marketingowych bez zgody osoby, której dane te dotyczyły, lub pomimo wniesienia przez nią sprzeciwu, na wspólnoty i spółdzielnie mieszkaniowe udostępniające dane osobowe najemców osobom nieupoważnionym poprzez wywieszanie ich na klatkach schodowych, tablicach ogłoszeń czy też poprzez publikowanie w uchwałach oraz na praktyki wykonywania zdjęć i kopii dokumentów tożsamości przez firmy ubezpieczeniowe i pozyskiwanie przez nie danych osobowych klientów w zbyt szerokim zakresie.

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 lekceważeniu ustawowych regulacji dotyczących analizowanej problematyki. W takich sprawach Generalny Inspektor Ochrony Danych Osobowych konsekwentnie wydawał decyzje nakazujące jego spełnienie.

W podsumowaniu należy stwierdzić, że przyczyn niewielkiego wzrostu liczby skarg, które wpłynęły do GIODO w 2009 r. należy upatrywać przede wszystkim we wzroście świadomości społeczeństwa co do zasad ochrony danych osobowych i jego aktywności w dochodzeniu przysługujących mu praw.

Istotną rolę w strzeżeniu praworządności w obszarze ochrony danych osobowych jest wynikające z art. 19 ustawy o ochronie danych osobowych uprawnienie Generalnego Inspektora do kierowania (w przypadku uzasadnionego podejrzenia popełnienia przestępstwa) do organu powołanego do ścigania przestępstw, **zawiadomienia o popełnieniu przestępstwa**.²¹⁴ W omawianym okresie sprawozdawczym Generalny Inspektor 27 razy skorzystał z tego uprawnienia. Niestety, w dalszym ciągu utrzymuje się duża liczba 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 GIODO, 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 nieznaną przepisów o ochronie danych osobowych oraz bezzasadną oceną przypadków złamania tej ustawy jako czynów o znikomej społecznej szkodliwości. Dlatego do Sejmu RP wniesiony został prezydencki projekt ustawy o zmianie ustawy o ochronie danych osobowych wyposażający organ ds. ochrony danych osobowych w bardziej skuteczne instrumenty egzekwowania prawa.

Z kolei analiza **projektów aktów normatywnych** przesyłanych w 2009 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 lub takiego formułowania przepisów, z których wynika dowolność zakresu przetwarzanych danych w zależności od swobodnego uznania administratora.

²¹⁴ Zgodnie z treścią art. 19 ustawy o ochronie danych osobowych: w razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Nieprawidłowości najczęściej pojawiające się w opiniowanych projektach aktów prawnych najczęściej dotyczyły braku doprecyzowania zakresu przetwarzania danych, np. poprzez używanie ogólnych sformułowań, jak *„odpowiednie zaświadczenia wydawane w określonych państwach”* albo *„inne rodzaje dokumentów”*, regulowanie kwestii ochrony danych osobowych w aktach o randze niższej niż ustawa,²¹⁵ tendencja do coraz większej ingerencji w prawo do ochrony danych osobowych, argumentowana koniecznością usprawnienia działalności danej instytucji, np. w odniesieniu do instytucji finansowych - zniesienia barier dla celów oceny zdolności kredytowej i analizy ryzyka kredytowego, pobierania od osoby, której dane dotyczą, opłaty za udzielenie jej przez administratora danych informacji, o których mowa w art. 33 ust. 1 ustawy o ochronie danych osobowych, a także niezachowania szczególnej ostrożności w kwestii przetwarzania danych tzw. szczególnie chronionych. Generalny Inspektor Ochrony Danych Osobowych sceptycznie odniósł się także do propozycji wprowadzenia „jednolitego europejskiego numeru identyfikacyjnego dla celów kredytowych” zawartej w jednym z opiniowanych projektów. Powyższe mogłoby bowiem doprowadzić do podobnych skutków, jak stworzenie ogólnoeuropejskiej bazy kredytowej. Zdaniem organu, przyjęte rozwiązania powinny raczej zmierzać w kierunku weryfikowania tożsamości klienta w oparciu o już istniejące w danym państwie członkowskim rejestry zawierające dane osobowe.

Natomiast w związku z pracami legislacyjnymi nad innym projektem,²¹⁶ Generalny Inspektor zaoponował nie tylko przeciwko niektórym z zawartych w tym projekcie propozycjom unormowań, ale również trybowi ich wprowadzenia do dokumentu. Zwrócił bowiem uwagę, że pomimo iż projektodawcy zapowiedzieli skierowanie do Generalnego Inspektora Ochrony Danych Osobowych pytania w przedmiocie opiniowanego projektu, to jednak tego nie zrobili i bez konsultacji zamieścili przedmiotową regulację.

W tym miejscu należy jednak 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 prawniczych.

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 obywateli polskich na granicach wewnętrznych Unii Europejskiej. Gwarantuje on, że każde państwo będące stroną Konwencji Wykonawczej do Układu z Schengen [KWS] będzie posiadało zestaw informacji pozwalających na dostęp – przy użyciu

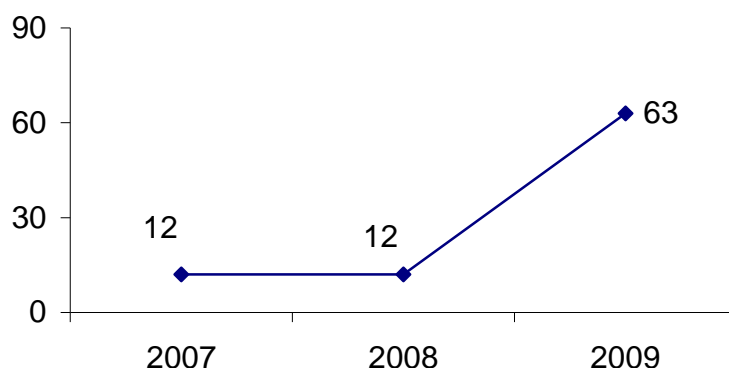
²¹⁵ Ustawa bowiem jest zasadniczym źródłem prawa, na co wskazuje Konstytucja Rzeczypospolitej Polskiej ustanawiająca zasadę wyłączności regulacji ustawowej.

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. Z chwilą włączenia Polski w dniu 21 grudnia 2007 r. do systemu Schengen zadania Generalnego Inspektora Ochrony Danych Osobowych zostały poszerzone 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.

W 2009 r. Generalny Inspektor Ochrony Danych Osobowych brał aktywny udział w pracach Biura Komitetu Konsultacyjnego Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (T-PD) nad projektem rekomendacji w sprawie ochrony osób w związku z przetwarzaniem danych osobowych podczas profilowania (*Draft Recommendation on the Protection of Individuals with regard to Automatic Processing of Personal Data in the framework of Profiling*). Zjawisko profilowania polegające na pozyskiwaniu oraz analizowaniu informacji na temat użytkowników wykorzystujących nowoczesne technologie staje się coraz bardziej powszechne. Z profilowaniem związane jest najczęściej przetwarzanie informacji o charakterze osobowym, w tym między innymi danych o ruchu w sieci, danych rejestrowanych przez wyszukiwarki internetowe, pozwalających na prześledzenie aktywności użytkowników w sieci oraz ich nawyków, upodobań konsumenckich lub zainteresowań, danych geolokalizacyjnych zgromadzonych przez operatorów sieci telefonii komórkowej lub systemy video nadzoru bądź systemy identyfikacji za pomocą fal radiowych (RFID). Tego rodzaju praktyki mogą prowadzić do poważnych naruszeń w sferze prywatności i ochrony danych użytkowników. W związku z powyższym organy ochrony danych osobowych współpracujące w ramach forum T-PD postanowiły opracować zestaw wytycznych zawartych w projektowanej obecnie rekomendacji w celu wyeliminowania zagrożeń dla prywatności mogących pojawić się podczas tworzenia profili użytkowników. W trakcie prac nad projektem rekomendacji Generalny Inspektor Ochrony Danych Osobowych opowiedział się za wyłączeniem z jej zakresu kwestii dotyczących przetwarzania danych osobowych w celach związanych z obronnością i bezpieczeństwem wewnętrznym oraz uregulowaniem ich w innym, odpowiednim akcie (np. w Rekomendacji (87) 15 o wykorzystywaniu danych osobowych w sektorze policji). GIODO, opiniując załącznik do wspomnianego projektu rekomendacji, zaproponował rozszerzenie zakresu informacji, które powinny być przekazywane osobom, których dane dotyczą, o informacje na temat odbiorców tych danych, a także przyznanych uprawnień osób mających na celu ochronę ich prywatności, jak również zwrócił uwagę na kwestie terminologiczne.

²¹⁶ Projekt ustawy o centralnej ewidencji pojazdów i centralnej ewidencji kierowców oraz o zmianie niektórych innych ustaw (projekt z dnia 1 czerwca 2009 r.) DOLiS-033-325/08.

W 2009 r. do Generalnego Inspektora wpłynęły **54 wnioski o udzielenie zgody na przekazanie danych osobowych do państwa trzeciego**, czyli o 26 wniosków więcej niż w roku 2008. Jednocześnie Generalny Inspektor wydał 63 decyzje administracyjne. W porównaniu z poprzednimi latami jest to największy wzrost liczby decyzji wydanych przez Generalnego Inspektora w tym zakresie.



Wykres 38: Zestawienie porównawcze liczby decyzji dotyczących wyrażenia zgody na przekazanie danych osobowych do państwa trzeciego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2009.

W 61 sprawach Generalny Inspektor zezwolił na przekazanie danych, w tym w 3 sprawach równocześnie częściowo umorzył postępowanie ze względu na przekazywanie danych do Kanady. Kraj ten bowiem - zgodnie z decyzją Komisji Europejskiej z dnia 20 grudnia 2001 r. w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych - zapewnia adekwatny poziom ochrony danych osobowych.²¹⁷ W jednej sprawie GODO częściowo umorzył postępowanie ze względu na rezygnację wnioskodawcy z części wniosku,²¹⁸ w innej umorzył postępowanie ze względu na to, że odbiorca danych należał do amerykańskiego programu „bezpiecznej przystani”,²¹⁹ natomiast w kolejnej sprawie umorzenie postępowania było spowodowane wycofaniem złożonego wniosku.²²⁰

Znacząca część wniosków dotyczyła m.in. przekazywania danych pracowników, klientów, dostawców (oraz innych podobnych kategorii osób) w ramach jednej międzynarodowej grupy kapitałowej/korporacji, w celu ujednolicenia procesów zarządzania zasobami ludzkimi, prowadzenia rachunkowości lub zwiększeniem bezpieczeństwa danych poprzez zastosowanie jednolitych praktyk oraz procedur (bądź zlecenie takich zadań podmiotom trzecim tzw. *outsourcing*). Zmieniła się też i znacznie powiększyła liczba państw, do których administratorzy danych zamierzali przekazywać dane. Wśród nich najczęściej wymieniane były Stany Zjednoczone Ameryki oraz Republika Indii.

²¹⁷ DESiWM/DEC-976/35238/09, DESiWM/DEC1146/42078/09, DESiWM/DEC-1291/47885/09.

²¹⁸ DESiWM/DEC-1219/45176/09.

²¹⁹ DESiWM/DEC-270/11420/09.

Wnioski dotyczyły także: Arabskiej Republiki Egiptu, Boliwariańskiej Republiki Wenezueli, Brytyjskiej Wyspy Dziewiczej, Chińskiej Republiki Ludowej (oraz Specjalnego Regionu Administracyjnego Hongkongu), Federacji Rosyjskiej, Federacji Malezji, Federacyjnej Republiki Brazylii, Republiki Indonezji, Islamskiej Republiki Pakistanu, Jamajki, Japonii, Kanady, Królestwa Marokańskiego, Królestwa Tajlandii, Nowej Zelandii, Państwa Izraela, Republiki Argentyńskiej, Republiki Chile, Republiki Chińskiej, Republiki Chorwacji, Republiki Dominikańskiej, Republiki Ekwadoru, Republiki Filipin, Republiki Gwatemali, Republiki Kolumbii, Republiki Korei, Republiki Kostaryki, Republiki Kuby, Republiki Panamy, Republiki Peru, Republiki Południowej Afryki, Republiki Salwadoru, Republiki Singapuru, Republiki Turcji, Socjalistycznej Republiki Wietnamu, Wolnego Stowarzyszonego Państwa Portoryko, Wschodniej Republiki Urugwaju, Zjednoczonych Emiratów Arabskich oraz Związku Australijskiego.

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 Europejską²²¹ oraz wiążące reguły korporacyjne.²²² 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

²²⁰ DESiWM/DEC-887/32565/09.

²²¹ Komisja Europejska, na mocy art. 26 ust. 4 dyrektywy 95/46/WE, jest uprawniona do uznania w drodze decyzji, że określone standardowe klauzule umowne zapewniają odpowiednią ochronę danych osobowych oraz praw i wolności jednostek. Decyzje te wymagają, aby Państwa Członkowskie nie odmawiały uznania zabezpieczeń ustanowionych w standardowych klauzulach umownych określonych w decyzjach za zapewniające odpowiedni poziom ochrony danych osobowych. Nie wyłącza to jednak obowiązku spełnienia pozostałych wymogów nałożonych przez właściwe przepisy krajowe. Komisja Europejska wydała trzy takie decyzje: decyzję KE z dnia 15 czerwca 2001 r. 2001/497/WE w sprawie standardowych klauzul umownych w związku z przekazywaniem danych osobowych do państw trzecich na podstawie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 181/19 z 4.07.2001); decyzję z dnia 27 grudnia 2004 r. 2004/915/WE zmieniającą decyzję 2001/497/WE w zakresie alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz. Urz. WE L 385/19 z 29.12.2004). Powołane decyzje wprowadziły dwa zestawy klauzul umownych, które administrator danych może wykorzystać w przypadku przekazywania danych do innego administratora danych w państwie trzecim. Trzecia decyzja KE z dnia 27 grudnia 2001 r. 2002/16/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych przetwarzanych w krajach trzecich na podstawie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. UE L 006 z 10.01.2002) wprowadziła standardowe klauzule umowne mające zastosowanie do przekazywania danych osobowych w przypadku powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy o ochronie danych osobowych.

²²² 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.

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 wpływały wnioski, w których administratorzy danych najczęściej powoływali się na zastosowanie wspomnianych standardowych klauzul umownych, ustanowionych przez Komisję Europejską. Administratorzy danych nie korzystali natomiast z innych rozwiązań umownych. Jak dotąd nie wpłynęły do Generalnego Inspektora formalne wnioski o wyrażenie zgody na przekazanie danych do państwa trzeciego na podstawie wiążących reguł korporacyjnych, aczkolwiek GODO, wraz z innymi organami ochrony danych osobowych, uczestniczył w kilku procedurach koordynacyjnych mających na celu wypracowanie przez międzynarodowe korporacje wiążących reguł korporacyjnych. Zadeklarowanie przez wnioskodawcę zastosowania standardowych klauzul umownych określonych decyzjami Komisji Europejskiej powoduje konieczność porównania przez Generalnego Inspektora przyjętych przez wnioskodawcę rozwiązań z treścią standardowych klauzul umownych. Ponadto Generalny Inspektor szczegółowo bada okoliczności planowanego transferu danych (w tym również przyjęte przez odbiorcę danych środki organizacyjno-techniczne).

Administratorzy danych często na podstawie standardowych klauzul umownych przygotowywali własne umowy. I choć były one różnie nazywane – „umowy globalne”, „umowy ramowe” czy też „umowy wewnątrz-korporacyjne”, to jednak w warstwie merytorycznej nie odbiegały one od standardowych klauzul umownych. W niektórych sytuacjach standardowe klauzule umowne stanowiły część bądź załącznik do ww. umów. Były też nieliczne podmioty, które w ramach umowy globalnej załączały zarówno standardowe klauzule umowne pomiędzy administratorami oraz klauzule dotyczące powierzenia przetwarzania danych.²²³

W tym miejscu warto wspomnieć o kwestii modyfikacji standardowych klauzul umownych, która była rozpatrywana w ramach jednego z postępowań.²²⁴ Co do zasady standardowe klauzule umowne zatwierdzone przez Komisję Europejską stanowią narzędzie umożliwiające przedsiębiorcom przeprowadzanie międzynarodowych transferów danych przy jednoczesnym zapewnieniu niezbędnych gwarancji praw i wolności osób, których dane dotyczą. Przewidziane zabezpieczenia wynikają **w całości z postanowień zapisanych w standardowych klauzulach umownych**. Jeśli podmiot decyduje się na wykorzystanie części, a nie całości klauzul, wówczas tracą one przymiot klauzul zatwierdzonych przez Komisję Europejską.

Niektóre z nadesłanych wniosków były obarczone brakami formalnymi. Do najczęściej spotykanych należały te, w których osoba podpisana pod wnioskiem nie była należycie umocowana

²²³ Np. DESiWM/DEC-133/6101/09, DESiWM/DEC-1291/47885/09.

²²⁴ DESiWM/DEC-1146/42078/09.

do reprezentowania spółki (czego potwierdzeniem był wyciąg z rejestru przedsiębiorców lub pełnomocnictwo podpisane przez osobę wymienioną w rejestrze), brak było załączników w postaci odpisu wyciągu z rejestru przedsiębiorców, i/lub pełnomocnictwa (czasem także dowodu uiszczenia opłaty skarbowej w wysokości 17 zł za pełnomocnictwo), do wniosku nie został załączony dowód zapłaty opłaty skarbowej w wysokości 10 zł za wydanie decyzji przez Generalnego Inspektora oraz przesłanie wniosku lub dokumentacji w języku obcym, podczas gdy zgodnie z ustawą z dnia 7 października 1999 r. o języku polskim (Dz. U. 1999 r. Nr 90, poz. 999 z późn. zm.), język polski jest językiem urzędowym na terytorium Rzeczypospolitej Polskiej. W związku z tym wszelkie dokumenty składane do Biura Generalnego Inspektora Ochrony Danych Osobowych powinny być tłumaczone na język polski, choć nie muszą to być tłumaczenia przysięgłe.

Zgodnie z art. 48 ustawy o ochronie danych osobowych, Generalny Inspektor, wyrażając zgodę na przekazanie danych osobowych do państwa spoza Europejskiego Obszaru Gospodarczego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Polski, musi ocenić, czy administrator danych zapewnił odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osób, których dane dotyczą. Oceny tej dokonuje z uwzględnieniem tych samych przesłanek, co przy ogólnej ocenie poziomu ochrony w danym państwie trzecim (art. 25 ust. 2 dyrektywy 95/46/WE). W ramach tej oceny Generalny Inspektor bierze pod uwagę środki prawne mające na celu zagwarantowanie praw i wolności osób, których dane dotyczą, w tym m.in. umów będących podstawą przekazania danych (np. standardowe klauzule umowne), a także środki organizacyjno-techniczne, które odbiorca danych w państwie trzecim zastosuje w celu zabezpieczenia przekazywanych danych. Na terytorium Rzeczypospolitej Polskiej aktem prawnym określającym minimalny poziom ochrony urządzeń i systemów informatycznych służących do przetwarzania danych osobowych jest 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 (Dz. U. z 2004 r. Nr 100, poz. 1024). W związku z powyższym administrator danych, poza przygotowaniem odpowiedniej podstawy prawnej, musi również sprawdzić, czy odbiorca danych spełnia minimalne wymagania określone w tym rozporządzeniu. Dlatego jeśli we wniosku, w załączniku do umowy o przekazanie danych bądź w innym dokumencie załączonym do wniosku (np. polityce prywatności) występować będą ogólne sformułowania dotyczące przyjętych przez odbiorcę danych środków organizacyjno-technicznych, nie zostaną one uznane za wystarczające do wydania zgody przez Generalnego Inspektora na transfer danych do państwa trzeciego.²²⁵

²²⁵ Np. „Załącznik A: Zasady przekazywania danych” do alternatywnych standardowych klauzul umownych stanowiących załącznik do decyzji Komisji Europejskiej 2004/915/WE z dnia 27 grudnia 2004 r. zmieniająca decyzję Komisji Europejskiej 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych

Najczęściej występującym brakiem merytorycznym dotyczącym przyjętych przez odbiorcę danych środków organizacyjno-technicznych było niespełnienie wymogów posiadania przez system informatyczny funkcjonalności w zakresie odnotowywania informacji, o której mowa w § 7 rozporządzenia MSWiA, oraz wymogów związanych z uwierzytelnianiem użytkowników (w przypadku, gdy do uwierzytelniania użytkownika wykorzystywane jest hasło - co do jego długości, złożoności i częstotliwości zmiany). Inne wady merytoryczne w tym zakresie to brak informacji o tym, czy dane osobowe będą przekazywane przy użyciu środków teletransmisji wykorzystujących sieci publiczne oraz związane z tym zabezpieczenia, informacji na temat sposobu zabezpieczenia transferu danych, środków kryptograficznej ochrony m.in. wobec danych wykorzystywanych do uwierzytelnienia, informacji na temat środków zabezpieczenia przed zagrożeniami pochodzącymi z sieci zewnętrznej, polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym oraz zabezpieczenia danych osobowych przetwarzanych na komputerach przenośnych.

W przedmiocie **zgłoszeń zbiorów danych osobowych do rejestracji**, do istotnych spraw związanych z ochroną danych osobowych, które miały miejsce w 2009 r., zaliczyć należy przede wszystkim wprowadzenie od 10 lutego 2009 r. nowego wzoru zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Wzór ten wprowadzony został na mocy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536). Głównym celem modyfikacji wzoru zgłoszenia było uproszczenie części E zgłoszenia dotyczącej informacji o środkach technicznych i organizacyjnych zastosowanych w celu zabezpieczenia danych. Po prawie rocznym okresie stosowania tego wzoru zgłoszenia można stwierdzić, iż cel ten został osiągnięty. Głównym tego przejawem jest wyraźne zmniejszenie liczby nieprawidłowo wypełnionych zgłoszeń – głównie w części E, co z kolei przekłada się na przyspieszenie postępowania rejestracyjnego. Wprowadzenie nowego wzoru zgłoszenia jest przede wszystkim ułatwieniem dla administratorów danych w spełnieniu obowiązku rejestracyjnego. Zmianie uległa bowiem forma prezentowania informacji w części D i E formularza zgłoszenia, a więc informacji o sposobie zbierania i udostępniania danych oraz opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy.

Należy zwrócić uwagę, że wraz z wprowadzeniem nowego formularza zgłoszenia zmienił się tylko sposób przekazywania informacji o zbiorach, natomiast nie zmienił się zakres informacji, jakie powinny znaleźć się w zgłoszeniu, który określony jest w art. 41 ust. 1 ustawy. Zatem wprowadzenie

dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE (Dz.Urz. WE L 385/19, z 29.12.2004) przedstawia jedynie ogólny zarys niektórych przyjętych przez odbiorcę danych środków organizacyjno-

nowego formularza zgłoszenia nie niosło za sobą obowiązku aktualizacji dokonanego już zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Nie wszyscy administratorzy prawidłowo zinterpretowali tę zasadę, co skutkowało przesyłaniem Generalnemu Inspektorowi Ochrony Danych Osobowych formularzy zgłoszeń – zdaniem administratorów w trybie art. 41 ust. 1 ustawy, z których w istocie nie wynikały żadne zmiany w zgłoszonym do rejestracji zbiorze danych. Wprawdzie wprowadzenie nowego wzoru zgłoszenia spowodowało zmniejszenie liczby nieprawidłowo wypełnionych zgłoszeń, wymagających prowadzenia postępowania wyjaśniającego, które przedłuża proces rejestracji zbioru, to jeszcze wielu administratorów nadsyła zgłoszenia, w stosunku do których zachodzi konieczności prowadzenia takich postępowań. Ujawniane nieprawidłowości dotyczyły w zasadzie wszystkich elementów ujętych w zgłoszeniu, wśród najczęściej powtarzających się uchybień należy wymienić nieadekwatny (zbyt szeroki), w stosunku do celu przetwarzania, zakres danych osobowych pozyskiwanych do zbioru.

Do charakterystycznych błędów popełnianych w 2009 r. przez administratorów w związku z realizacją obowiązku zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych należy zaliczyć wypełnienie jednego formularza zgłoszenia dla kilku zbiorów. Tymczasem treść art. 41 ust. 1 ustawy wskazuje, iż jedno zgłoszenie powinno obejmować swym zakresem tylko jeden zbiór danych osobowych. Przykładem administratorów, łamiących zasadę <<jedno zgłoszenie – jeden zbiór>> były jednostki samorządu terytorialnego (gminy, powiaty), które zgłaszały do rejestracji zbiór utworzony w związku z wdrożeniem elektronicznego systemu obiegu dokumentów. Jednakże prowadzone w tych sprawach postępowania wykazały, że zastosowanie przez te podmioty elektronicznego systemu obiegu dokumentów nie skutkowało powstaniem nowego zbioru danych osobowych, a przesłane zgłoszenia dotyczyły wielu zbiorów danych osobowych prowadzonych przez te podmioty z wykorzystaniem ww. systemu.

Należy również zasygnalizować, że w roku sprawozdawczym 2009 r., tak jak w roku 2008, wśród wniosków o rejestrację pochodzących od podmiotów prywatnych dominowały zgłoszenia od przedsiębiorców, którzy przetwarzając dane osobowe, wykorzystują sieć Internet. Najwięcej zgłoszeń do rejestracji, których prowadzenie jest związane z funkcjonowaniem sieci Internet, dotyczyło sklepów internetowych oraz serwisów związanych z pośrednictwem w zatrudnieniu. Do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były również zbiory danych dotyczące tzw. newsletterów, za pomocą których administratorzy powiadamiają swoich klientów m.in. o nowościach w swojej ofercie.

Część IV.

Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych

Ustawowym obowiązkiem Generalnego Inspektora Ochrony Danych Osobowych jest coroczne składanie Sejmowi sprawozdania ze swej działalności, w którym analiza spraw dotyczących naruszeń ochrony danych, wyników przeprowadzonych kontroli, wydanych opinii, przedsięwzięć legislacyjnych i innych działań ujętych w art. 12 ustawy o ochronie danych osobowych, stanowią podstawę do formułowania wniosków na temat stanu przestrzegania prawa o ochronie danych osobowych w Polsce. Sygnalizowana jest w nich konieczność, na przykład zmiany jakiejś praktyki w celu dostosowania jej do przepisów o ochronie danych osobowych, bądź też konieczność podjęcia działań w celu dostosowania obowiązujących przepisów prawa do zasad określonych w ustawie o ochronie danych osobowych. W szczególności wobec wyzwań nowych technologii ochrona prywatności i danych osobowych nabiera specyficznego wymiaru. Oczywiście jest na przykład to, że zarówno administrator danych, jak i podmiot danych powinni zadbać o bezpieczeństwo danych osobowych, ale z drugiej – nie można nie brać pod uwagę postępu cywilizacyjnego i osiągnięć nowoczesnych technologii, które mądrze zastosowane mogą okazać się bardzo pomocne w codziennym życiu.

Dlatego m.in. w związku z docierającymi do GODO sygnałami dotyczącymi niedostosowania obowiązujących przepisów prawa pracy do potrzeb zarówno pracodawców, jak i pracowników, Michał Serzycki zwrócił się do różnych środowisk z prośbą o opinię dotyczącą kierunków koniecznych zmian w przepisach prawa pracy w kontekście ochrony danych osobowych i prawa do prywatności. Po ich analizie wystąpił zaś do Ministerstwa Pracy i Polityki Społecznej z prośbą o rozważenie propozycji podjęcia prac legislacyjnych nad zmianą przepisów regulujących przetwarzanie danych osobowych pracowników i kandydatów do pracy przez pracodawców. Niemniej, w opinii Generalnego Inspektora, poprzedzić je powinna publiczna debata na temat dopuszczalnego zakresu danych pozyskiwanych przez pracodawców. Tym bardziej że obowiązujące przepisy prawa pracy stwarzają poważne trudności interpretacyjne, a temat ten wywołuje duże zainteresowanie społeczne. Potrzebne jest zaś opracowanie i wprowadzenie takich uregulowań prawnych, które wyważą interesy obu stron stosunku pracy – pracodawcom zapewnią właściwą kontrolę pracowników, a pracownikom zagwarantują prawo do ochrony ich prywatności.

Niezmiennie przez wszystkie lata sprawowania urzędu, Generalnego Inspektora wciąż niepokoi tendencja do pozyskiwania przez różne podmioty danych osobowych w zbyt szerokim zakresie w stosunku do celu ich przetwarzania i tworzenie megabaz takich danych.

Jako przykład podać można uregulowania dotyczące planowanego na 2011 r. powszechnego spisu ludności i mieszkań, którego przebieg będzie przedmiotem szczególnego zainteresowania GIODO.

Generalny Inspektor Ochrony Danych Osobowych w ramach swoich kompetencji prowadzi szeroko zakrojone działania informacyjno – edukacyjne. Edukowanie uznał bowiem za jeden ze swoich konsekwentnie realizowanych priorytetów, a wzrost świadomości społeczeństwa w zakresie ochrony danych osobowych stał się jego kluczowym zadaniem. Jest więc organizatorem i uczestnikiem wielu konferencji krajowych i międzynarodowych, podejmuje liczne inicjatywy upowszechniające wiedzę (np. wydawanie broszur na temat ochrony danych i prywatności, tworzenie specjalnych zakładki na portalach tematycznych i społecznościowych). Ponadto organizuje bezpłatne szkolenia i warsztaty adresowane głównie do przedstawicieli administracji rządowej i samorządowej. Od czasu objęcia funkcji GIODO w lipcu 2006 r. w szkoleniach tych udział wzięło kilkanaście tysięcy osób. Natomiast dzięki uruchomieniu przez GIODO platformy e-learningowej wszyscy zainteresowani mogą samodzielnie podnosić swoje kwalifikacje.

Generalny Inspektor Ochrony Danych Osobowych, mając świadomość istnienia zapotrzebowania na wykwalifikowaną kadrę specjalistów w dziedzinie ochrony danych osobowych, od wielu lat współpracuje ze szkołami wyższymi, jak np. Uniwersytet Kardynała Stefana Wyszyńskiego, Akademia Leona Koźmińskiego w Warszawie, np. WSZECHNICA POLSKA Szkoła Wyższa Towarzystwa Wiedzy Powszechnej w Warszawie, Wyższa Szkoła Finansów i Administracji w Gdańsku i Wyższa Szkoła Biznesu National-Louis University w Nowym Sączu. W ramach zawartych z tymi szkołami porozumień podejmowane są różnego rodzaju inicjatywy, jak organizacja studiów podyplomowych, konferencji, debat i seminariów promujących tematykę prywatności i ochrony danych osobowych. Generalny Inspektor współpracuje również z różnymi organizacjami, jak np. samorządowe ośrodki doskonalenia zawodowego nauczycieli, z którymi prowadzi na zasadzie partnerstwa program pilotażowy „Twoje dane – twoja sprawa”. Program ten skierowany jest do nauczycieli i uczniów szkół gimnazjalnych, a jego celem jest zwiększenie ich wiedzy na temat ochrony danych osobowych i prawa każdego człowieka do prywatności. Program przewiduje przeszkolenie kadry nauczycielskiej szkół objętych pilotażem, by móc następnie włączyć zagadnienia związane z ochroną danych osobowych do programu zajęć szkolnych. W szkołach wytypowanych do projektu, w ramach pilotażu, powstaną konspekty zajęć dla nauczycieli i uczniów, raport ewaluacyjny podjętych działań oraz opracowany zostanie edukacyjny program ogólnopolski.

Na arenie międzynarodowej na podkreślenie zasługuje również wciąż wysoka aktywność Generalnego Inspektora Ochrony Danych Osobowych, który poprzez uczestnictwo w różnych formach współpracy zarówno w I, jak i w III filarze Unii Europejskiej, zaangażowany jest w proces przygotowywania istotnych dla ochrony danych osobowych dokumentów. Przeprowadza również

inspekcje oraz inne czynności wyjaśniające w ramach skoordynowanych działań kontrolnych. Już w 2001 r. polski Generalny Inspektor Ochrony Danych Osobowych zainicjował międzynarodową współpracę między organami ochrony danych osobowych z państw Europy Środkowej i Wschodniej dla wspierania rozwoju ochrony prywatności na tym obszarze. Głównym celem tego forum jest m.in. wytyczanie kierunków przyszłych rozwiązań problemów dotyczących ochrony danych osobowych z uwzględnieniem specyfiki tego obszaru geograficznego oraz wymiana doświadczeń dotyczących interpretacji i stosowania przepisów o ochronie danych osobowych.

Ponadto GIODO uczestniczy w pracach Grupy Roboczej Art. 29 ds. ochrony danych osobowych, w tym m.in. w pracach Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości i Grupie Roboczej ds. Telekomunikacji (tzw. Grupie Berlińskiej). Zaangażowany jest też w prace grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac oraz w prace Komitetu Konsultacyjnego ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Co roku bierze udział w Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności, Wiosennej Konferencji Europejskich Organów Ochrony Danych oraz w Warsztatach Rozpatrywania Spraw.

W ramach wszystkich swoich zadań współpracuje z różnymi partnerami zarówno na poziomie międzynarodowym (Rada Europy, Komisja Europejska, organy ochrony danych osobowych z innych państw, w tym przede wszystkim państw Europy Środkowej i Wschodniej) oraz krajowym (organy administracji publicznej, organizacje pozarządowe oraz szkoły wyższe). To między innymi te działania przyczyniły się do tego, że Polacy - według badań Eurobarometru²²⁶ przeprowadzonych w 2008 r. - stali się najbardziej świadomi swoich praw do ochrony danych osobowych w całej Europie.

Ważnym zadaniem na 2010 r. stojącym przed Generalnym Inspektorem Ochrony Danych Osobowych będzie zorganizowanie w Polsce **XII. Spotkania Grupy Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (Central and Eastern European Data Protection Authorities)**. Jest to już drugie spotkanie członków tej grupy organizowane przez polski organ ds. ochrony danych osobowych. W 2008 r. w Kazimierzu Dolnym odbyło się dziesiąte, jubileuszowe Spotkanie Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej. Powierzenie organizacji tych spotkań polskiemu organowi do spraw ochrony danych osobowych należy traktować jako wyraz uznania dla jego pozycji na tym forum.

Ponadto Biuro Generalnego Inspektora Ochrony Danych Osobowych zostało wyselekcjonowane do realizacji wizyty studyjnej finansowanej z środków Unii Europejskiej w ramach

²²⁶ 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. Raporty krajowe powstają dwa razy w roku. Całościowe wyniki badań są dostępne na stronie internetowej: http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm.

Programu Wizyt Studyjnych, będącego częścią Programu „Uczenie się przez całe życie” (Lifelong Learning Programme). Już sam tytuł projektu „Zagadnienia ochrony danych osobowych i prywatności w edukacji” wskazuje, że jego celem będzie wymiana informacji i doświadczeń na temat sposobu i metod przekazywania dzieciom i młodzieży wiedzy z dziedziny ochrony danych osobowych. W trakcie spotkania podjęta zostanie ocena możliwości wprowadzenia programów edukacyjnych dotyczących ochrony danych osobowych do szkół podstawowych, gimnazjów i liceów oraz przedyskutowane zostaną najbardziej efektywne formy prowadzenia edukacji w tym obszarze. Uczestnikami wizyty będą reprezentanci europejskich organów ochrony danych osobowych oraz instytucji zajmujących się edukacją, w tym przedstawiciele europejskich organów ochrony danych osobowych, przedstawiciele instytucji i środowisk (związki, zrzeszenia) związanych z edukacją i doradztwem, nauczyciele szkół podstawowych, gimnazjów i liceów, decydenci w zakresie programów edukacyjnych z Ministerstwa Edukacji Narodowej, przedstawiciele lokalnych i regionalnych władz związanych z edukacją, a także przedstawiciele środowisk, które monitorują zagrożenia płynące z korzystania Internetu.

Natomiast w odniesieniu do kwestii wdrażania dyrektywy 95/46/WE i dyrektywy 2002/58/WE oraz innych zmian legislacyjnych, wskazać należy, że z chwilą uzyskania przez Polskę członkostwa w Unii Europejskiej weszły w życie przepisy ustawy z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 33, poz. 285). Ustawa ta wprowadziła liczne zmiany w przepisach ustawy o ochronie danych osobowych, a jej uchwalenie miało na celu wdrożenie do polskiego porządku prawnego postanowień dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. o ochronie osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Ponadto w 2009 r. w Sejmie złożony został prezydencki projekt ustawy o zmianie ustawy o ochronie danych osobowych, którego celem jest wyposażenie organu ds. ochrony danych osobowych w bardziej skuteczne instrumenty egzekwowania prawa. Z postanowień ww. dyrektywy, na której wzorowana była polska ustawa o ochronie danych osobowych, wynika bowiem konieczność wprowadzenia skutecznych rozwiązań w kwestii egzekwowania tego prawa. Art. 24 dyrektywy 95/46/WE obliguje państwa członkowskie do podjęcia działań zmierzających do zapewnienia pełnej realizacji praw i obowiązków, które zostały w niej określone, wiążąc jedynie co do celu jaki należy osiągnąć, a pozostawiając swobodę w wyborze drogi do jego osiągnięcia.

W sprawie wdrożenia do polskiego porządku prawnego dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej, w uzasadnieniu rządowego projektu ustawy Prawo telekomunikacyjne (aktualnie: ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne) stwierdza się, że projekt ten w pełni implementuje regulacje Unii Europejskiej w tej materii.

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych
w roku 2009 o charakterze generalnym do centralnych organów państwa i do innych podmiotów
z sektora publicznego**

Lp.	Nazwa podmiotu, do którego skierowano wystąpienie	Data wystąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	Prezydent Miasta Gdańska	27.01.2009 r. DOLiS-035-81/09/2520	Wystąpienie dotyczące konieczności wprowadzenia rozwiązań, które uniemożliwią przetwarzanie w aktach postępowań wszczynanych z urzędu danych osobowych osób informujących o okolicznościach będących podstawą do wszczęcia takich postępowań.
2.	Prezes Izby Karnej Sądu Najwyższego	30.01.2009 r. DOLiS-440-175/07/3043/09	Wystąpienie dotyczące zawężającej interpretacji przepisu art. 51 ust. 1 ustawy o ochronie danych osobowych jaka pojawiła się w praktyce orzeczniczej sądów powszechnych.
3.	Prezes Krajowej Rady Notarialnej	02.02.2009 r. DOLiS-035-145/09/2968	Wystąpienie o wskazanie notariuszom na konieczność respektowania przepisów o ochronie danych osobowych przy umieszczaniu w aktach notarialnych danych jedynie w zakresie określonym w przepisach prawa.
4.	Prezydent Miasta Tychy	10.02.2009 r. DOLiS-440-679/08/4313/09	Wystąpienie o podjęcie działań w celu dostosowania treści formularza „Karta zapisu dziecka do przedszkola na rok szkolny 2008/2009” do wymogów ustawy o ochronie danych osobowych.
5.	Minister Infrastruktury	18.02.2009 r. DOLiS-440-502/08/5373/09	Wystąpienie o rozważenie możliwości wprowadzenia w obowiązujących przepisach prawa zmian, które spowodują usunięcie wątpliwości w ustaleniu obowiązków inwestorów składających do właściwych organów administracji wnioski o ustalenie warunków zabudowy lub lokalizacji inwestycji celu publicznego.
6.	Prezydent m.st. Warszawy	10.03.2009 r. DOLiS-440-228/07/8374/09	Wystąpienie o podjęcie odpowiednich działań mających na celu zapewnienie legalności udostępniania danych osobowych przez podległe Prezydentowi zakłady gospodarstwa nieruchomości na rzecz innych podmiotów, stosownie do wymogów ustawy o ochronie danych osobowych.
7.	Prezes Naczelnego Sądu Administracyjnego	16.03.2009 r. GI-DS-430/161/06/ 8944/09/DOLiS	Wystąpienie, w którym została zwrócona uwaga na dokonaną przez NSA w wyroku z dnia 25 listopada 2008 r. interpretację przesłanki dopuszczalności przetwarzania danych osobowych określonej w art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych.
8.	Prezydent Miasta Szczecina	26.03.2009 r. DOLiS-440-516/08/10812	Wystąpienie o podjęcie stosownych działań celem wyeliminowania w przyszłości wypadków udostępnienia danych osobowych członków założeń stowarzyszeń zwykłych.

9.	Powiatowy Inspektor Nadzoru Budowlanego w Krośnie	09.04.2009 r. DOLiS-035-278/09/12786	Wystąpienie dotyczące procesu doręczania stronom postępowania administracyjnego „Zawiadomień o złożeniu listu poleconego w postępowaniu administracyjnym”, poprzez ich umieszczanie w sposób naruszający przepisy ustawy Kodeks postępowania administracyjnego i ustawy o ochronie danych osobowych.
10.	Komendant Straży Miejskiej w Łodzi	09.04.2009 r. DOLiS-035-543/09/12794	Wystąpienie, w którym została zwrócona uwaga na praktykę fotografowania przez strażników miejskich osób zatrzymanych w izbach wytrzeźwień.
11.	Minister Zdrowia	16.04.2009 r. DOLiS-035-550/09/13516	Wystąpienie dotyczące problemu ustalania przez zakłady opieki zdrowotnej tożsamości (danych osobowych) osób, których tożsamość w momencie przyjęcia do placówki opieki zdrowotnej nie była znana.
12.	Prezes Sądu Rejonowego w Skierniewicach	24.04.2009 r. DOLiS-440-873/08/14723/09	Wystąpienie w sprawie zobowiązania komornika sądowego do nieudostępniania danych osobowych o dłużniku pozyskanych w toku innego postępowania egzekucyjnego jego wierzycielowi.
13.	Minister Sprawiedliwości	04.05.2009 r. DOLiS-035-1503/08/15826/09	Wystąpienie o weryfikację ustaleń dokonanych w toku postępowania przygotowawczego, zakończonego zatwierdzeniem przez prokuraturę postanowieniem o umorzeniu dochodzenia w sprawie podejrzenia umożliwienia dostępu do danych osobowych.
14.	Bank Gospodarstwa Krajowego	07.05.2009 r. DOLiS-440-243/09/16350	Wystąpienie o uwzględnienie wymogów ustanowionych przepisami o ochronie danych osobowych, w procesie przekazywania podmiotowi zewnętrznemu obsługi plac pracowników Banku.
15.	Komendant Główny Policji	15.05.2009 r. DOLiS-035-996/08/14620/09	Wystąpienie dotyczące konieczności wprowadzenia do porządku prawnego przepisów stanowiących podstawę do wymiany przez polską Policję informacji dotyczących DNA z innymi państwami.
16.	Ministerstwo Spraw Wewnętrznych i Administracji	15.05.2009 r. DOLiS-035-996/08/17621/09	Wystąpienie dotyczące konieczności wprowadzenia do porządku prawnego przepisów stanowiących podstawę do wymiany przez polską Policję informacji dotyczących DNA z innymi państwami.
17.	Minister Sprawiedliwości Prokurator Generalny	22.05.2009 r. DIS-K-421/30/09	Podjęcie działań w zakresie objęcia nadzorem postępowania przygotowawczego, prowadzonego przez właściwą jednostkę prokuratury w sprawie dotyczącej niewykonania przez towarzystwo ubezpieczeniowe decyzji nakazującej przywrócenie stanu zgodnego z prawem.
18.	Komisja Budżetu i Finansów Publicznych Senatu RP	22.05.2009 r. DIS-K-421/30/09	Podjęcie stosownych działań w ramach posiadanych kompetencji w sprawie dotyczącej niewykonania przez towarzystwo ubezpieczeniowe decyzji nakazującej przywrócenie stanu zgodnego z prawem.
19.	Komisja Nadzoru Finansowego	22.05.2009 r. DIS-K-421/30/09	Podjęcie stosownych działań w ramach posiadanych kompetencji w sprawie dotyczącej niewykonania przez towarzystwo ubezpieczeniowe decyzji nakazującej przywrócenie stanu zgodnego z prawem.

20.	Rzecznik Ubezpieczonych	22.05.2009 r. DIS-K-421/30/09	Podjęcie stosownych działań w ramach posiadanych kompetencji w sprawie dotyczącej niewykonania przez towarzystwo ubezpieczeniowe decyzji nakazującej przywrócenie stanu zgodnego z prawem.
21.	Komisja Finansów Publicznych Sejmu RP	22.05.2009 r. DIS-K-421/30/09	Podjęcie stosownych działań w ramach posiadanych kompetencji w sprawie dotyczącej niewykonania przez towarzystwo ubezpieczeniowe decyzji nakazującej przywrócenie stanu zgodnego z prawem.
22.	Urząd Ochrony Konkurencji i Konsumentów	22.05.2009 r. DIS-K-421/30/09	Podjęcie stosownych działań w ramach posiadanych kompetencji w sprawie dotyczącej niewykonania przez towarzystwo ubezpieczeniowe decyzji nakazującej przywrócenie stanu zgodnego z prawem.
23.	Marszałek Sejmu RP	22.05.2009 r. DIS-K-421/30/09	Podjęcie stosownych działań w ramach posiadanych kompetencji w sprawie dotyczącej niewykonania przez towarzystwo ubezpieczeniowe decyzji nakazującej przywrócenie stanu zgodnego z prawem.
24.	Prezydent Miasta Białegostoku	29.05.2009 DOLiS-035-665/09/19637	Wystąpienie w sprawie upubliczniania danych osobowych dzieci i ich rodziców w przedszkolach poprzez wywieszanie list zawierających te dane na drzwiach wejściowych do przedszkoli.
25.	Prezydent m.st. Warszawy	01.06.2009 r. DOLiS-035-807/09/20001	Wystąpienie o podjęcie odpowiednich działań mających na celu zaprzestanie upubliczniania danych osobowych dzieci i ich rodziców w przedszkolach poprzez wywieszanie list zawierających te dane na drzwiach wejściowych do przedszkoli.
26.	Minister Nauki i Szkolnictwa Wyższego	01.06.2009 r. DOLiS-035-634/09/19906	Wystąpienie o wskazanie rektorom uczelni wyższych na konieczność przestrzegania zasad przewidzianych w przepisach prawa w związku z przetwarzaniem danych osobowych absolwentów uczelni w celach marketingowych.
27.	Wójt Gminy Żary	22.06.2009 r. DOLiS-035-852/09/22467	Wystąpienie o niepodawanie do publicznej wiadomości niejawnych części oświadczeń majątkowych.
28.	Minister Sprawiedliwości	29.06.2009 r. DOLiS-440-37/09/23567	Wystąpienie dotyczące udostępniania danych adresowych funkcjonariuszy policji ze zbioru PESEL w związku z wzywaniem przez sądy osób pozywających ww. do wskazywania adresów ich zamieszkania celem nadania biegu sprawie cywilnej.
29.	Archiwum Państwowe w Warszawie	06.07.2009 r. DIS-K-421/71/09	Podjęcie działań w związku z nieprawidłowym postępowaniem z dokumentacją archiwalną (na którą składają się akta osobowe pracowników i dokumenty finansowo-księgowe), wytworzoną przez Kombinat Budownictwa Komunalnego Województwa Sieradzkiego Zakładu Produkcji Materiałów Budowlanych w Łask Kolumna, Wojewódzkie Przedsiębiorstwo Prefabrykatów w Łask Kolumna, Przedsiębiorstwo Produkcyjno Handlowe „Prefabrykaty” Sp. z o. o. w Łask Kolumna a obecnie przechowywaną w warunkach grożących jej zniszczeniem oraz dostępem osób nieuprawnionych.

30.	Prezydent Miasta Gdańska	10.07.2009 r. DOLiS-035-1156/09/25062	Wystąpienie dotyczące konieczności wprowadzenia rozwiązań, które uniemożliwią przetwarzanie w aktach postępowań wszczynanych z urzędu danych osobowych osób informujących o okolicznościach będących podstawą do wszczęcia takich postępowań.
31.	Prezydent Miasta Krakowa	23.07.2009 r. DOLiS-035-1018/09/26754	Wystąpienie dotyczące dostarczania korespondencji osobom, których sprawy załatwiane są w urzędzie, bez kopert, tj. niewłaściwego zabezpieczenia danych.
32.	Przewodniczący Komisji Nadzoru Finansowego	30.07.2009 r. DOLiS-440-868/08/27821	Wystąpienie o zwrócenie instytucjom, nad którymi Przewodniczący KNF sprawuje nadzór, w tym szczególności bankom, uwagi na konieczność respektowania przepisów ustawy Prawo bankowe w odniesieniu do tajemnicy bankowej, w sytuacji gdy podmioty te ulegają łączeniu, podziałowi lub przekształceniu w rozumieniu przepisów ustawy Kodeks spółek handlowych i jednocześnie przestrzegania zasad określonych w ustawie o ochronie danych osobowych.
33.	Prezydent Miasta Kołobrzegu	05.08.2009 r. DOLiS-035-1376/09/28595	Wystąpienie o zmianę praktyki urzędu polegającej na udostępnianiu na jego stronach internetowych dokumentacji projektowej zawierającej dane osobowe.
34.	Prezydent Miasta Gdyni	07.08.2009 r. DOLiS-440-427/09/28915	Wystąpienie o podjęcie niezbędnych działań w celu zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi przepisami w związku z uzyskaniem informacji o udostępnianiu przez Prezydenta Miasta Gdyni danych osobowych w zakresie daty zameldowania na pobyt stały bez dochowania należytej staranności, czy osoba wnioskująca o te dane jest uprawniona do ich otrzymania.
35.	Minister Sprawiedliwości	10.08.2009 r. DOLiS-440-756/08/29280/09	Wystąpienie o zwrócenie szczególnej uwagi na konieczność respektowania przepisów ustawy o ochronie danych osobowych przy udostępnianiu danych osobowych z Krajowego Rejestru Karnego.
36.	Prezes Zakładu Ubezpieczeń Społecznych	31.08.2009 r. DOLiS-035-1247/09/31521	Wystąpienie w sprawie zabezpieczenia danych osobowych.
37.	Dyrektor Generalny Ministerstwo Kultury i Dziedzictwa Narodowego	16.09.2009 r. DOLiS-440-396/09/33711	Wystąpienie o podjęcie odpowiednich działań mających na celu zagwarantowanie zgodności przetwarzania danych osobowych pracowników i byłych pracowników Ministerstwa z przepisami ustawy o ochronie danych osobowych.
38.	Minister Zdrowia	15.10.2009 r. DOLiS-440-374/09/ 37706,37818	Wystąpienie o podjęcie odpowiednich działań mających na celu zagwarantowanie zgodności przetwarzania danych osobowych świadczeniobiorców z przepisami ustawy o ochronie danych osobowych, przekazanych przez świadczeniodawców NFZ.

39.	Archiwum Państwowe w Warszawie	16.10.2009 r. DIS-K-421/107/09	Podjęcie działań w związku z nieprawidłowym postępowaniem z dokumentacją archiwalną (na którą składają się akta osobowe pracowników i dokumenty finansowo-księgowe), wytworzoną przez Przedsiębiorstwo Prefabrykacji Przemysłu Węglowego – PREFBET S.A. w Katowicach, a obecnie przechowywaną w warunkach grożących jej zniszczeniem oraz dostępem osób nieuprawnionych.
40.	Prezes Narodowego Funduszu Zdrowia	29.10.2009 r. DOLiS-035-1534/09/39900	Wystąpienie w sprawie przekazywania danych osobowych pacjentów wymagających opieki lekarskiej w niedziele i święta zakładom opieki zdrowotnej, które mają podpisane stosowne umowy z NFZ.
41.	Minister Finansów	17.11.2009 r. DOLiS-440-582/09/42413	Wystąpienie dotyczące wątpliwości odnośnie legalności praktyki polegającej na udostępnianiu z Krajowej Ewidencji Podatników na rzecz organów podatkowych danych osobowych.
42.	Prokurator Generalny RP	26.11.2009 r. DOLiS-440-184/08/43888/09	Wystąpienie o podjęcie działań mających na celu wyeliminowanie stosowanej przez prokuratury praktyki polegającej na wpisywaniu na zwrotnym potwierdzeniu odbioru pism informacji wskazujących na charakter, w jakim uczestniczy w prowadzonym postępowaniu adresat.
43.	Prezes Narodowego Funduszu Zdrowia	10.12.2009 r. DOLiS-035-2228/09/46160	Wystąpienie w sprawie zaprzestania wydawania przez ZUS legitymacji ubezpieczeniowych.
44.	Minister Rolnictwa i Rozwoju Wsi	15.12.2009 r. DOLiS-035-2338/09/46881	Wystąpienie dotyczące zmiany brzmienia przepisów ustawy o Inspekcji Weterynaryjnej.
45.	Główny Inspektor Pracy	15.12.2009 r. DIS-K-421/156/09	Opinia w zakresie zgodności zapisów zawartych w § 17 „Zakładowego Układu Zbiorowego Pracy” z dnia 25 lutego 1998 r. obowiązującego w Totalizatorze Sportowym Sp. z o. o. w Warszawie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21 poz. 94 z późn. zm.), w szczególności z art. 9 i 22 ¹ ww. ustawy.
46.	Marszałek Województwa Mazowieckiego	29.12.2009 r. DIS-K-421/132/09	Opinia w sprawie zgodności działalności agencji zatrudnienia „Centrum Pośrednictwa ELIZABETH Matki Zastępcze Surogatki” w Piasecznie z przepisami 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.).

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych
w roku 2009 do podmiotów prywatnych**

Lp.	Nazwa podmiotu, do którego skierowano wystąpienie	Data wystąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	Wspólnota Mieszkaniowa „Osowska 45”	13.01.2009 r. DOLiS-440-616/08/930/09	Wystąpienie o respektowanie przepisów ustawy o ochronie danych osobowych przy podejmowaniu działań będących przedmiotem działalności Wspólnoty Mieszkaniowej w związku z zamieszczeniem przez nią na tablicy ogłoszeń w miejscu publicznie dostępnym danych osobowych.
2.	Agora S.A.	19.01.2009 r. DOLiS-035-48/09/1463	Wystąpienie o respektowanie przepisów ustawy o ochronie danych osobowych w związku z „niekontrolowanym” rozsyłaniem e-maili przeznaczonych dla jednego odbiorcy także do innych osób/podmiotów (niezabezpieczenie danych i obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą).
3.	Spółdzielnia Mieszkaniowa Zachęta	21.01.2009 r. DOLiS-035-1640/08/1815	Wystąpienie w sprawie stosowania video-nadzoru (o zaniechanie tej praktyki).
4.	Spółdzielnia Mieszkaniowa Lokatorsko-Własnościowa „Dążność”	22.01.2009 r. DOLiS-440-716/08/2014/09	Wystąpienie o zaniechanie praktyki polegającej na wykorzystywaniu danych osobowych członków Spółdzielni niezgodnie z celem, dla którego zostały pozyskane oraz udostępnianiu tych danych osobom nieupoważnionym.
5.	ITI Neovision Sp. z o.o.	30.01.2009 r. DOLiS-440-763/08/2985/09	Wystąpienie o uwzględnienie w działalności Spółki zasad wynikających z przepisów o ochronie danych osobowych, w szczególności w odniesieniu do przetwarzania danych w celach marketingowych.
6.	Okręgowy Zarząd Polskiego Związku Działkowców w Koszalinie	10.02.2009 r. DOLiS-440-812/08/4406/09	Wystąpienie o nieudostępnianie danych osobowych w zakresie szerszym niż niezbędny dla realizacji zamierzonego celu.
7.	Sferis Sp. z o.o.	17.02.2009 r. DOLiS-440-517/08/5280/09	Wystąpienie o przestrzeganie przez Spółkę przepisów ustawy o ochronie danych osobowych przy rozpatrywaniu reklamacji składanych przez klientów.
8.	Orbis S.A.	25.02.2009 r. DOLiS-440-941/08/6300/09	Wystąpienie o podjęcie stosownych działań mających na celu wyeliminowanie nieprawidłowości polegających na udostępnieniu na stronie internetowej www.orbis.pl danych osobowych.
9.	Polska Telefonía Cyfrowa Sp. z o.o.	25.02.2009 r. DOLiS-440-766/08/6460/09	Wystąpienie o dostosowanie do przepisów ustawy o ochronie danych osobowych formularza karty rejestracyjnej „Karty Tak Tak”.
10.	Stowarzyszenie Marketingu Bezpośredniego	16.03.2009 r. DOLiS-440-303/08/8960/09	Wystąpienie o podjęcie działań uczulających Skarbnicę Narodową Sp. z o.o. - członka Stowarzyszenia Marketingu Bezpośredniego - na respektowanie przepisów ustawy o ochronie danych osobowych.

11.	Krajowa Rada Spółdzielcza	24.03.2009 r. DOLiS-440-877/08/10453/09	Wystąpienie o wprowadzenie rozwiązań, które umożliwią ujawnienie w protokołach lustracji spółdzielni mieszkaniowych danych osób informujących o okolicznościach podlegających badaniu w trakcie przeprowadzanej lustracji.
12.	TUI Poland Sp. z o.o.	07.04.2009 r. DOLiS-035-181/09/12215	Wystąpienie o respektowanie przepisów ustawy o ochronie danych osobowych, w szczególności w odniesieniu do przetwarzania danych w celach marketingowych, obowiązku informacyjnego, także w związku z przysyłaniem informacji handlowej drogą elektroniczną.
13.	Bank Pocztowy S.A.	09.04.2009 r. DOLiS-035-286/09/12791	Wystąpienie w sprawie nieprawidłowej klauzuli zgody zawartej we wniosku o założenie lokaty/otwarcie rachunku terminowych lokat oszczędnościowych w aspekcie przekazywania danych osobowych innym podmiotom oraz w sprawie obowiązku informacyjnego.
14.	Nowa Itaka Sp. z o.o.	09.04.2009 r. DOLiS-035-180/09/12809	Wystąpienie w sprawie nieprawidłowej klauzuli zgody - nieprecyzyjne sformułowanej i uzależniającej skorzystanie z usług administratora od zgody na marketing. Wystąpienie dotyczy także obowiązku informacyjnego.
15.	Sony Poland Sp. z o.o.	09.04.2009 r. DOLiS-035-351/09/12898	Wystąpienie o podjęcie stosownych działań mających na celu prawidłowe dopełnienie obowiązku informacyjnego.
16.	Wakacje.pl S.A.	16.04.2009 r. DOLiS-035-179/09/13596	Wystąpienie o dostosowanie do przepisów ustawy klauzuli zgody zamieszczonej na stronach internetowych www.wakacje.pl (jej doprecyzowanie) i dopełnienie obowiązku informacyjnego.
17.	Bank Zachodni WBK S.A.	15.05.2009 r. DOLiS-440-861/08/17642/09	Wystąpienie dotyczące respektowania zasad wynikających z przepisów ustawy o ochronie danych osobowych celem wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych klienta archiwalnego.
18.	Kredyt Bank S.A.	26.05.2009 r. DOLiS-440-143/09/19041	Wystąpienie o uwzględnienie w działalności Banku przepisów ustawy o ochronie danych osobowych, zwłaszcza jej art. 36 ust. 1.
19.	Związek Banków Polskich	26.05.2009 r. DOLiS-440-143/09/19043	Wystąpienie o podjęcie działań zwracających bankom uwagę na konieczność respektowania przepisów ustawy o ochronie danych osobowych, zwłaszcza jej art. 36 ust. 1.
20.	Polkomtel S.A.	9.06.2009 r. DOLiS-440-156/09/21050	Wystąpienie o podjęcie działań mających na celu wyeliminowanie w nieprawidłowości polegającej na przetwarzaniu danych w celach marketingowych pomimo wniesienia sprzeciwu w tym zakresie.
21.	Euro Bank S.A.	18.06.2009 r. DOLiS-035-305/09/22146	Wystąpienie o odstąpienie od praktyki polegającej na telefonicznym potwierdzaniu prawdziwości podanych przez kredytobiorców danych osobowych.
22.	PHU Trans Bis Wieteki Robert	23.06.2009 r. DOLiS-035-347/09/22697	Wystąpienie o odstąpienie od praktyki polegającej na zatrzymywaniu dowodu tożsamości w zastaw za wypożyczenie wózka-koszyka służącego do przewozu dziecka w centrum handlowym.

23.	Eller Service S.C. Rafał Peisert, Iwona Kwiatkowska	23.06.2009 r. DOLiS-035-903/09/22810	Wystąpienie dotyczące respektowania zasad wynikających z przepisów ustawy o ochronie danych osobowych celem wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych dotyczących stosowania regulaminu zamieszczonego na stronie www.pobieraczek.pl (obowiązek informacyjny, nieprecyzyjna klauzula zgody).
24.	PKO BP S.A.	24.06.2009 r. DOLiS-440-208/09/22865	Wystąpienie o dostosowanie do przepisów ustawy o ochronie danych osobowych treści formularza „Krótkiej ankiety produktowej”.
25.	o2.pl Sp. z o.o.	24.07.2009 r. DOLiS-035-974/09/26903	Wystąpienie w związku z pozyskiwaniem za pomocą strony internetowej www.najPraca.pl danych osobowych w zakresie szerszym, niż dopuszczone jest to przepisami prawa a także dotyczące obowiązków administratora danych.
26.	PZU S.A.	28.07.2009 r. DOLiS-440-470/09/27355	Wystąpienie o niezwłoczne zaprzestanie praktyki polegającej na umieszczeniu na kopertach wysyłanej korespondencji informacji o statusie prawnym adresatów objętych tą korespondencją pism.
27.	Salon Gier „ALA”	30.07.2009 r. DOLiS-035-348/09/27874	Wystąpienie o odstąpienie od praktyki polegającej na zatrzymywaniu dowodu tożsamości w zastaw za wypożyczenie wózka-koszyka służącego do przewozu dziecka w centrum handlowym.
28.	Żywiec Sprzedaż i Dystrybucja Sp. z o.o.	31.07.2009 r. DOLiS-035-1095/09/28022	Wystąpienie dotyczące respektowania zasad wynikających z przepisów ustawy o ochronie danych osobowych celem wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych pozyskiwanych za pomocą strony internetowej www.heineken.pl w trakcie uczestnictwa w konkursie (obowiązek informacyjny, nieprecyzyjna klauzula zgody).
29.	4call.pl Sp. z o.o.	31.07.2009 r. DOLiS-035-1047/09/27943	Wystąpienie o weryfikację zakresu zbieranych danych osobowych, w związku z dochodzeniem roszczeń z tytułu pobranych opłat za wydanie karty pojazdu (kserowanie dowodów osobistych).
30.	Abi-security Sp. z o.o.	03.08.2009 r. DOLiS-035-1353/09/28230	Wystąpienie o respektowanie przepisów o ochronie danych osobowych (ogólne).
31.	NetArt Piotr Nowak	04.08.2009 r. DOLiS-035-640/09/28389	Wystąpienie o respektowanie przepisów o ochronie danych osobowych (ogólne).
32.	GG Network S.A.	10.08.2009 r. DOLiS-035-1397/09/29190	Wystąpienie dotyczące respektowania zasad wynikających z przepisów ustawy o ochronie danych osobowych celem wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych pozyskiwanych za pomocą strony internetowej www.zrodzina.pl (obowiązek informacyjny, nieprecyzyjna klauzula zgody).
33.	Polskie Górnictwo Naftowe i Gazownictwo S.A.	12.08.2009 r. DOLiS-440-269/09/29594	Wystąpienie o podjęcie działań w celu dostosowania treści stosowanych przez Spółkę wzorców formularzy umowy służących do aktualizacji umów sprzedaży paliw do wymogów ustawy o ochronie danych osobowych.

34.	Polskie Linie Lotnicze LOT S.A.	27.08.2009 r. DOLiS-035-1699/08/31166	Wystąpienie o realizowanie obowiązku informacyjnego w chwili pozyskiwania danych za pomocą strony internetowej https://www.lot.com .
35.	Bank Polska Kasa Opieki S.A.	15.10.2009 r. DOLiS-440-558/09/37717	Wystąpienie o podjęcie stosownych działań w związku z uzyskaniem informacji o udostępnieniu osobie nieupoważnionej przez Bank danych osobowych.
36.	Netia S.A.	22.10.2009 r. DOLiS-440-528/09/38755/09	Wystąpienie o dopełnianie przez Spółkę obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych.
37.	DHL Express (Poland) Sp. z o.o.	22.10.2009 r. DOLiS-035-1925/09/35754	Wystąpienie o dostosowanie regulaminu dotyczącego pozyskiwania danych osobowych przy doręczaniu przesyłek do stosowanej przez tą firmę praktyki pozyskiwania danych ich odbiorców.
38.	Żabka Polska S.A.	18.11.2009 r. DOLiS-035-572/09/42634	Wystąpienie o odstąpienie od praktyki pozyskiwania (spisywania) danych osobowych klientów w sytuacji płacenia przez nich elektroniczną kartą płatniczą.
39.	Alior Bank S.A.	26.11.2009 r. DOLiS-440-368/09/43963	Wystąpienie o podjęcie odpowiednich działań mających na celu wyczerpanie pracowników na niedopuszczenie do sytuacji udostępniania danych osobowych klientów osobom nieupoważnionym.
40.	Pliva Kraków Zakłady Farmaceutyczne S.A.	14.12.2009 r. DOLiS-035-2337/09/46621	Wystąpienie dotyczące dostosowania procesu przetwarzania danych osobowych pracowników do przepisów Kodeksu Pracy (w aspekcie zakresu danych) oraz ustawy o ochronie danych osobowych (w aspekcie zgody na pozyskiwanie danych).
41.	Zielonogórski Klub Żużlowy Sportowa Spółka Akcyjna	19.12.2009 r. DOLiS-035-339/09/2231	Wystąpienie dotyczące pozyskiwania danych osobowych w związku z wydawaniem Karty Kibica, oraz nieprawidłowości w regulaminie tego dotyczącym.
42.	Legia Warszawa S.S.A.	21.12.2009 r. DOLiS-440-544/08/47724/09	Wystąpienie o prawidłowe wykonanie obowiązku informacyjnego z art. 33 ust. 1 ustawy o ochronie danych osobowych.

Wykaz kontroli przeprowadzonych w 2009 r.

L.p.	Data / Sygnatura kontroli	Nazwa i miejsce podmiotu kontrolowanego	Inicjatywa kontroli	Rozstrzygnięcie oraz/lub data i sygnatura decyzji
1.	12-14.01.2009 r. DIS-K-421/1/09	Polska Telefonia Komórkowa Centertel Sp. z o.o. Warszawa, ul. Skierniewicka 10A	Departament Orzecznictwa Legislacji i Skarg	30.06.2009 r. Decyzja DIS/DEC-585/23652/09
2.	12-14.01.2009 r. DIS-K-421/2/09	Spółdzielnia Mieszkaniowa Nowe Miasto, Warszawa, ul. Bonifraterska 14	z urzędu	16.04.2009 r. Decyzja DIS/DEC-307/13545/09
3.	12-15.01.2009 r. DIS-K-421/3/09	RWE Polska S.A. Warszawa, Wybrzeże Kościuszkowskie 41	Departament Orzecznictwa Legislacji i Skarg	10.04.2009 r. Decyzja DIS/DEC-286/13004/09
4.	13-16.01.2009 r. DIS-K-421/4/09	Małgorzata Komor i Wspólnicy Klubu Delfin s.c. Gdańsk, ul. Małachowskiego 1	z urzędu	nie stwierdzono uchybień
5.	19-23.01.2009 r. DIS-K-421/5/09	Rainbow Tours S.A. Łódź, ul. Piotrkowska 270	z urzędu	13.05.2009 r. Decyzja DIS/DEC-390/17359/09
6.	19-23.01.2009 r. DIS-K-421/6/09	Nasza Klasa Sp. z o.o. Wrocław, ul. Dembowskiego 57/5	Departament Orzecznictwa Legislacji i Skarg	09.04.2010 r. Decyzja DIS/DEC-394/15034/10
7.	19-22.01.2009 r. DIS-K-421/7/09	Varena Group Sp. z o.o. Warszawa, Pl. Konstytucji 2/49	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
8.	23.01.2009 r. DIS-K-421/15/09	Sylwester Kiedrowicz prowadzący działalność gospodarczą pod nazwą „E-Grupa Sylwester Kiedrowicz”, Warszawa, ul. Milanowska 9	w związku z kontrolą DIS-K-421/7/09	przywrócono stan zgodny z prawem
9.	26-28.01.2009 r. DIS-K-421/8/09	Marek Wróbel prowadzący działalność gospodarczą pod nazwą „NETim Usługi Informatyczne Marek Wróbel”, Wrocław, ul. Marka Hłaski 6/1	Naczelna Izba Lekarska	nie stwierdzono uchybień
10.	26-30.01.2009 r. DIS-K-421/9/09	Elektroniczne Systemy Sprzedaży Sp. z o.o., Wrocław, ul. Supińskiego 1	w związku z kontrolą DIS-K-421/159/08	15.04.2009 r. Decyzja DIS/DEC-300/13355/09
11.	26-28.01.2009 r. DIS-K-421/10/09	Freshmind Sp. z o.o. Warszawa, ul. Okrzei 23/42	Departament Orzecznictwa Legislacji i Skarg	27.05.2009 r. Decyzja DIS/DEC-443/19249/09
12.	26-29.01.2009 r. DIS-K-421/11/09	Świstak.pl Sp. z o.o. Warszawa, Al. Solidarności 61	z urzędu	nie stwierdzono uchybień
13.	26-27.01.2009 r. DIS-K-421/12/09	Telekomunikacja Polska S.A. Warszawa, ul. Twarda 18	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
14.	26-30.01.2009 r. DIS-K-421/13/09	Niepubliczny Zakład Opieki Zdrowotnej „Lumed” Sp. z o.o. Lubaczów, ul. Kościuszki 16	z urzędu	30.06.2009 r. - zawiadomienie o przestępstwie, 29.07.2009 r. - Decyzja DIS/DEC-746/27492/09
15.	26-27.01.2009 r. DIS-K-421/14/09	Przedsiębiorstwo Produkcyjne Kabin Łazienkowych Sp. z o.o. Nowe Lipiny, ul. Niska 1	z urzędu	11.05.2009 r. Decyzja DIS/DEC-366/16756/09

16.	03-05.02.2009 r. DIS-K-421/16/09	Zakład Gospodarowania Nieruchomościami w Dzielnicy m.st. Warszawy, Warszawa, ul. Szwoleżerów 5	Departament Orzecznictwa Legislacji i Skarg	07.08.2009 r. decyzja DIS/DEC-796/28953,28993/09
17.	04-06.02.2009 r. DIS-K-421/17/09	Agito S.A. Warszawa, ul. Jagiellońska 82	z urzędu	10.04.2009 r. Decyzja DIS/DEC-287/13013/09
18.	04-06.02.2009 r. DIS-K-421/18/09	Philipiak Polska Sp. z o.o. Warszawa, ul. Strażacka 63/65	Departament Orzecznictwa Legislacji i Skarg	04.11.2009 r. decyzja DIS/DEC-1109/40731/09
19.	04-06.02.2009 r. DIS-K-421/19/09	Ministerstwo Sprawiedliwości, Warszawa, Al. Ujazdowskie 11	z urzędu	22.06.2009 r. Decyzja DIS/DEC-545/22484/09
20.	09-11.02.2009 r. DIS-K-421/20/09	INCO-VERITAS S.A. Warszawa, ul. Wspólna 25	w związku z kontrolą DIS-K- 421/196/08	09.06.2009 r. Decyzja DIS/DEC-514/21093/09
21.	09-13.02.2009 r. DIS-K-421/21/09	Szef Urzędu ds. Cudzoziemców, Warszawa, ul. Koszykowa 16	z urzędu	w toku
22.	11-13.02.2009 r. DIS-K-421/22/09	Strabag Sp. z o.o. Warszawa, ul. Brechta 7	w związku z kontrolą DIS-K- 421/196/08	nie stwierdzono uchybień
23.	11-13.02.2009 r. DIS-K-421/23/09	Tomasz Branecki Agencja Jartom, Warszawa, ul. Kopernika 30	z urzędu	nie stwierdzono uchybień
24.	11-13.02.2009 r. DIS-K-421/24/09	Contenta.com.pl Sp. z o.o. Warszawa, ul. Puławska 90 lok.4	z urzędu	30.04.2009 r. Decyzja DIS/DEC-352/15651/09
25.	16-18.02.2009 r. DIS-K-421/25/09	International Data Group Poland S.A. Warszawa, ul. Jordanowska 12	z urzędu	28.12.2009 r. decyzja DIS/DEC-1327/48391/09
26.	17-26.02.2009 r. DIS-K-421/26/09	Unilever Polska Sp. z o.o. Warszawa, ul. Postępu 18A	Departament Edukacji Społecznej i Współpracy Międzynarodowej	11.09.2009 r. Decyzja DIS/DEC-911/33162/09
27.	17-26.02.2009 r. DIS-K-421/27/09	Unilever Polska S.A. Warszawa, ul. Postępu 18A	Departament Edukacji Społecznej i Współpracy Międzynarodowej	11.09.2009 r. Decyzja DIS/DEC-907/33129/09
28.	17-26.02.2009 r. DIS-K-421/28/09	Unilever Poland Services Sp. z o.o. Warszawa, ul. Postępu 18A	Departament Edukacji Społecznej i Współpracy Międzynarodowej	11.09.2009 r. Decyzja DIS/DEC-908/33134/09
29.	18-20.02.2009 r. DIS-K-421/29/09	Grażyna Kozłowska prowadząca działalność gospodarczą pod nazwą „ART-DOM”, Warszawa, ul. Targowa 15/60A	z urzędu	nie stwierdzono uchybień
30.	18-19.02.2009 r. DIS-K-421/30/09	Link4 Towarzystwo Ubezpieczeń S.A. Warszawa, ul. Postępu 15	z urzędu	15.04.2009 r. zawiadomienie o przestępstwie
31.	25-27.02.2009 r. DIS-K-421/31/09	Mirosław Świstak prowadzący działalność gospodarczą pod nazwą „Assertor”, Warszawa, ul. Inżynierska 11	z urzędu	nie stwierdzono uchybień
32.	25-27.02.2009 DIS-K-421/32/09	Brandt S.A. Warszawa, ul. Zakopiańska 5 lok. 2	z urzędu	nie stwierdzono uchybień
33.	25-27.02.2009 r. DIS-K-421/33/09	GoldenLine Sp. z o.o. Warszawa, ul. Skrzetuskiego 17A	z urzędu	30.06.2009 r. Decyzja DIS/DEC-583/23647/09
34.	25-27.02.2009 r. DIS-K-421/34/09	Presco Media Sp. z o.o. Warszawa, ul. Garażowa 5	z urzędu	nie stwierdzono uchybień
35.	03-06.03.2009 r. DIS-K-421/35/09	Adesko Sp. z o.o. Warszawa, ul. Ateńska 61	Departament Orzecznictwa Legislacji i Skarg	05.06.2009 r. Decyzja DIS/DEC-497/20695/09

36.	03-06.03.2009 r. DIS-K-421/36/09	Ministerstwo Spraw Zagranicznych, Warszawa, Al. Szucha 23	w związku z kontrolami DIS-K-421/149/08 i DIS-K-421/193/08	16.04.2009 r. pismo do Ministra Spraw Zagranicznych
37.	03-06.03.2009 r. DIS-K-421/37/09	Lebiedź i Lebiedź, Joanna Lebiedź, Tomasz Lebiedź sp.j. Warszawa, ul. Estrady 65	z urzędu	nie stwierdzono uchybień
38.	09-11.03.2009 r. DIS-K-421/38/09	Szybko.pl Sp. z o.o. Warszawa, ul. Rakowiecka 39A/16	z urzędu	22.05.2009 r. Decyzja DIS/DEC-411/18722/09
39.	09-13.03.2009 DIS-K-421/39/09	Home Broker S.A. Warszawa, ul. Domaniewska 39	z urzędu	27.05.2009 r. Decyzja DIS/DEC-444/19255/09
40.	10-13.03.2009 r. DIS-K-421/40/09	Dorota Jeska prowadząca działalność gospodarczą pod nazwą „Nieruchomości Dorota Jeska”, Warszawa, ul. Pasaż Ursynowski 7	z urzędu	13.05.2009 r. Decyzja DIS/DEC-389/17355/09
41.	10-13.03.2009 r. DIS-K-421/41/09	Mainframe Sp. z o.o. Raszyn, ul. Zielona 18	w związku z kontrolą DIS-K-421/19/09	22.06.2009 r. Decyzja DIS/DEC-546/22486/09
42.	12-13.03.2009 r. DIS-K-421/42/09	Krajmed Laryngologia i Chirurgia Plastyczna Nosa Niepubliczny Zakład Opieki Zdrowotnej, Warszawa, ul. Wałbrzyska 11	Okręgowy Rzecznik Odpowiedzialności Zawodowej Izby Lekarskiej	24.06.2009 r. - zawiadomienie o przestępstwie, 31.08.2009 r. - Decyzja DIS/DEC-877/31613/09
43.	11-12.03.2009 r. DIS-K-421/43/09	Centrum Medyczne Damiana Sp. z o.o. Warszawa, ul. Wałbrzyska 46	Okręgowy Rzecznik Odpowiedzialności Zawodowej Izby Lekarskiej	24.06.2009 r. - zawiadomienie o przestępstwie DIS/ZAW-13/22899/09, 31.08.2009 r. - Decyzja DIS/DEC-877/31613/09
44.	16-19.03.2009 r. DIS-K-421/44/09	Rzecznik Praw Obywatelskich, Warszawa, Al. Solidarności 77	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
45.	17-20.03.2009 r. DIS-K-421/45/09	Trader.com (Polska) Sp. z o.o. Warszawa, ul. Towarowa 22	z urzędu	22.05.2009 r. Decyzja DIS/DEC-410/18720/09
46.	17-20.03.2009 r. DIS-K-421/46/09	Wojciech Kamiński prowadzący działalność gospodarczą pod nazwą „Wojciech Kamiński APP Wakat”, Warszawa, ul. Walecznych 64	Departament Orzecznictwa Legislacji i Skarg	18.08.2009 r. Decyzja DIS/DEC-827/30231/09
47.	16-20.03.2009 r. DIS-K-421/47/09	Burmistrz Miasta Żywiec – Urząd Miejski w Żywcu, Żywiec, ul. Rynek 2	Prokuratura Rejonowa w Bielsku - Białej	ustalenia przekazano do Prokuratury Rejonowej w Bielsku - Białej
48.	18-20.03.2009 r. DIS-K-421/48/09	MetLife Towarzystwo Ubezpieczeń na Życie S.A. Warszawa, ul. Puławska 17	w związku z kontrolą DIS-K-421/1/09	nie stwierdzono uchybień
49.	24-27.03.2009 r. DIS-K-421/49/09	Urząd Miejski w Biskupcu, Biskupiec, Al. Niepodległości 2	Agencja Bezpieczeństwa Wewnętrznego	07.08.2009 r. Decyzja DIS/DEC-795/28947/09
50.	23-26.03.2009 r. DIS-K-421/50/09	Tomasz Klimczak prowadzący działalność gospodarczą pod nazwą „Pless Intermedia”, Pszczyna, ul. Batorego 27	Departament Orzecznictwa Legislacji i Skarg	16.07.2009 r. Decyzja DIS/DEC-635/25711/09
51.	23-26.03.2009 r. DIS-K-421/51/09	Polanowscy Nieruchomości Sp. z o.o. Warszawa, ul. Marszałkowska 83 lok. 55	z urzędu	30.06. r.2009 r. Decyzja DIS/DEC-586/23654/09
52.	24-27.03.2009 r. DIS-K-421/52/09	HomeNet Technologies Sp. z o.o. Białystok, ul. Świętojańska 13/2	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
53.	24-26.03.2009 r. DIS-K-421/53/09	Grupa Stereo S.A. Warszawa, ul. Rydygiera 8	z urzędu	30.10.2009 r. decyzja DIS/DEC-1086/39944/09

54.	25-27.03.2009 r. DIS-K-421/54/09	Tomasz Zienkiewicz prowadzący działalność gospodarczą pod nazwą „Tomasz Zienkiewicz”, Warszawa, ul. Dzieci Warszawy 27B/29	Departament Orzecznictwa Legislacji i Skarg	22.10.2009 r. decyzja DIS/DEC-1055/38764/09
55.	30.03.-03.04.2009 DIS-K-421/55/09	Poznań Indoor Karting Sp. z o.o. Poznań, ul. Bolesława Krzywoustego 72	Departament Orzecznictwa Legislacji i Skarg	24.08.2009 r. Decyzja DIS/DEC-829/30716/09
56.	01-03.04.2009 r. DIS-K-421/56/09	HSBC Bank Polska S.A. Warszawa, Pl. Piłsudskiego 2	z urzędu	24.10.2009 r. Decyzja DIS/DEC-990/36524/09
57.	01-03.04.2009 r. DIS-K-421/57/09	Maxon Nieruchomości Sp. z o.o. Warszawa, ul. Okopowa 58/72	z urzędu	nie stwierdzono uchybień
58.	01-03.04.2009 r. DIS-K-421/58/09	Atrium 21 – Agencja Nieruchomości Sp. z o.o. Warszawa, ul. Batorego 20	z urzędu	nie stwierdzono uchybień
59.	06-09.04.2009 r. DIS-K-421/59/09	Stowarzyszenie Rodziców i Opiekunów Dzieci Niepełnosprawnych „Wspólna Troska”, Skierniewice, ul. Jagiellońska 28	Departament Rejestracji Zbiorów Danych Osobowych	07.08.2009 r. Decyzja DIS/DEC-794/28936/09
60.	07-08.04.2009 r. DIS-K-421/60/09	Laboratorium Dialab Jacek Borowicz, Podkowa Leśna - Owczarnia, ul. Letniskowa 1	Departament Orzecznictwa Legislacji i Skarg	24.06.2009 r. - zawiadomienie o przestępstwie, 31.08.2009 r. - Decyzja DIS/DEC-876/31611/09
61.	06.04.2009 r. DIS-K-421/61/09	Piotr Mówiński, Działdowo, ul. Karłowicza 6/52	z urzędu	ustalenia wykorzystane w postępowaniu DIS-K-421/78/09
62.	07-09.04.2009 r. DIS-K-421/62/09	PMICOMBERA Sp. z o.o. Warszawa, ul. Filomatów 27	Departament Rejestracji Zbiorów Danych Osobowych	11.09.2009 r. Decyzja DIS/DEC-909/33136/09
63.	08-09.04.2009 r. DIS-K-421/63/09	CPU-Service A. i Z. Maryniak sp.j. Warszawa, ul. Modlińska 199	w związku z kontrolą DIS-K- 421/41/09	nie stwierdzono uchybień
64.	15-17.04.2009 r. DIS-K-421/64/09	Emmerson S.A. Warszawa, Al. Jana Pawła II 27	z urzędu	23.06.2009 r. Decyzja DIS/DEC-555/22716/09
65.	20-23.04.2009 r. DIS-K-421/65/09	Telekomunikacja Polska S.A. Warszawa, ul. Twarda 18	z urzędu	ustalenia wykorzystane do opracowania raportu dla Grupy Roboczej Art. 29
66.	20-24.04.2009 r. DIS-K-421/66/09	Foxberg Sp. z o.o. Częstochowa, ul. Krótka 27A	Starostwo Powiatowe w Nowym Tomyślu	15.09.2009 r. Decyzja DIS/DEC-919/33569/09
67.	20-23.04.2009 r. DIS-K-421/67/09	Polska Telefonía Cyfrowa Sp. z o.o. Warszawa, Al. Jerozolimskie 181	z urzędu	ustalenia wykorzystane do opracowania raportu dla Grupy Roboczej Art. 29
68.	20-23.04.2009 r. DIS-K-421/68/09	Polska Telefonía Komórkowa Centertel Sp. z o.o. Warszawa, ul. Skierniewicka 10A	z urzędu	ustalenia wykorzystane do opracowania raportu dla Grupy Roboczej Art. 29
69.	20-23.04.2009 r. DIS-K-421/69/09	Polkomtel S.A. Warszawa, ul. Postępu 3	z urzędu	ustalenia wykorzystane do opracowania raportu dla Grupy Roboczej Art. 29
70.	22-23.04.2009 r. DIS-K-421/71/09	Mirosław Prądyński prowadzący działalność gospodarczą pod nazwą „Przedsiębiorstwo Handlowo – Usługowe ALPOL”, Łask Kolumna, ul. Armii Ludowej 10	z urzędu	06.07.2009 r. pismo do Archiwum Państwowego w Warszawie
71.	27-30.04.2009 r. DIS-K-421/72/09	Geoformat sp.j. Florek - Paszkowscy, Kraków, ul. Kronikarza Galla 17/3	z urzędu	nie stwierdzono uchybień
72.	28-30.04.2009 r. DIS-K-421/73/09	CP Roman Fortuna Sp. z o.o. Warszawa, ul. Grzybowska 80/82	z urzędu	30.10.2009 r. decyzja DIS/DEC-1087/39964/09

73.	27-30.04.2009 r. DIS-K-421/74/09	Sąd Rejonowy w Sokołowie Podlaskim, Sokołów Podlaski, ul. ks. Bosco 3	z urzędu	30.06.2009 r. Decyzja DIS/DEC-587/23662/09
74.	27-30.04.2009 r. DIS-K-421/75/09	Dorota Chojnacka i Krzysztof Chojnacki prowadzący działalność gospodarczą pod nazwą „Global House Nieruchomości s.c.”, Łódź, ul. Zachodnia 70 lok. 113	z urzędu	nie stwierdzono uchybień
75.	28-30.04.2009 r. i 05-06.05.2009 DIS-K-421/76/09	Multikino S.A. Warszawa, ul. Wiertnicza 166	Departament Orzecznictwa Legislacji i Skarg	12.10.2009 r. decyzja DIS/DEC-1002/37026/09
76.	04-08.05.2009 r. DIS-K-421/77/09	Lidia Sołtysik prowadząca działalność gospodarczą pod nazwą „Przedsiębiorstwo Informatyczne KAMSOFT”, Katowice, ul. 1-go Maja 133	Departament Edukacji Społecznej i Współpracy Międzynarodowej	17.09.2009 r. Decyzja DIS/DEC-931/33969/09
77.	06-08.05.2009 r. DIS-K-421/78/09	Anna Brzozowska prowadząca działalność gospodarczą pod nazwą „eStore”, Częstochowa, ul. Czecha 2C/10	z urzędu	15.01.2010 r. decyzja DIS/DEC-28/1778/10
78.	11-13.05.2009 r. DIS-K-421/79/09	Skarbnica Narodowa Sp. z o.o. Warszawa, Al. Jana Pawła II 29	Departament Orzecznictwa Legislacji i Skarg	30.09.2009 r. Decyzja DIS/DEC-985/35481/09
79.	11-15.05.2009 r. DIS-K-421/80/09	Tomasz Majdan prowadzący działalność gospodarczą pod nazwą „Atago Soft”, Zielona Góra, ul. Piękna 2	Departament Edukacji Społecznej i Współpracy Międzynarodowej	brak przetwarzania danych osobowych
80.	11-14.05.2009 r. DIS-K-421/81/09	Łódzki Urząd Wojewódzki, Łódź, ul. Piotrkowska 104	z urzędu	13.11.2009 r. decyzja DIS/DEC-1139/41929/09
81.	11-15.05.2009 r. DIS-K-421/82/09	Madkom Sp. z o.o. Gdynia, Al. Zwycięstwa 96/98	Departament Orzecznictwa Legislacji i Skarg	13.05.2010 r. Decyzja DIS/DEC-576/19843/10
82.	18-20.05.2009 r. DIS-K-421/83/09	Carrefour Polska Sp. z o.o. Warszawa, ul. Targowa 72	z urzędu	01.02.2010 r. decyzja DIS/DEC-119/4291/10
83.	18-20.05.2009 r. DIS-K-421/84/09	Sąd Okręgowy Warszawa – Praga, Warszawa, Al. Solidarności 127	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
84.	18-21.05.2009 r. DIS-K-421/85/09	Akson sp.j. Padjasek – Krysowski, Katowice, ul. Ziołowa 47	z urzędu	16.07.2009 r. Decyzja DIS/DEC-636/25715/09
85.	20-22.05.2009 r. DIS-K-421/86/09	OME EQUÉ – Robert Wasik, Warszawa, ul. Osmańczyka 22/141	Departament Rejestracji Zbiorów Danych Osobowych	11.09.2009 r. Decyzja DIS/DEC-910/33153/09
86.	18-22.05.2009 r. DIS-K-421/87/09	Vattenfall Business Services Poland Sp. z o.o. Gliwice, Wybrzeże Armii Krajowej 19B	Departament Rejestracji Zbiorów Danych Osobowych	25.11.2009 r. decyzja DIS/DEC-1175/43655/09
87.	20-26.05.2009 r. DIS-K-421/88/09	Zarząd Transportu Miejskiego, Warszawa, ul. Senatorska 37	Departament Orzecznictwa Legislacji i Skarg	03.07.2009 r. Decyzja DIS/DEC-598/24248/09
88.	25-27.05.2009 r. DIS-K-421/89/09	Reader's Digest Przegląd Sp. z o.o. Warszawa, ul. Taśmowa 7	Departament Edukacji Społecznej i Współpracy Międzynarodowej	22.10.2009 r. decyzja DIS/DEC-1056/38787/09
89.	26-28.05.2009 r. DIS-K-421/90/09	Górnośląski Zakład Elektroenergetyczny S.A. Gliwice, ul. Barlickiego 2	Departament Rejestracji Zbiorów Danych Osobowych	28.09.2009 r. Decyzja DIS/DEC-972/35149/09

90.	26-29.05.2009 r. DIS-K-421/91/09	Vattenfall Distribution Poland S.A. Gliwice, ul. Portowa 14A	Departament Rejestracji Zbiorów Danych Osobowych	18.09.2009 r. Decyzja DIS/DEC-934/34058/09
91.	25-28.05.2009 r. DIS-K-421/92/09	Gestamp Polska Sp. z o.o. Września, ul. Działkowców 12	z urzędu	04.11.2009 r. decyzja DIS/DEC-1106/40727/09
92.	25-28.05.2009 r. DIS-K-421/93/09	Sąd Okręgowy w Siedlcach, Siedlce, ul. Sądowa 2	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
93.	27-29.05.2009 r. DIS-K-421/94/09	Sąd Okręgowy w Warszawie, Warszawa, Al. Solidarności 127	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
94.	01-03.06.2009 r. DIS-K-421/95/09	Naczelnik Urzędu Skarbowego w Siemianowicach Śląskich, Siemianowice Śląskie, ul. Świerczewskiego 84	z urzędu	17.08.2009 r. Decyzja DIS/DEC-812/30026/09
95.	02-04.06.2009 r. DIS-K-421/96/09	Polfactor S.A. Warszawa, ul. Królewska 14	z urzędu	16.07.2009 r. Decyzja DIS/DEC-634/25708/09
96.	03-05.06.2009 r. DIS-K-421/97/09	Krystyna Zdziechowska prowadząca działalność gospodarczą pod nazwą „Femaris Pharma Consulting”, Piaseczno, ul. Czarnieckiego 29	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
97.	03-05.06.2009 r. DIS-K-421/98/09	Generali Powszechnie Towarzystwo Emerytalne S.A. Warszawa, ul. Postępu 15B	Departament Orzecznictwa Legislacji i Skarg	18.08.2009 r. Decyzja DIS/DEC-826/30202/09
98.	08.06.2009 r. DIS-K-421/99/09	Ministerstwo Finansów, Warszawa, ul. Świętokrzyska 12	z urzędu	nie stwierdzono uchybień
99.	15-17.06.2009 r. DIS-K-421/100/09	Gemius S.A. Warszawa, ul. Wołoska 7	Departament Orzecznictwa Legislacji i Skarg	28.09.2009 r. Decyzja DIS/DEC-973/35153/09
100.	15-17.06.2009 r. DIS-K-421/101/09	Easycall.pl Sp. z o.o. Warszawa, ul. Poniecka 2/16	Departament Orzecznictwa Legislacji i Skarg	28.09.2009 r. Decyzja DIS/DEC-971/35147/09
101.	16-19.06.2009 r. DIS-K-421/102/09	Naczelnik Urzędu Skarbowego w Zawierciu, Zawiercie, ul. Leśna 8	z urzędu	16.09.2009 r. Decyzja DIS/DEC-926/33785/09
102.	15-17.06.2009 r. DIS-K-421/103/09	Niepubliczny Zakład Opieki Zdrowotnej „Hipokrates”, Piotrków Trybunalski ul. Wolborska 7A	Prokuratura Rejonowa w Piotrkowie Tryb.	18.09.2009 r. Decyzja DIS/DEC-933/34056/09
103.	17-19.06.2009 r. DIS-K-421/104/09	TNT Express Worldwide (Poland) Sp. z o.o. Warszawa, ul. Wirżowa 35	z urzędu	nie stwierdzono uchybień
104.	22-24.06.2009 r. DIS-K-421/105/09	DPD Polska Sp. z o.o. Warszawa, ul. Mineralna 15	z urzędu	30.09.2009 r. Decyzja DIS/DEC-984/35479/09
105.	22-26.06.2009 r. DIS-K-421/106/09	Bank Ochrony Środowiska S.A. Warszawa, Al. Jana Pawła II 12	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
106.	22-24.06.2009 r. DIS-K-421/107/09	Prefbet I Sp. z o.o. Dąbrowa Górnicza, ul. Fabryczna 1	Komisariat Policji	16.10.2009 r. pismo do Archiwum Państwowego w Warszawie
107.	22-25.06.2009 r. DIS-K-421/108/09	AEGON Towarzystwo Ubezpieczeń na Życie S.A. Warszawa, ul. Wołoska 5	Departament Orzecznictwa Legislacji i Skarg	03.12.2009 r. decyzja DIS/DEC-1204/44968/09
108.	29.06.-03.07.2009 DIS-K-421/109/09	Aviva Towarzystwo Ubezpieczeń Ogólnych S.A. Warszawa, ul. Prosta 70	Departament Rejestracji Zbiorów Danych Osobowych	12.10.2009 r. decyzja DIS/DEC-1000/37021/09

109.	22.06.2009 r. DIS-K-421/110/09	Abdank Sp. z o.o. Warszawa, ul. Brzozkowiowa 13	z urzędu	28.07.2009 r. zawiadomienie o przestępstwie
110.	29.06.-01.07.2009 DIS-K-421/111/09	Bibby Financial Services Sp. z o.o. Warszawa, ul. Rotmistrza Pileckiego 63	z urzędu	27.11.2009 r. decyzja DIS/DEC-1189/44066/09
111.	29.06.-01.07.2009 DIS-K-421/112/09	Hilton – Baird Polska Sp. z o.o. Warszawa, ul. Puławska 39/78	z urzędu	15.09.2009 r. decyzja DIS/DEC-920/33576/09
112.	06-09.07.2009 r. DIS-K-421/113/09	Miejskie Przedsiębiorstwo Komunikacyjne – Lublin Sp. z o.o. Lublin, Al. Kraśnicka 25	Departament Orzecznictwa Legislacji i Skarg	d31.03.2010 r. decyzja DIS/DEC-343/13671/10
113.	07-10.07.2009 r. DIS-K-421/114/09	Active Pharma Sp. z o.o. Legionowo, ul. Strużańska 7A	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
114.	08-10.07.2009 r. DIS-K-421/115/09	Warszawskie Zakłady Farmaceutyczne Polfa S.A. Warszawa, ul. Karolkowa 22/24	z urzędu	przywrócono stan zgodny z prawem
115.	08-10.07.2009 r. DIS-K-421/116/09	Grodziskie Zakłady Farmaceutyczne Polfa Sp. z o.o. Grodzisk Maz., ul. ks. J. Poniatowskiego 5	z urzędu	27.10.2009 r. decyzja DIS/DEC-1068/39457/09
116.	13-15.07.2009 r. DIS-K-421/117/09	Sąd Apelacyjny w Warszawie, Warszawa, Pl. Krasińskich 2/4/6	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
117.	13-15.07.2009 r. DIS-K-421/119/09	Sąd Okręgowy w Toruniu, Toruń, ul. Piekary 51	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
118.	20-23.07.2009 r. DIS-K-421/120/09	Siódemka S.A. Warszawa, ul. Matuszewska 14	z urzędu	17.11.2009 r. decyzja DIS/DEC-1148/42379/09
119.	20-23.07.2009 r. DIS-K-421/121/09	Powiatowy Urząd Pracy w Kielcach, Kielce, ul. Kolberga 4	Departament Rejestracji Zbiorów Danych Osobowych	18.02.2010 r. decyzja DIS/DEC-178/7025/10
120.	21-23.07.2009 r. DIS-K-421/122/09	Boiron Sp. z o.o. Piaseczno, ul. Raszyńska 13	z urzędu	nie stwierdzono uchybień
121.	20-23.07.2009 r. DIS-K-421/123/09	Sąd Okręgowy w Łodzi, Łódź, Pl. Dąbrowskiego 5	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
122.	20-23.07.2009 r. DIS-K-421/124/09	Sąd Apelacyjny w Łodzi, Łódź, Pl. Dąbrowskiego 5	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
123.	24 i 27.07.2009 r. DIS-K-421/125/09	Bank Handlowy w Warszawie S.A. Warszawa, ul. Senatorska 16	w związku z kontrolą DIS-K- 421/103/08	ustalenia wykorzystane w postępowaniu DIS-K-421/103/08
124.	27-29.07.2009 r. DIS-K-421/126/09	Sanofi – Aventis Sp. z o.o. Warszawa, ul. Bonifraterska 17	z urzędu	03.12.2009 r. decyzja DIS/DEC-1208/45000/09
125.	28-30.07.2009 r. DIS-K-421/127/09	Ministerstwo Sprawiedliwości, Warszawa, Al. Ujazdowskie 11	z urzędu	23.09.2009 r. pismo do Ministra Sprawiedliwości
126.	29.07.-04.08.2009 DIS-K-421/128/09	Link4 Towarzystwo Ubezpieczeń S.A. Warszawa, ul. Postępu 15	Departament Rejestracji Zbiorów Danych Osobowych	15.12.2009 r. decyzja DIS/DEC-1258/46983/09
127.	28-31.07.2009 r. DIS-K-421/129/09	ING Commercial Finance Polska S.A. Warszawa, ul. Chmielna 85/87	z urzędu	12.10.2009 r. decyzja DIS/DEC-1001/37022/09
128.	03-06.08.2009 r. DIS-K-421/130/09	Regionalny Szpital Specjalistyczny im. Biegańskiego w Grudziądzu, Grudziądz, ul. Sikorskiego 32	Prokuratura Rejonowa w Grudziądzu	03.12.2009 r. decyzja DIS/DEC-1207/44995/09
129.	04-07.08.2009 r. DIS-K-421/131/09	ZKM Veolia Transport Tczew Sp. z o.o. Tczew, ul. Armii Krajowej 86	z urzędu	03.12.2009 r. decyzja DIS/DEC-1205/44971/09

130.	10-13.08.2009 r. DIS-K-421/132/09	Pani Elżbieta Szymańska prowadząca działalność gospodarczą pod nazwą „Centrum Pośrednictwa Elizabeth Matki Zastępcze Surogatki”, Piaseczno, ul. Nad Perełką 21/20	Departament Rejestracji Zbiorów Danych Osobowych	29.12.2009 r. pismo do Marszałka Województwa Mazowieckiego oraz do Głównego Inspektora Pracy
131.	10-13.08.2009 r. DIS-K-421/133/09	Przedsiębiorstwo Komunikacji Miejskiej Sp. z o.o. Jaworzno, ul. Krakowska 9	Departament Orzecznictwa Legislacji i Skarg	06.05.2010 r. decyzja DIS/DEC-550/18830/10
132.	10-12.08.2009 r. DIS-K-421/134/09	Specjalistyczna Spółdzielnia Pracy „Skarbiec”, Warszawa, ul. Strzelecka 30/32	z urzędu	12.10.2009 r. Decyzja DIS/DEC-999/37016/09
133.	10-12.08.2009 r. DIS-K-421/135/09	Korurs Sp. z o.o. Warszawa, ul. Gierdziejewskiego 17	z urzędu	30.10.2009 r. decyzja DIS/DEC-1088/39966/09
134.	10-13.08.2009 r. DIS-K-421/136/09	Prografix Sp. z o.o. Dębica, ul. Drogowców 16	z urzędu	25.01.2010 r. decyzja DIS/DEC-93/3187/10
135.	17-20.08.2009 r. DIS-K-421/137/09	Starostwo Powiatowe w Łęborku, Łębork, ul. Czołgistów 5	z urzędu	18.02.2010 r. decyzja DIS/DEC-179/7035/10
136.	17-20.08.2009 r. DIS-K-421/138/09	Przedsiębiorstwo Informatyczne KAMSOFT Lidia Sołtysiak - Kamińska, Katowice, ul. 1-go Maja 133	z urzędu	15.12.2009 r. decyzja DIS/DEC-1261/46988/09
137.	17-18.08.2009 r. DIS-K-421/139/09	Kredyt Bank S.A., Warszawa, ul. Kasprzaka 2/8	z urzędu	nie stwierdzono uchybień
138.	17-21.08.2009 r. DIS-K-421/140/09	Zarząd Transportu Miejskiego, Gdańsk, ul. Na Stoku 49	z urzędu	15.01.2010 r. decyzja DIS/DEC-29/1781/10
139.	24-25.08.2009 r. DIS-K-421/141/09	Anmark B. Kryńska i Wspólnicy sp.j. Warszawa, ul. Fasolowa 1	z urzędu	30.10.2009 r. decyzja DIS/DEC-1089/39969/09
140.	24-27.08.2009 r. DIS-K-421/142/09	Starostwo Powiatowe w Wejherowie, Wejherowo, ul. 3-go Maja 4	w związku z kontrolą DIS-K-421/82/08	15.01.2010 r. decyzja DIS/DEC-30/1786/10
141.	24-26.08.2009 r. DIS-K-421/143/09	Adam Suchanecki prowadzący działalność gospodarczą pod nazwą „AS-INTER-BOX Drukarnia i Wytwórnia Opakowań Kartonowych do Żywności”, Warszawa, ul. Obozowa 84	z urzędu	nie stwierdzono uchybień
142.	25-28.08.2009 r. DIS-K-421/144/09	Violetta Szczepańska – Łacwik, Komornik Sądowy przy Sądzie Rejonowym dla Łodzi Śródmieścia, Łódź, ul. Próchnika 7	z urzędu	nie stwierdzono uchybień
143.	31.08.-03.09.2009 DIS-K-421/145/09	Julian Banachowicz, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Pragi Północ, Warszawa, ul. Ostrobramska 101	z urzędu	21.12.2009 r. decyzja DIS/DEC-1277/47648/09
144.	31.08.-03.09.2009 DIS-K-421/146/09	Piotr Adamczyk, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Śródmieścia, Warszawa, ul. Słomińskiego 1	z urzędu	15.12.2009 r. decyzja DIS/DEC-1259/46985/09
145.	07-10.09.2009 r. DIS-K-421/147/09	Miłosz Naworski, Piotr Wilczek, Mateusz Feldman i Marek Juszczynski – wspólnicy „4 Web Solutions s.c.” Wrocław, ul. Manganowa 4A/26	z urzędu	15.02.2010 r. decyzja DIS/DEC-164/6413/10
146.	07-10.09.2009 r. DIS-K-421/148/09	Leszek Cabaj, Komornik Sądowy przy Sądzie Rejonowym w Legionowie, Legionowo, ul. Kopernika 19	z urzędu	13.11.2009 r. decyzja DIS/DEC-1141/41947/09

147.	07-10.09.2009 r. DIS-K-421/149/09	Miejskie Przedsiębiorstwo Komunikacyjne w Siedlcach Sp. z o.o. Siedlce, ul. Starzyńskiego 20	z urzędu	30.04.2010 r. Decyzja DIS/DEC-544/18387/10
148.	14-17.09.2009 r. DIS-K-421/150/09	Jacek Bogiel, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Woli, Warszawa, ul. Karolkowa 58A	z urzędu	nie stwierdzono uchybień
149.	14-17.09.2009 r. DIS-K-421/151/09	Miejskie Przedsiębiorstwo Komunikacyjne Sp. z o.o. Inowrocław, ul. ks. Wawrzyniaka 33	z urzędu	18.01.2010 r. decyzja DIS/DEC-28/1981/10
150.	14-17.09.2009 r. DIS-K-421/152/09	Komunikacja Miejska – Płock Sp. z o.o. Płock, ul. Przemysłowa 17	z urzędu	27.04.2010 r. Decyzja DIS/DEC-516/17652/10
151.	10-11.09.2009 r. DIS-K-421/153/09	Zarząd Transportu Miejskiego, Warszawa, ul. Senatorska 37	z urzędu	Sprawa zakończona pismo z dn. 03.03.2010 r.
152.	15-18.09.2009 r. DIS-K-421/154/09	Prezydent Miasta Rybnika, Rybnik, ul. Bolesława Chrobrego 2	z urzędu	w toku
153.	21-25.09.2009 r. DIS-K-421/155/09	Grzegorz Oleśków prowadzący działalność gospodarczą pod nazwą „Inter Group”, Nysa, ul. Jeziorna 2 lok. 1	z urzędu	01.02.2010 r. Zawiadomienie o przestępstwie
154.	21-23.09.2009 r. DIS-K-421/156/09	Totalizator Sportowy Sp. z o.o. Warszawa, ul. Targowa 25	Departament Orzecznictwa Legislacji i Skarg	15.12.2009 r. pismo do Głównego Inspektora Pracy
155.	21-23.09.2009 r. DIS-K-421/157/09	Łukasz Łukaszewicz prowadzący działalność gospodarczą pod nazwą „TeamQuest Łukasz Łukaszewicz, Warszawa, Al. Jerozolimskie 49 lok. 3	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
156.	28-30.09.2009 r. DIS-K-421/158/09	Prezydent Miasta Krakowa, Kraków, Pl. Wszystkich Świętych 3/4	Departament Orzecznictwa Legislacji i Skarg	22.12.2009 r. decyzja DIS/DEC-1290/48005/09
157.	22-24.09.2009 r. DIS-K-421/159/09	EFG Eurobank Ergasias S.A. Oddział w Polsce, Warszawa, ul. Mokotowska 19	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
158.	21-25.09.2009 r. DIS-K-421/160/09	Grimp Sp. z o.o. Zielona Góra, ul. Lisowskiego 7	z urzędu	29.12.2009 r. decyzja DIS/DEC-1328/48578/09
159.	21-25.09.2009 r. DIS-K-421/161/09	QLS Sp. z o.o. Zielona Góra, ul. Lisowskiego 9A	z urzędu	29.12.2009 r. decyzja DIS/DEC-1329/48580/09
160.	21-24.09.2009 r. DIS-K-421/162/09	ENEA S.A., Poznań, ul. Nowowiejskiego 11	Departament Orzecznictwa Legislacji i Skarg	15.12.2009 r. decyzja DIS/DEC-1262/46989/09
161.	29.09.-02.10.2009 DIS-K-421/163/09	Artur Królasik, Komornik Sądowy przy Sądzie Rejonowym w Wołominie, Wołomin, ul. Legionów 8	z urzędu	13.11.2009 r. decyzja DIS/DEC-1140/41931/09
162.	28-29.09.2009 r. DIS-K-421/164/09	Agnieszka Bekisz prowadząca działalność gospodarczą pod nazwą „Doradztwo Finansowe”, Warszawa, ul. Jana Olbrachta 15 m. 3	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
163.	28.09.-01.10.2009 DIS-K-421/165/09	Dariusz Dybcio, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Mokotowa, Warszawa, ul. Puławska 12/1	z urzędu	23.11.2009 r. decyzja DIS/DEC-1173/43215/09
164.	28-29.09.2009 r. 01.10.2009 r. DIS-K-421/166/09	Polski Związek Działkowców – Okręgowy Zarząd Mazowiecki, Warszawa, ul. Dywizjonu 303 nr 7	Departament Orzecznictwa Legislacji i Skarg	23.02.2010 r. decyzja DIS/DEC-189/7691/10

165.	06.10.2009 r. DIS-K-421/167/09	Google Poland Sp. z o.o. Warszawa, ul. E. Plater 53	Departament Orzecznictwa Legislacji i Skarg	22.12.2009 r. decyzja DIS/DEC-1289/47989/09
166.	06-09.10.2009 r. DIS-K-421/168/09	Powiatowy Urząd Pracy w Wołominie, Wołomin, ul. Warszawska 5A	z urzędu	nie stwierdzono uchybień
167.	06-09.10.2009 r. DIS-K-421/169/09	Powiatowy Urząd Pracy w Nowym Dworze Mazowieckim, Nowy Dwór Mazowiecki, ul. Słowackiego 6	z urzędu	nie stwierdzono uchybień
168.	05-08.10.2009 r. DIS-K-421/170/09	Prezydent Miasta Tczewa, Tczew, Pl. Piłsudskiego 1	w związku z kontrolą DIS-K- 421/131/09	23.02.2010 r. Decyzja DIS/DEC-188/76881/10
169.	06-09.10.2009 r. DIS-K-421/171/09	Wojewódzki Urząd Pracy w Warszawie, Warszawa, ul. Młynarska 16	z urzędu	nie stwierdzono uchybień
170.	12-15.10.2009 r. DIS-K-421/172/09	Powiatowy Urząd Pracy w Wyszkanie, Wyszaków, ul. Kościuszki 15	z urzędu	nie stwierdzono uchybień
171.	12-14.10.2009 r. DIS-K-421/173/09	Marek Michalewicz, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Żoliborza, Warszawa, ul. Wrocławska 2A	z urzędu	09.12.2009 r. decyzja DIS/DEC-1237/46117/09
172.	13-15.10.2009 r. DIS-K-421/174/09	Anna Bachańska, Komornik Sądowy przy Sądzie Rejonowym w Otwocku, Otwock, ul. Andriollego 40/6	z urzędu	nie stwierdzono uchybień
173.	14-16.10.2009 r. DIS-K-421/175/09	Maciej Gierszewski, Komornik Sądowy przy Sądzie Rejonowym w Nowym Dworze Mazowieckim, Nowy Dwór Mazowiecki, ul. Nałęczka 37	z urzędu	23.11.2009 r. decyzja DIS/DEC-1174/43217/09
174.	13-16.10. 2009 r. 21-22.10.2009 r. DIS-K-421/176/09	MNI Premium S.A. Warszawa, ul. Żurawia 8	Departament Orzecznictwa Legislacji i Skarg	w toku
175.	16.10.2009 r. DIS-K-421/177/09	Piotr Bławicki prowadzący działalność gospodarczą pod nazwą „DATA Piotr Bławicki”, Warszawa, ul. Skarbka z Gór 17D/28	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
176.	19-22.10.2009 r. DIS-K-421/178/09	Powiatowy Urząd Pracy w Legionowie, Legionowo, ul. Sikorskiego 11	z urzędu	nie stwierdzono uchybień
177.	19-22.10.2009 r. DIS-K-421/179/09	Powiatowy Urząd Pracy w Otwocku, Otwock, ul. Górna 11	z urzędu	nie stwierdzono uchybień
178.	21-23.10.2009 r. DIS-K-421/180/09	Krzysztof Pawkowski, Komornik Sądowy przy Sądzie Rejonowym w Piasecznie, Piaseczno, ul. Powstańców Warszawy 21A	z urzędu	przywrócono stan zgodny z prawem
179.	21-23.10.2009 r. DIS-K-421/181/09	Jakub Jabłoński, Komornik Sądowy przy Sądzie Rejonowym w Wyszkanie, Wyszaków, ul. Daszyńskiego 21	z urzędu	15.12.2009 r. decyzja DIS/DEC-1263/46990/09
180.	21-23.10.2009 r. DIS-K-421/182/09	Maria Wasilewska, Komornik Sądowy przy Sądzie Rejonowym w Pruszkowie, Pruszków, ul. Kraszewskiego 44/5	z urzędu	12.01.2010 r. decyzja DIS/DEC-7/1147/10

181.	26-28.10.2009 r. DIS-K-421/183/09	Ireneusz Grobelny, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Pragi Południe, Warszawa, ul. Targowa 33	z urzędu	15.01.2010 r. decyzja DIS/DEC-31/1788/10
182.	26-29.10.2009 r. DIS-K-421/184/09	Powiatowy Urząd Pracy w Pruszkowie, Pruszków, ul. Andrzeja 29	z urzędu	nie stwierdzono uchybień
183.	26-29.10.2009 r. DIS-K-421/185/09	Provident Polska S.A. Warszawa, ul. Polna 11	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
184.	28-30.10.2009 r. DIS-K-421/186/09	Agora S.A., Warszawa, ul. Czerska 8/10	z urzędu	01.02.2010 r. decyzja DIS/DEC-118/4289/10
185.	27-30.10.2009 r. DIS-K-421/187/09	Powiatowy Urząd Pracy w Piasecznie, Piaseczno, ul. Szkolna 20	z urzędu	nie stwierdzono uchybień
186.	04-06.11.2009 r. DIS-K-421/188/09	Magdalena Zgutczyńska prowadząca działalność gospodarczą pod nazwą „Arsedo Poland”, Warszawa, ul. Głuszcza 6	Departament Orzecznictwa Legislacji i Skarg	13.05.2010 r. Decyzja DIS/DEC-575/19830/10
187.	04-06.11.2009 r. DIS-K-421/189/09	Renata Delert, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Pragi Północ, Warszawa, ul. Lęborska 8/10	z urzędu	nie stwierdzono uchybień
188.	05-06.11.2009 r. 09.11.2009 r. DIS-K-421/190/09	Piotr Tyc, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Śródmieścia, Warszawa, ul. Śniadeckich 17	z urzędu	17.03.2010 r. Decyzja DIS/DEC-276/11299/10
189.	04-05.11.2009 r. DIS-K-421/191/09	Polski Związek Działkowców, Warszawa, ul. Towarowa 7A	w związku z kontrolą DIS-K-421/166/09	12.01.2010 r. decyzja DIS/DEC-14/1248/10
190.	12-13.11.2009 r. DIS-K-421/192/09	Happy Holiday Travel Duo Sp. z o.o. Warszawa, ul. Czackiego 3/5	z urzędu	wykonano decyzję DIS/DEC-317/14294/09
191.	09-10.11.2009 r. DIS-K-421/193/09	Spółdzielnia Mieszkaniowa „Nowe Miasto”, Warszawa, ul. Bonifraterska 14	z urzędu	wykonano decyzję DIS/DEC-307/13545/09
192.	17-18.12.2009 r. DIS-K-421/194/09	Info Veriti Polska Sp. z o.o. Warszawa, ul. Serwituty 23	Departament Orzecznictwa Legislacji i Skarg	W toku
193.	16-19.11.2009 r. DIS-K-421/195/09	Powiatowy Urząd Pracy w Mińsku Mazowieckim Mińsk Mazowiecki, ul. Warszawska 222	z urzędu	nie stwierdzono uchybień
194.	17-19.11.2009 r. DIS-K-421/196/09	Magdalena Gulcz prowadząca działalność gospodarczą pod nazwą „Centrum Terapii Poznawczo – Behawioralnej Magdalena Gulcz”, Warszawa, ul. Wilcza 28/20	Departament Orzecznictwa Legislacji i Skarg	03.03.2010 r. decyzja DIS/DEC-236/9120/10
195.	18-20.11.2009 r. DIS-K-421/197/09	Maciej Simbierowicz, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Woli, Warszawa, ul. Złota 81	z urzędu	nie stwierdzono uchybień
196.	23-24.11.2009 r. DIS-K-421/198/09	Spółdzielnia Budowlano – Mieszkaniowa „Batory”, Warszawa, ul. Bruna 32	z urzędu	wykonano decyzję DIS/DEC-858/35334/08
197.	23-24.11.2009 r. DIS-K-421/199/09	Cinema City Poland Sp. z o.o. Warszawa, ul. Fosa 37	z urzędu	wykonano decyzję DIS/DEC-582/25214/08
198.	23-24.11.2009 r. DIS-K-421/200/09	Spółdzielnia Mieszkaniowa „3 Maja”, Warszawa, Al. 3 Maja 5/4	z urzędu	wykonano decyzję DIS/DEC-748/31712/08

199.	24-27.11.2009 r. DIS-K-421/201/09	Powiatowy Urząd Pracy w Grodzisku Mazowieckim, Grodzisk Maz., ul. Daleka 11A	z urzędu	nie stwierdzono uchybień
200.	23-24.11.2009 r. DIS-K-421/202/09	Spółdzielnia Mieszkaniowa „Górczewska”, Warszawa, ul. Doroszewskiego 4	z urzędu	wykonano decyzję DIS/DEC-775/33105/08
201.	25-27.11.2009 r. DIS-K-421/203/09	EuroLot S.A. Warszawa, ul. 17 Stycznia 39	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
202.	17-19.11.2009 r. DIS-K-421/204/09	Info Veriti Polska Sp. z o.o. Obsługa Serwisu Internetowego sp.j. Warszawa, ul. Serwituty 23	w związku z kontrolą DIS-K- 421/194/09	w toku
203.	02-04.12.2009 r. DIS-K-421/205/09	Marcin Bielicki, Warszawa, ul. Wałowa 7/30	Departament Rejestracji Zbiorów Danych Osobowych	12.03.2010 r. decyzja DIS/DEC-259/10562/10
204.	02-04.12.2009 r. DIS-K-421/206/09	Marcin Pieńkos, Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Mokotowa, Warszawa, ul. Cybernetyki 13	z urzędu	nie stwierdzono uchybień
205.	08-09.12.2009 r. DIS-K-421/208/09	Polski Związek Działkowców – Okręgowy Zarząd Mazowiecki, Warszawa, ul. Dywizjonu 303 nr 7	w związku z kontrolą DIS-K- 421/166/09	23.02.2010 r. decyzja DIS/DEC-189/7691/10
206.	03-04.12.2009 r. DIS-K-421/209/09	Stowarzyszenie „Mieszkańcy Osiedla Grabina”, Michałów – Grabina, ul. Grabowa 7	z urzędu	w toku
207.	07-10.12.2009 r. DIS-K-421/210/09	Handelo Sp. z o.o. Michałowice, ul. 11 Listopada 13	Departament Orzecznictwa Legislacji i Skarg	27.04.2010 r. decyzja DIS/DEC-511/17640/10
208.	08.12.2009 r. DIS-K-421/211/09	Blueberry Communication Group Sp. z o.o. Warszawa, ul. Jelinka 27	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
209.	07-10.12.2009 r. DIS-K-421/212/09	Naftor Sp. z o.o. Warszawa, ul. Smoleńskiego 2	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
210.	09-11.12.2009 r. DIS-K-421/213/09	Operator Logistyczny Paliw Płynnych Sp. z o.o. Warszawa, ul. Chałbińskiego 8	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
211.	10-11.12.2009 r. 14.12.2009 r. DIS-K-421/214/09	Unicomp-WZA Sp. z o.o. Warszawa, ul. Bacha 34A	z urzędu	nie stwierdzono uchybień
212.	14-18.12.2009 r. DIS-K-421/215/09	Votum-RehaPlus S.A. Kraków, ul. Golikówka 6	Departament Rejestracji Zbiorów Danych Osobowych	w toku
213.	15-16.12.2009 r. DIS-K-421/216/09	Home Broker S.A. Warszawa, ul. Domaniewska 39A	z urzędu	zakończona - wykonano w całości decyzję GIDO
214.	14-18.12.2009 r. DIS-K-421/217/09	Quality Audit House Sp. z o.o. Łódź, ul. Zawiszy Czarnego 8/10	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
215.	14-18.12.2009 r. DIS-K-421/218/09	Zarząd Transportu Miejskiego w Poznaniu, Poznań, ul. Grunwaldzka 104	z urzędu	w toku
216.	14-18.12.2009 r. DIS-K-421/219/09	Miejskie Przedsiębiorstwo Komunikacyjne w Poznaniu Sp. z o.o. Poznań, ul. Głogowska 131/133	z urzędu	nie stwierdzono uchybień

217.	14-18.12.2009 r. DIS-K-421/220/09	Wykop Sp. z o.o. Poznań, ul. Zakręt 8	z urzędu	02.04.2010 r. decyzja DIS/DEC-366/14077/10
218.	14-18.12.2009 r. DIS-K-421/221/09	Szpital Specjalistyczny św. Wojciecha – Samodzielny Publiczny Zakład Opieki Zdrowotnej, Gdańsk, Al. Jana Pawła II 50	Departament Orzecznictwa Legislacji i Skarg	06.05.2010 r. decyzja DIS/DEC-551/18832/10
219.	17-18.12.2009 r. DIS-K-421/222/09	Grono.net S.A., Warszawa, ul. Szturmowa 2A	w związku z kontrolami DIS-K- 421/62/08 i DIS-K- 421/81/08	nie stwierdzono uchybień
220.	18 i 21-22.12.2009 DIS-K-421/223/09	Jolanta Połajewska, Komornik Sądowy przy Sądzie Rejonowym dla m.st. Warszawy, Warszawa, ul. Wojciechowskiego 17	z urzędu	nie stwierdzono uchybień

**Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie
i Naczelnego Sądu Administracyjnego
wydanych w 2009 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.	16.01.2009 r. II SA/Wa 1550/07	GI-DEC-DOLiS- 154/07/4023	Skarga kasacyjna na postanowienie WSA w Warszawie w sprawie skargi na decyzje GODO w przedmiocie przetwarzania danych osobowych	odrzućcie skargi kasacyjnej
2.	20.01.2009 r. II SA/Wa 1003/08	DOLiS/DEC- 300/08/12622,12625, 12626,12628,12630,1 2632,12633	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
3.	20.01.2009 r. II SA/Wa 763/08	DOLiS/DEC- 230/08/911,9115, 9117	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
4.	22.01.2009 r. II SA/Wa 1710/08	DEC/DOLiS- 629/08/26650	Wniosek o wstrzymanie wykonania zaskarżonej decyzji	odmowa wstrzymania zaskarżonej decyzji
5.	23.01.2009 r. II SA/Wa 917/08	DOLiS/DEC- 257/08/10742	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych ze zbioru danych	uchylenie zaskarżonej decyzji
6.	28.01.2009 r. I OSK 8/09	DOLiS/DEC- 354/08/14530	Zażalenie na postanowienie WSA w Warszawie o odmowie wstrzymania wykonania decyzji GODO	oddalenie zażalenia
7.	03.02.2009 r. II SA/Wa 1156/08	DOLiS/DEC- 345/08/14201,14206, 14209	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
8.	04.02.2009 r. II SA/Wa 615/08	DOLiS/DEC- 180/08/6930,6935	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
9.	09.02.2009 r. II SA/Wa 222/08	GI-DEC-DOLiS- 272/07/7160,7161	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
10.	10.02.2009 r. I OSK 1743/07	GI-DEC-DOLiS- 451/06/1307,1308	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
11.	12.02.2009 r. II SA/Wa 1721/08	DOLiS/DEC- 609/08/26029,26032	Skarga na decyzję w przedmiocie udostępniania danych osobowych	oddalenie skargi
12.	13.02.2009 r. II SA/Wa 16/09	DOLiS/DEC- 710/08/29509,29512	Wniosek o wstrzymanie wykonania zaskarżonej decyzji	odmowa wstrzymania zaskarżonej decyzji
13.	17.02.2009 r. II SA/Wa 688/08	GI-DS-430- 867/05/3397/07/ DOLiS	Wniosek o przywrócenie terminu do wniesienia skargi na postanowienie w przedmiocie odmowy przywrócenia terminu	przywrócenie terminu do wniesienia skargi
14.	17.02.2009 r. II SA/Wa 1711/08	DEC/DOLiS- 629/08/26649	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi

15.	18.02.2009 r. I OSK 174/08	GI-DEC-DOLiS - 109/07/2885	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
16.	18.02.2009 r. II SA/Wa 1568/08	DOLiS/DEC- 535/08/23778,23782, 23786	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych	uchylenie zaskarżonej decyzji
17.	23.02.2009 r. II SAB/Wa 1/09	DOLiS/DEC- 8/09/301,305	Skarga na bezczynność GODO w przedmiocie przetwarzania danych osobowych	umorzenie postępowania przed WSA w Warszawie
18.	26.02.2009 r. I OSK 499/08	GI-DEC-DIS- 46/07/340	Opracowanie i wdrożenie polityki bezpieczeństwa, zmodyfikowanie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w zakresie dotyczącym częstotliwości zmiany hasła użytkownika, tak, aby zawierała postanowienie wskazujące na zmianę hasła nie rzadziej niż raz na 30 dni, zapewnienie, aby system informatyczny o nazwie „WF-MAG” zapewniał dla każdej osoby, której dane osobowe są przetwarzane w tym systemie, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego te dane.	oddalenie skargi kasacyjnej
19.	26.03.2009 r. I OSK 227/07	DIS/DEC- 421/17115/08	Przetwarzanie danych osobowych użytkowników imiennych przedpłaconych kart płatniczych na podstawie zgody wyrażonej przez użytkowników ww. kart, realizacja obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych, wobec użytkowników imiennych przedpłaconych kart płatniczych.	wstrzymanie wykonania decyzji
20.	28.08.2009 r. I OSK 1472/08	DIS/DEC- 217/8459/08	Zapewnienie, aby system informatyczny służący do przetwarzania danych zapewniał odnotowanie, sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w tym systemie, raportu zawierającego w powszechnie zrozumiałej formie informacje o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, których dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.	oddalenie skargi kasacyjnej
21.	27.02.2009 r. II SA/Wa 1252/07	GI-DEC-DOLiS - 109/07/2885	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
22.	02.03.2009 r. II SA/Wa 1177/08	DOLiS/DEC- 375/08/15721,15725	Skarga na decyzję w przedmiocie nakazania wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych.	oddalenie skargi
23.	02.03.2009 r. II SA/Wa 688/08	GI-DS-430- 867/05/3397/07/DOLi S	Wniosek o przywrócenie terminu do wniesienia skargi na postanowienie w przedmiocie odmowy przywrócenia terminu	przywrócenie terminu do wniesienia skargi
24.	03.03.2009 r. II SA/Wa 1495/08	DOLiS/DEC- 515/0822854,22857	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
25.	06.03.2009 r. II SA/Wa 1554/08	DOLiS/DEC- 511/08/22299,22300, 22301	Skarga na decyzję w przedmiocie ochrony danych osobowych	stwierdzenie nieważności zaskarżonej decyzji

26.	10.03.2009 r. II SA/Wa 1706/08	DOLiS/DEC- 630/08/26741,26742, 26745,26748	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych.	uchylenie zaskarżonej decyzji
27.	10.03.2009 r. II SA/Wa 1707/08	DOLiS/DEC- 630/08/26741,26742, 26745,26748	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych.	uchylenie zaskarżonej decyzji
28.	12.03.2009 r. II SA/Wa 526/08	DOLiS/POST- 37/08/2663,2664	Skarga na postanowienie w przedmiocie odmowy przywrócenia terminu	uchylenie zaskarżonego postanowienia
29.	12.03.2009 r. II SA/Wa 1408/08	DOLiS/DEC- 468/08/20369,20373, 20376	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	uchylenie zaskarżonej decyzji
30.	18.03.2009 r. I OSK 544/08	GI-DEC-DOLiS- 98/07/2672,2673,267 4	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego wyroku
31.	19.03.2009 r. II SA/Wa 1349/08	DOLiS/DEC- 479/08/20756,20759	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ochrony danych osobowych	uchylenie zaskarżonej decyzji
32.	23.03.2009 r. I OSK 376/08	GI-DS- 430/559/06/3118,311 9/07/DOLiS	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	uchylenie zaskarżonego wyroku
33.	02.04.2009 r. II SA/Wa 230/09	DOLiS/DEC- 807/08/34464,34466	Skarga na decyzję w przedmiocie nakazu udostępniania danych osobowych dziennikarza	oddalenie skargi
34.	02.04.2009 r. I OSK 377/08	GI-DS- 430/558/06/3116,311 7/07/DOLiS	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku o przesłanie kserokopii i odpisu materiału dowodowego	uchylenie zaskarżonego wyroku WSA w Warszawie
35.	03.04.2009 r. I OZ 271/09	DOLiS/DEC- 629/08/26650	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych ze zbioru danych	oddalenie zażalenia
36.	09.04.2009 r. II SA/Wa 1711/08	DOLiS/DEC- 629/08/26649	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
37.	10.04.2009 r. II SA/Wa 1823/07	GI-DEC-DOLiS- 148/07/3926,3927	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego WSA w Warszawie
38.	15.04.2009 r. II SA/Wa 1568/08	DOLiS/DEC- 535/08/23778,23782, 23786	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych.	uchylenie zaskarżonej decyzji
39.	24.04.2009 r. I OSK 500/08	GI-DEC-DOLiS- 186/07/4985,4986,49 87	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzje GIODO w przedmiocie przetwarzania danych osobowych.	oddalenie skargi kasacyjnej
40.	04.05.2009 r. II SA/Wa 1818/07	GI-DEC-DOLiS- 186/07/4985,4986,49 87	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
41.	04.05.2009 r. I OZ 375/09	DOLiS/DEC- 710/08/29509,29512	Zażalenie na postanowienie WSA w Warszawie o odmowie wstrzymania wykonania zaskarżonej decyzji GIODO	oddalenie zażalenia
42.	05.05.2009 r. II SA/Wa 363/09	DOLiS/DEC- 806/08/34210,34212, 34214	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	umorzenie postępowania przed WSA w Warszawie
43.	13.05.2009 r. II SA/Wa 1706/08	DOLiS/DEC- 630/08/26741,26742, 26745,26748	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych.	uchylenie zaskarżonej decyzji
44.	13.05.2009 r. II SA/Wa 1707/08	DOLiS/DEC- 630/08/26741,26742, 26745,26748	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	uchylenie zaskarżonej decyzji

45.	13.05.2009 r. II SA/Wa 1554/08	DOLiS/DEC- 511/08/22299,22300, 22301	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzje GODO w przedmiocie ochrony danych osobowych.	oddalenie skargi kasacyjnej
46.	14.05.2009 r. II SA/Wa 1430/08	DOLiS/DEC- 481/08/21011,21015, 21019	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	oddalenie skargi
47.	15.05.2009 r. II SA/Wa 365/09	DOLiS/DEC- 711/08/29649,29651, 29656,29658,29660	Skarga na decyzję w przedmiocie ochrony danych osobowych	umorzenie postępowania przed WSA w Warszawie
48.	18.05.2009 r. II SA/Wa 567/09	DOLiS/DEC- 109/09/4751,4752	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
49.	21.05.2009 r. II SA/Wa 1347/08	DOLiS/DEC- 488/08/21517,21518, 21519,21520	Skarga na decyzję w przedmiocie umorzenia postępowania	uchylenie zaskarżonej decyzji
50.	27.05.2009 r. II SA/Wa 1614/08	DOLiS/DEC- 546/08/24129,24321	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	uchylenie zaskarżonej decyzji
51.	29.05.2009 r. I OZ 533/09	DOLiS/DEC- 598/08/25416	Zażalenie na postanowienie WSA w Warszawie o odmowie wstrzymania wykonania zaskarżonej decyzji GODO	uchylenie zaskarżonej decyzji
52.	01.06.2009 r. II SA/Wa 364/09	DOLiS/DEC- 806/08/34210,34212, 34214	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
53.	03.06.2009 r. II SA/Wa 86/09	DOLiS/POST- 351/08/32706,32709	Skarga na postanowienie w przedmiocie stwierdzenia nie dopuszczalności wniosku o ponowne rozpatrzenie sprawy	uchylenie zaskarżonego postanowienia
54.	08.06.2009 r. II SA/Wa 230/09	DOLiS/DEC- 807/08/34464,34466	Skarga na decyzję w przedmiocie nakazu udostępnienia danych dziennikarza	oddalenie skargi
55.	09.06.2009 r. II SA/Wa 248/09	DOLiS/DEC- 903/08/35920,35923	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
56.	10.06.2009 r. II SA/Wa 1233/08	DOLiS/DEC- 393/08/16167	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych ze zbioru danych	uchylenie zaskarżonej decyzji
57.	10.06.2009 r. II SA/Wa 124/09	DIS/DEC- 752/32101/08	Zaprzestanie przetwarzania danych bez podstawy prawnej, opracowanie w formie pisemnej polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych, wyznaczenie administratora bezpieczeństwa informacji.	uchylenie zaskarżonej decyzji
58.	20.06.2009 r. II SA/Wa 234/09	DOLiS/DEC- 904/08/35949	Skarga na decyzję w przedmiocie odmowy stwierdzenia nieważności decyzji w sprawie usunięcia uchyleń w procesie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
59.	22.06.2009 r. II SA/Wa 1165/08	GI-DOLiS- 430/210/07	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych ze zbioru danych	uchylenie zaskarżonej decyzji
60.	22.06.2009 r. II SA/Wa 412/09	GI-DEC-DOLiS- 148/07/3926,3927	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
61.	24.06.2009 r. I OSK 440/08	GI-DEC-DOLiS- 113/07/2904,2905,29 06	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzje GODO w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
62.	25.06.2009 r. II SA/Wa 1710/08	DOLiS/DEC- 629/08/26650	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
63.	26.06.2009 r. I OSK 667/09	DOLiS/DEC- 515/08/22854,22857	Wniosek o wstrzymanie wykonania zaskarżonej decyzji GODO	oddalenie wniosku

64.	30.06.2009 r. I OSK 808/08	GI-DEC-DOLiS- 24/07/579,580,581,58 2,583,584,585	Skarga kasacyjna na postanowienie WSA w Warszawie w sprawie skargi na decyzje GODO w przedmiocie przetwarzania danych osobowych	oddalenie skargi kasacyjnej
65.	01.07.2009 r. II SA/Wa 1765/08	DOLiS/DEC- 663/08/27697,27698, 27699,27705	Skarga na decyzję w przedmiocie odmowy wznowienia postępowania	uchylenie zaskarżonej decyzji
66.	02.07.2009 r. I OSK 674/06	GI-DEC-DOLiS- 199/07/5336,5337,53 38	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzje GODO w przedmiocie nakazania usunięcia danych osobowych	oddalenie skargi kasacyjnej
67.	06.07.2009 r. I OZ 626-628/09	GI-DEC-DOLiS- 154/07/4023	Zażalenie na postanowienie WSA w Warszawie odrzucające zażalenie na postanowienie WSA w Warszawie o odrzuceniu skargi kasacyjnej na decyzję GODO w przedmiocie przetwarzania danych osobowych	oddalenie zażalenia
68.	07.07.2009 r. II SA/Wa 340/09	GI-DS- 430/559/06/3118,311 9/07/DOLiS	Skarga na postanowienie GODO w przedmiocie odmowy uwzględnienia wniosku.	oddalenie skargi
69.	08.07.2009 r. II SA/Wa 1644/08	DOLiS/DEC- 543/08/24258,24262	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
70.	08.07.2009 r. II SA/Wa 645/07	GI-DEC-DOLiS- 24/07/579,580,581,58 2,583,584,585	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
71.	09.07.2009 r. II SA/Wa 1685/08	DOLiS/DEC- 605/08/25845,25846	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
72.	10.07.2009 r. II SA/Wa 1979/07	GI-DEC-DOLiS- 199/07/5336,5337,53 38	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych	uchylenie zaskarżonej decyzji
73.	13.07.2009 r. II SA/Wa 65/09	DOLiS/DEC- 731/08/31085,31088	Skarga na decyzję w przedmiocie umorzenia postępowania	oddalenie skargi
74.	16.07.2009 r. II SA/Wa 527/08	DOLiS/DEC- 75/08/2351	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
75.	20.07.2009 r. II SA/Wa 1614/08	DOLiS/DEC- 546/08/24129,24321	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	uchylenie zaskarżonej decyzji
76.	24.07.2009 r. II SA/Wa 31/09	DOLiS/DEC- 701/08/29206,29213, 29215,29217	Skarga na decyzję w przedmiocie udostępniania danych osobowych	umorzenie postępowania w sprawie
77.	24.07.2009 r. II SA/Wa 364/09	DOLiS/DEC- 806/08/34210,34212, 34214	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	odrzućcie skargi
78.	27.07.2009 r. I OSK 748/08	GI-DOLiS- 430/131/07/4446	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na postanowienie GODO w przedmiocie zwrotu skargi w sprawie przetwarzania danych osobowych	uchylenie zaskarżonego wyroku
79.	27.07.2009 r. I OSK 633/08	GI-DEC-DOLiS- 176/07/4650,4651,46 52	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzje GODO w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
80.	31.07.2009 r. II SA/Wa 324/09	GI-DEC-DOLiS- 98/07/2672,2673,267 4	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
81.	03.08.2009 r. II SA/Wa 1801/07	GI-DEC-DOLiS- 176/07/4650,4651,46 52	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi

82.	05.08.2009 r. II SA/Wa 1726/08	DOLiS/POST- 329/08/29221	Skarga na postanowienie w przedmiocie zwrotu skargi wobec nie uiszczenia należności tytułem opłaty skarbowej	uchylenie zaskarżonego postanowienia
83.	06.08.2009 r. II SA/Wa 940/09	DOLiS/DEC- 285/09/12865,12867	Skarga na decyzję w przedmiocie nakazania udostępniania danych osobowych	wstrzymanie wykonania zaskarżonej decyzji
84.	06.08.2009 r. II SA/Wa 304/09	DOLiS/DEC- 64/09/2530,2532	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
85.	13.08.2009 r. II SA/Wa 234/09	DOLiS/DEC- 904/08/35949	Skarga na decyzję w przedmiocie odmowy stwierdzenia nieważności decyzji w sprawie usunięcia uchybień w procesie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
86.	18.08.2009 r. II SA/Wa 1550/07	GI-DEC-DOLiS- 154/07/4023	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
87.	20.08.2009 r. II SA/Wa 1165/08	GI-DEC-DOLiS- 430/210/07	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych	uchylenie zaskarżonej decyzji
88.	27.08.2009 r. II SA/Wa 1710/08	DOLiS/DEC- 629/08/26650	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
89.	31.08.2009 r. II SA/Wa 1165/08	DOLiS/DEC- 663/08/27697,27698, 27699,277705	Skarga na decyzję w przedmiocie odmowy wznowienia postępowania	uchylenie zaskarżonej decyzji
90.	02.09.2009 r. II SA/Wa 1233/08	DOLiS/DEC- 393/08/16167	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych ze zbioru danych	uchylenie zaskarżonej decyzji
91.	08.09.2009 r. II SA/Wa 1554/08	DOLiS/DEC- 511/08/22299,22300, 22301	Skarga na decyzję w przedmiocie ochrony danych osobowych	stwierdzenie nieważności zaskarżonej decyzji
92.	08.09.2009 r. I OSK 1377/08	DIS/DEC-172/6400, 6404/08	Zapewnienie, aby system informatyczny służący do przetwarzania danych zapewniał odnotowanie, sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w tym systemie, raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu.	uchylenie zaskarżonego wyroku i oddalenie skargi
93.	08.09.2009 r. I OSK 1378/08	DIS/DEC- 216/8457/08	Zapewnienie, aby system informatyczny służący do przetwarzania danych zapewniał odnotowanie, sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w tym systemie, raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu.	uchylenie zaskarżonego wyroku i oddalenie skargi
94.	08.09.2009 r. I OSK 1379/08	DIS/DEC- 215/8454/08	Przyznanie statusu administratora danych.	oddalenie skargi
95.	09.09.2009 r. II SA/Wa 365/09	DOLiS/DEC- 711/08/29649,29651, 29656,29658,29660	Skarga na decyzję w przedmiocie ochrony danych osobowych	umorzenie postępowania w sprawie
96.	10.09.2009 r. II SA/Wa 257/09	DOLiS/DEC-1/09/8,9	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
97.	16.09.2009 r. II SA/Wa 31/09	DOLiS/DEC- 701/08/29206,29213, 29215,29217	Skarga na decyzję w przedmiocie udostępniania danych osobowych	umorzenie postępowania w sprawie

98.	17.09.2009 r. I OSK 1049/08	GI-DEC-DOLiS- 276/07/7245,7246, 7247	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję GODO w przedmiocie przetwarzania danych osobowych	oddalenie skargi kasacyjnej
99.	18.09.2009 r. I OSK 1049/08	GI-DEC-DOLiS- 223/07/5896,5897	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję GODO w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonego wyroku
100.	23.09.2009 r. II SAB/Wa 57/09	W sprawie nie było wydanej decyzji. Zakończona została poprzez skierowanie pisma do podmiotu wnioskującego	Bezczynność w przedmiocie dostępu do informacji publicznej.	zobowiązanie GODO do rozpoznania wniosku o udostępnienie informacji publicznej
101.	02.10.2009 r. II SA/Wa 336/08	GI-DEC-DOLiS- 276/07/7245,7246, 7247	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
102.	05.10.2009 r. I OSK 1521/08	DOLiS/DEC- 1/174,178/08	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję GODO w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
103.	05.10.2009 r. II SA/Wa 1764/08	DOLiS/DEC- 664/08/27777	Skarga na decyzję w przedmiocie odmowy stwierdzenia nieważności decyzji	oddalenie skargi
104.	14.10.2009 r. II SA/Wa 359/09	DOLiS/DEC- 23/09/897,905	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie udostępniania danych osobowych	oddalenie skargi
105.	15.10.2009 r. II SA/Wa 335/08	DOLiS/DEC- 1/174,178/08	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
106.	16.10.2009 r. II SA/Wa 1428/08	GI-DEC-DOLiS- 184/07/4906,4907	Skarga w przedmiocie wznowienia postępowania w sprawie zakończonej prawomocnym wyrokiem WSA w Warszawie	oddalenie skargi
107.	22.10.2009 r. II SA/Wa 312/09	DOLiS/DEC- 16/09/635	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
108.	24.10.2009 r. I OSK 1115/08	DOLiS/DEC- 53/1776,1777,1778/ 08	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję GODO w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonego wyroku
109.	27.10.2009 r. II SA/Wa 561/09	DOLiS/DEC- 117/09/5738,5745/09	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie udostępniania danych osobowych	oddalenie skargi
110.	27.10.2009 r. II SA/Wa 1540/09	DOLiS/DEC- 205/09/9095/9096	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
111.	29.10.2009 r. I OSK 1245/08	GI-DEC-DOLiS- 264/07/6789,6790, 6791	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję GODO w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
112.	03.11.2009 r. I OSK 1670/09	DOLiS/DEC- 768/09/28679	Skarga na decyzję w przedmiocie ochrony danych osobowych	umorzenie postępowania w sprawie
113.	04.11.2009 r. II SA/Wa 330/09	GI-DEC-DOLiS- 254/07/6562,6563, 6564	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku o nakazie sprostowania danych o stanie zdrowia	zawieszenie postępowania przed WSA w Warszawie

114.	05.11.2009 r. II SA/Wa 754/09	DOLiS/DEC- 199/09/8964,8966	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję GODO w przedmiocie udostępniania danych osobowych	oddalenie skargi kasacyjnej
115.	05.11.2009 r. II SA/Wa 229/08	GI-DEC-DOLiS- 264/07/6789/6790, 6791	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
116.	19.11.2009 r. II SA/Wa 297/09	DOLiS/DEC- 914/08/36153,36156, 36157,36158,36160	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
117.	20.11.2009 r. II SA/Wa 16/09	DOLiS/DEC- 710/08/29509,29512	Skarga na decyzję w przedmiocie nakazu zaprzestania pozyskiwania danych osobowych	uchylenie zaskarżonej decyzji
118.	26.11.2009 r. II SA/Wa 1093/09	DOLiS/POST- 119/09/17216,17218, 17233	Skarga na postanowienie GODO w przedmiocie odmowy przywrócenia terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy.	uchylenie zaskarżonego postanowienia
119.	26.11.2009 r. II SA/Wa 725/09	DOLiS/DEC- 163/098406/8407/841 2/8415/8418	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
120.	27.11.2009 r. II SA/Wa 1393/09	DOLiS/DEC- 531/09/22131	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
121.	01.12.2009 r. I OSK 249/09	DIS/DEC- 254/10616/08	Zaprzestanie przetwarzania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych pracowników Spółki.	uchylenie wyroku i oddalenie skargi
122.	01. 12. 2009 r. II OSK 227/09	DIS/DEC- 421/17115/08	Przyznanie statusu administratora danych.	oddalenie skargi
123.	03.12.2009 r. II SA/Wa 357/09	DOLiS/DEC- 79/09/4073,4101, 4106	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
124.	09.12.2009 r. II SA/Wa 249/09	DOLiS/POST- 370/08/35735,35739, 35741,35747,35754,3 5756,35758	Skarga na postanowienie w przedmiocie uchybienia terminu do złożenia wniosku o ponowne rozpatrzenie sprawy.	oddalenie skargi
125.	11.12.2009 r. II SA/Wa 545/09	DOLiS/DEC- 97/09/4397,4399, 4403	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie usunięcia danych osobowych	oddalenie skargi
126.	15.12.2009 r. II SA/Wa 1582/09	DOLiS/DEC- 677/09/26243,26244/ 09	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
127.	18.12.2009 r. II SA/Wa 1602/09	DOLiS/DEC- 53/1776,1777,1778/ 08	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji

**Informacje przekazane przez organy ścigania
w sprawach skierowanych w 2009 r.
przez Generalnego Inspektora Ochrony Danych Osobowych
zawiadomień o popełnieniu przestępstwa**

Informacja	Rok 2007	Rok 2008	Rok 2009
Umorzenie dochodzenia	17	18	11
Umorzenie dochodzenia w części	-	-	-
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	5		1
Umorzenie dochodzenia i odmowa podjęcia go na nowo	-	-	2
Wszczęcie dochodzenia	-	-	3
Odmowa wszczęcia dochodzenia	5	8	3
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 2009 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	22.01.2009 r.	Warszawa	pracownicy Ministerstwa Spraw Zagranicznych wyjeżdżający na placówki zagraniczne
2.	03.02.2009 r.	Kraków	Forum Sekretarzy Samorządów Polski Południowej
3.	05.02.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
4.	12.02.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
5.	26.02.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
6.	10.03.2009 r.	Warszawa	Ministerstwo Spraw Zagranicznych
7.	13.03.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
8.	19.03.2009 r.	Warszawa	Ministerstwo Infrastruktury
9.	20.03. 2009 r.	Warszawa	Narodowy Fundusz Zdrowia
10.	27.03.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
11.	31.03.2009 r.	Warszawa	Ministerstwo Infrastruktury
12.	03.04.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
13.	21.04.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
14.	22.04.2009 r.	Częstochowa	Sąd Okręgowy w Częstochowie
15.	28.04.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
16.	05.05.2009 r.	Warszawa	Ministerstwo Infrastruktury
17.	11.05.2009 r.	Łódź	Sąd Apelacyjny w Łodzi
18.	13.05.2009 r.	Szczawnica	Sąd Okręgowy w Nowym Sączu
19.	14.05.2009 r.	Łódź	Sąd Apelacyjny w Łodzi
20.	14.05.2009 r.	Warszawa	Ministerstwo Infrastruktury
21.	20.05.2009 r.	Warszawa	Ministerstwo Spraw Zagranicznych
22.	26.05.2009 r.	Otwock	funkcjonariusze celni
23.	27.05.2009 r.	Warszawa	Ministerstwo Infrastruktury
24.	01.06.2009 r.	Kraków	Urząd Marszałkowski Województwa Małopolskiego
25.	09.06.2009 r.	Otwock	funkcjonariusze celni
26.	15.06.2009 r.	Łódź	Sąd Rejonowy dla Łodzi – Śródmieścia w Łodzi
27.	17.06.2009 r.	Warszawa	Ministerstwo Sprawiedliwości
28.	19.06.2009 r.	Warszawa	Ministerstwo Finansów
29.	22.06.2009 r.	Łódź	Sąd Rejonowy dla Łodzi – Śródmieścia w Łodzi
30.	25.06.2009 r.	Warszawa	Ministerstwo Spraw Zagranicznych
31.	26.06.2009 r.	Warszawa	Ministerstwo Finansów
32.	07.07.2009 r.	Warszawa	Narodowy Fundusz Zdrowia

33.	14.07.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
34.	21.07.2009 r.	Warszawa	Narodowy Fundusz Zdrowia
35.	08.09.2009 r.	Warszawa	Urząd m. st. Warszawy
36.	14.09.2009 r.	Toruń	Związek Rewizyjny Spółdzielni Mieszkaniowych z siedzibą w Toruniu
37.	18.09.2009 r.	Warszawa	Urząd m. st. Warszawy
38.	22.09.2009 r.	Warszawa	funkcjonariusze celni
39.	29.09.2009 r.	Warszawa	Kancelaria Sejmu
40.	05.10.2009 r.	Warszawa	Urząd m. st. Warszawy
41.	20.10.2009 r.	Warszawa	funkcjonariusze celni
42.	28.10.2009 r.	Warszawa	Ministerstwo Spraw Zagranicznych
43.	04.11.2009 r.	Warszawa	Urząd Komisji Nadzoru Finansowego
44.	05.11.2009 r.	Warszawa	Komenda Stołeczna Policji
45.	13.11.2009 r.	Warszawa	Kancelaria Senatu
46.	17.11.2009 r.	Warszawa	Ministerstwo Spraw Wewnętrznych i Administracji (administracja gruzińska)
47.	17.10.2009 r.	Rynia	Krajowe Stowarzyszenie Ochrony Informacji Niejawnych
48.	23.11.2009 r.	Warszawa	Kancelaria Sejmu
49.	22-24.11.2009 r.	Warszawa	samorządowe ośrodki doskonalenia zawodowego nauczycieli (Gliwice i Kielce)
50.	27.11.2009 r.	Warszawa	Kancelaria Sejmu
51.	01.12.2009 r.	Warszawa	funkcjonariusze celni
52.	03.12.2009 r.	Warszawa	Urząd m. st. Warszawy
53.	08.12.2009 r.	Warszawa	Ministerstwo Spraw Zagranicznych
54.	08.12.2009 r.	Warszawa	Kancelaria Sejmu
55.	10.12.2009 r.	Warszawa	Urząd m. st. Warszawy
56.	14.12.2009 r.	Warszawa	Kancelaria Prezesa Rady Ministrów

**Wykaz decyzji Generalnego Inspektora Ochrony Danych Osobowych
wydanych w 2009 roku w sprawach o wyrażenie zgody
na przekazanie danych osobowych za granicę**

l.p.	Data wydania decyzji/ postanowienia	Nazwa podmiotu	Sygnatura decyzji/ postanowienia
1.	05.01.2009	UPS Polska Sp. z o.o.	DESiWM/DEC-2/122/09 zgoda na przekazanie danych osobowych
2.	05.01.2009	UPS SCS Polska Sp. z o.o.	DESiWM/DEC-3/123/09 zgoda na przekazanie danych osobowych
3.	10.02.2009	Samsung Electronics Polska Sp. z o.o.	DESiWM/DEC-85/4216/09 zgoda na przekazanie danych osobowych
4.	23.02.2009	Clifford Chance, Janicka, Namiotkiewicz, Dębowski i Wspólnicy Sp. K.	DESiWM/DEC-133/6101/09 zgoda na przekazanie danych osobowych
5.	09.03.2009	Sun Microsystems Poland Sp. z o.o.	DESiWM/DEC-270/11420/09 umorzenie postępowania (odbiorca należy do amerykańskiego programu „bezpiecznej przystani”)
6.	31.03.2009	Bristol-Myers Squibb Polska Sp. z o.o.	DESiWM/DEC-268/11399/09 zgoda na przekazanie danych osobowych
7.	31.03.2009	Bristol-Myers Squibb Services Sp. z o.o.	DESiWM/DEC-269/11402/09 zgoda na przekazanie danych osobowych
8.	10.04.2009	Hewitt Associates Sp. z o.o.	DESiWM/DEC-297/12981/09 zgoda na przekazanie danych osobowych
9.	27.04.2009	Kraton Polymers US LLC	DESiWM/DEC-333/15006/09 umorzenie postępowania (wycofanie wniosku)
10.	07.05.2009	Mio Technology UK Ltd. Sp. z o.o. Oddział w Polsce	DESiWM/DEC-364/16479/09 DESiWM/DEC-364/16480/09 zgoda na przekazanie danych osobowych (jedna decyzja, dwa numery)
11.	20.05.2009	C.H. Robinson Poland Sp. z o.o.	DESiWM/DEC-406/18293/09 zgoda na przekazanie danych osobowych
12.	26.05.2009	Aon Affinity Polska Sp. z o.o.	DESiWM/DEC-440/19191/09 zgoda na przekazanie danych osobowych
13.	26.05.2009	Aon Polska Sp. z o.o.	DESiWM/DEC-441/19192/09 zgoda na przekazanie danych osobowych
14.	02.06.2009	Otis Sp. z o.o.	DESiWM/DEC-486/20151/09 zgoda na przekazanie danych osobowych
15.	02.06.2009	Polskie Zakłady Lotnicze Sp. z o.o.	DESiWM/DEC-485/20147/09 zgoda na przekazanie danych osobowych
16.	02.06.2009	Wytwórnia Sprzętu Komunikacyjnego „PZL-Rzeszów” S.A.	DESiWM/DEC-484/20145/09 zgoda na przekazanie danych osobowych
17.	02.06.2009	Pratt & Whitney Kalisz Sp. z o.o.	DESiWM/DEC-483/20143/09 zgoda na przekazanie danych osobowych
18.	02.06.2009	Carrier Polska Sp. z o.o.	DESiWM/DEC-482/20182/09 zgoda na przekazanie danych osobowych
19.	02.06.2009	Carrier Rental Systems Polska Sp. z o.o.	DESiWM/DEC-481/20184/09 zgoda na przekazanie danych osobowych
20.	02.06.2009	Carrier Transicold Polska Sp. z o.o.	DESiWM/DEC-480/20193/09 zgoda na przekazanie danych osobowych

21.	03.06.2009	RGA International Reinsurance Company Limited Sp. z o.o.	DESIWM/DEC-495/20299/09 zgoda na przekazanie danych osobowych
22.	09.06.2009	Carrier Transicold Polska Sp. z o.o.	DESIWM/DEC-512/21046/09 zgoda na przekazanie danych osobowych
23.	09.06.2009	Carrier Rental Systems Polska Sp. z o.o.	DESIWM/DEC-511/21047/09 zgoda na przekazanie danych osobowych
24.	09.06.2009	Carrier Polska Sp. z o.o.	DESIWM/DEC-510/21049/09 zgoda na przekazanie danych osobowych
25.	09.06.2009	Otis Sp. z o.o.	DESIWM/DEC-509/21019/09 zgoda na przekazanie danych osobowych
26.	09.06.2009	Polskie Zakłady Lotnicze Sp. z o.o.	DESIWM/DEC-508/21018/09 zgoda na przekazanie danych osobowych
27.	09.06.2009	Wytwórnia Sprzętu Komunikacyjnego „PZL-Rzeszów” S.A.	DESIWM/DEC-507/21017/09 zgoda na przekazanie danych osobowych
28.	09.06.2009	Pratt & Whitney Kalisz Sp. z o.o.	DESIWM/DEC-506/21016/09 zgoda na przekazanie danych osobowych
29.	16.06.2009	Flextronics Logistics Poland Sp. z o.o.	DESIWM/DEC-525/21822/09 zgoda na przekazanie danych osobowych
30.	08.09.2009	Linde Gaz Polska Sp. z o.o.	DESIWM/DEC-888/32602/09 zgoda na przekazanie danych osobowych
31.	08.09.2009	Linde Gaz Polska Sp. z o.o.	DESIWM/DEC-889/32607/09 zgoda na przekazanie danych osobowych
32.	08.09.2009	JOBS.PL S.A.	DESIWM/DEC-887/32565/09 umorzenie postępowania (rezygnacja wnioskodawcy)
33.	28.09.2009	McCain Poland Sp. z o.o.	DESIWM/DEC-976/35238/09 zgoda na przekazanie danych osobowych; umorzenie postępowania w zakresie przekazania danych do Kanady
34.	12.10.2009	Carrier Rental Systems Polska Sp. z o.o.	DESIWM/DEC-1003/37104/09 zgoda na przekazanie danych osobowych
35.	12.10.2009	Wytwórnia Sprzętu Komunikacyjnego „PZL-Rzeszów” S.A.	DESIWM/DEC-1004/37114/09 zgoda na przekazanie danych
36.	12.10.2009	Carrier Polska Sp. z o.o.	DESIWM/DEC-1009/37078/09 zgoda na przekazanie danych
37.	12.10.2009	Carrier Transicold Polska Sp. z o.o.	DESIWM/DEC-1008/37080/09 zgoda na przekazanie danych osobowych
38.	12.10.2009	Otis Sp. z o.o.	DESIWM/DEC-1007/37084/09 zgoda na przekazanie danych osobowych
39.	12.10.2009	Polskie Zakłady Lotnicze Sp. z o.o.	DESIWM/DEC-1006/37086/09 zgoda na przekazanie danych
40.	12.10.2009	Pratt & Whitney Kalisz Sp. z o.o.	DESIWM/DEC-1005/37090/09 zgoda na przekazanie danych osobowych
41.	16.11.2009	LexisNexis Polska Sp. z o.o.	DESIWM/DEC-1146/42078/09 zgoda na przekazanie danych osobowych; umorzenie postępowania w zakresie przekazania danych do Kanady
42.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1197/44453/09 zgoda na przekazanie danych osobowych
43.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1196/44460/09 zgoda na przekazanie danych osobowych
44.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1195/44464/09 zgoda na przekazanie danych osobowych
45.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1194/44469/09 zgoda na przekazanie danych osobowych
46.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1193/44474/09 zgoda na przekazanie danych osobowych
47.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1192/44476/09 zgoda na przekazanie danych osobowych

48.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1191/44477/09 zgoda na przekazanie danych osobowych
49.	30.11.2009	Unilever Polska S.A.	DESIWM/DEC-1190/44478/09 zgoda na przekazanie danych osobowych
50.	04.12.2009	Reader's Digest Przegląd Sp. z o.o.	DESIWM/DEC-1219/45176/09 zgoda na przekazanie danych osobowych; postępowanie częściowo umorzone (rezygnacja wnioskodawcy z części wniosku)
51.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1218/45177/09 zgoda na przekazanie danych osobowych
52.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1217/45178/09 zgoda na przekazanie danych osobowych
53.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1216/45179/09 zgoda na przekazanie danych osobowych
54.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1215/45182/09 zgoda na przekazanie danych osobowych
55.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1214/45184/09 zgoda na przekazanie danych osobowych
56.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1213/45186/09 zgoda na przekazanie danych osobowych
57.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1212/45188/09 zgoda na przekazanie danych osobowych
58.	04.12.2009	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-1211/45189/09 zgoda na przekazanie danych osobowych
59.	10.12.2009	Loyalty Partner Polska Sp. z o.o.	DESIWM/DEC-1248/46344/09 zgoda na przekazanie danych osobowych
60.	22.12.2009	AT&T Global Network Services Polska Sp. z o.o.	DESIWM/DEC-1291/47885/09 zgoda na przekazanie danych osobowych; umorzenie postępowania w zakresie przekazania danych do Kanady
61.	22.12.2009	Siemens Sp. z o.o.	DESIWM/DEC-1292/48027/09 zgoda na przekazanie danych osobowych
62.	28.12.2009	Eurogaz-Gdynia Sp. z o.o.	DESIWM/DEC-1325/48358/09 zgoda na przekazanie danych osobowych
63.	28.12.2009	Eurogaz-Gdynia Sp. z o.o.	DESIWM/DEC-1326/48363/09 zgoda na przekazanie danych osobowych