

**Generalny Inspektor  
Ochrony Danych Osobowych**

**SPRAWOZDANIE  
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA  
OCHRONY DANYCH OSOBOWYCH  
W ROKU 2010**

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<sup>1</sup>.

---

<sup>1</sup> Niniejsze *Sprawozdanie* obejmuje okres działalności Generalnego Inspektora Ochrony Danych Osobowych od 1 stycznia 2010 r. do 31 grudnia 2010 r.

# SPIS TREŚCI

<b>Wprowadzenie .....</b>	<b>5</b>
<b>Część I. Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych .....</b>	<b>5</b>
<b>1. Informacje ogólne .....</b>	<b>5</b>
<b>2. Biuro Generalnego Inspektora Ochrony Danych Osobowych .....</b>	<b>7</b>
2.1. Struktura organizacyjna .....	7
2.2. Pracownicy Biura GIODO .....	7
2.3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2010 rok .....	8
<b>Część II. Stan wiedzy i przestrzegania przepisów o ochronie danych osobowych .....</b>	<b>9</b>
1. Informacje ogólne .....	9
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 .....	12
1) Administracja publiczna .....	12
2) Banki i inne instytucje finansowe .....	13
3) Internet .....	14
4) Oświata i szkolnictwo wyższe .....	15
5) Służba zdrowia .....	17
6) Ubezpieczenia społeczne, majątkowe i osobowe .....	19
7) Telekomunikacja .....	21
8) Zatrudnienie .....	23
9) Komunalne jednostki organizacyjne .....	24
10) Inne .....	26
2.3. Systemy informatyczne służące do przetwarzania danych osobowych .....	29
2.4. Wyniki kontroli w zakresie wypełnienia obowiązków formalnych i organizacyjnych .....	30
2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych .....	33
2.5.1. Ocena poziomu bezpieczeństwa .....	35
2.5.2. Outsourcing i kolokacja danych .....	36
2.5.3. Systemy sieciowe i wielostanowiskowe .....	38

3.	Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych .....	39
3.1.	Wydawanie decyzji .....	39
3.2.	Zawiadomienia o podejrzeniu popełnienia przestępstwa .....	40
3.3.	Rozpatrywanie skarg .....	42
4.	Prowadzenie rejestru zbiorów danych osobowych oraz udzielanie informacji o zarejestrowanych zbiorach .....	48
5.	Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych .....	59
6.	Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych .....	75
6.1.	Interpretacja przepisów .....	77
6.1.1.	Przetwarzanie danych osobowych za pośrednictwem sieci Internet .....	77
6.1.2.	Przetwarzanie danych osobowych z zastosowaniem systemów informatycznych oraz monitoringu .....	84
6.1.3.	Inne .....	87
6.2.	Działalność informacyjna .....	93
6.2.1.	Współpraca ze środkami masowego przekazu .....	94
6.2.2.	Publikacje .....	97
6.2.3.	Szkolenia .....	98
6.2.4.	Konkursy .....	99
6.2.5.	Projekty i programy .....	99
6.2.6.	Konferencje, seminaria, spotkania .....	103
6.2.7.	Internet .....	109
6.2.8.	Inne informacje .....	109
7.	Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych .....	111
7.1.	Międzynarodowe spotkania i konferencje .....	115
7.2.	Wizyty robocze .....	118
7.3.	Warsztaty Rozpatrywania Spraw .....	118
7.4.	Warsztaty TAIEX .....	119
<b>Część III.</b>	<b>Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2010 roku .....</b>	<b>119</b>
<b>Część IV.</b>	<b>Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych .....</b>	<b>135</b>

## **Załączniki**

<b>Załącznik nr 1</b>	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2010 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego.....	141
<b>Załącznik nr 2</b>	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2010 do podmiotów prywatnych .....	146
<b>Załącznik nr 3</b>	Wykaz kontroli przeprowadzonych w 2010 roku .....	149
<b>Załącznik nr 4</b>	Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2010 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych .....	158
<b>Załącznik nr 5</b>	Informacje przekazane przez organy ścigania w sprawach skierowanych w 2010 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa .....	164
<b>Załącznik nr 6</b>	Wykaz szkoleń przeprowadzonych przez GIODO w 2010 r. ....	165
<b>Załącznik nr 7</b>	Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych wydanych w 2010 roku w sprawach o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego .....	167

# **SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2010**

## **Wprowadzenie**

Rok 2010 był dwunastym rokiem obowiązywania ustawy o ochronie danych osobowych. Był to jednocześnie rok istotnych zmian w podstawach prawnych działania Generalnego Inspektora Ochrony Danych Osobowych (GIODO) przede wszystkim związanych z zakończeniem prac nad prezydenckim projektem nowelizacji ustawy o ochronie danych osobowych. W dniu 29 października 2010 r. Sejm RP ostatecznie przyjął poprawki do projektu zgłoszone przez Senat. Datą wejścia w życie zmian był 7 marca 2011 r. Omówiona w dalszej części Sprawozdania nowelizacja uzupełniła uprawnienia GIODO o zadania z zakresu egzekucji administracyjnej. Dokonano również zmiany na stanowisku Generalnego Inspektora Ochrony Danych Osobowych. W dniu 25 czerwca 2010 r. Sejm Rzeczypospolitej Polskiej powołał do pełnienia tej funkcji dra Wojciecha Rafała Wiewiórowskiego. Po zatwierdzeniu tego wyboru przez Senat i złożeniu ślubowania z dniem 4 sierpnia 2010 r. dr Wojciech Rafał Wiewiórowski objął obowiązki Generalnego Inspektora rozpoczynając swoją czteroletnią kadencję.

## **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 (t.j.: 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 załącznikiem zawierającym opis środków bezpieczeństwa na poziomie podstawowym, podwyższonym i wysokim (Dz. U. Nr 100, poz. 1024), wydane na podstawie art. 39a ustawy. Rozporządzenie określa:

- sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
  - podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
  - wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.
- b) 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 Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006 r. Nr 203, poz. 1494).

Ustawą z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. Nr 229, poz. 1497) wprowadzone zostały zmiany w przepisach dotychczas obowiązującej ustawy. Wejdą one w życie z dniem 7 marca 2011 r. Nowelizacja ustawy była również częścią procesu implementacji unijnej 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 281 z 23 listopada 1995 r. s. 31 z późn. zm.). Szczegóły nowelizacji przedstawione zostaną w dalszej części niniejszego Sprawozdania.

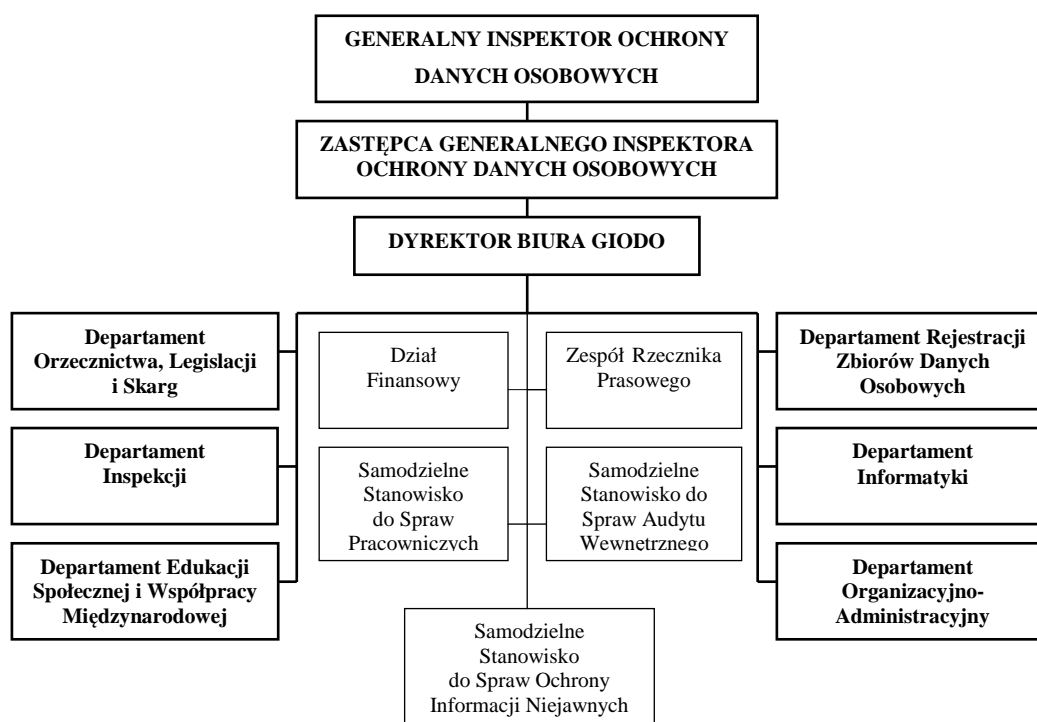
Na system ochrony danych osobowych składają się też przepisy szczególne innych ustaw, które regulują kwestie związane z przetwarzaniem danych osobowych przez różne podmioty. Organy władzy publicznej i obsługujące je urzędy, w myśl zasady praworządności wyrażonej w art. 7 Konstytucji Rzeczypospolitej 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. Również wolność przetwarzania informacji gwarantowana osobom fizycznym i podmiotom innym niż organy publiczne przez art. 54 ust. 1 Konstytucji RP, znajduje pewne ograniczenia w przepisach szczególnych chroniących prywatność osób fizycznych.

## 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<sup>2</sup>.

### 2.2. Pracownicy Biura GIODO

Stan zatrudnienia w Biurze GIODO w przeliczeniu na pełne etaty wynosił na dzień 1 stycznia 2010 r. – 120 etatów, zaś na dzień 31 grudnia 2010 r. – 127 etatów. Na stanowiskach merytorycznych

<sup>2</sup> 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.

zatrudnionych było 112 osób, a na stanowiskach pomocniczych 18 osób. Wyższe wykształcenie posiadało 115 pracowników, w tym 79 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GIODO na koniec 2010 r. przedstawia się następująco:

- GIODO - 1 osoba
- Zastępca 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) – 14 osób,
- Departament Inspekcji (DIS) – 17 osób,
- Departament Orzecznictwa, Legislacji i Skarg (DOLiS) – 35 osób,
- Departament Rejestracji Zbiorów Danych Osobowych (DRZDO) – 18 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 2010 rok**

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2010 r. wynosił: **13 842** tys. zł, w tym:

wynagrodzenia	9 305 tys. zł
pochodne od wynagrodzeń	1 451 tys. zł
wydatki majątkowe	81 tys. zł
pozostałe wydatki	3 005 tys. zł

Wydatki zrealizowane przez GIODO w 2010 roku w kwocie **13 720** tys. zł obejmowały:

wynagrodzenia	9 260 tys. zł
pochodne od wynagrodzeń	1 404 tys. zł
wydatki majątkowe	81 tys. zł
pozostałe wydatki	2 975 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 operacjach, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zdefiniowanych jako wszelkie informacje dotyczące osoby fizycznej, pozwalające bez większego wysiłku na określenie tożsamości tej osoby. Danymi osobowymi nie będą jednak pojedyncze informacje o dużym stopniu ogólności. Staną się nimi dopiero z chwilą zestawienia ich z innymi, dodatkowymi informacjami, które w konsekwencji pozwolą na odniesienie ich do konkretnej osoby.

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

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 26 ust. 1 ustawy, ujmując je w formę podstawowych obowiązków administratora danych<sup>3</sup>. Z jego treści wynika, że administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie, ma on przestrzegać wskazanych poniżej zasad:

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

Jako obywatele mamy możliwość skorzystania z przysługującego nam prawa do formalnej kontroli przetwarzania dotyczących nas danych, które ustanowione jest w rozdziale 4 ustawy. Możemy domagać się również: uzyskania informacji, czy zbiór danych istnieje, ustalenia administratora danych,

---

<sup>3</sup> 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.

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 dotyczących ich danych osobowych oraz ustanawia instrumenty umożliwiające realizację tego prawa.

Nad przestrzeganiem prawa jednostek do ochrony ich danych osobowych czuwa niezależny organ – Generalny Inspektor Ochrony Danych Osobowych. Postępowanie w sprawach uregulowanych w ustawie o ochronie danych osobowych prowadzi się 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, 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 w charakterze świadka oraz protokołów oględzin miejsca, pomieszczeń, dokumentów, urządzeń, nośników, systemów informatycznych służących do przetwarzania danych osobowych. Na podstawie ustaleń zawartych w ww. protokołach, analizy dokumentów przedłożonych w toku kontroli (stanowiących w szczególności uchwały i zarządzenia organów reprezentujących jednostkę kontrolowaną, regulaminy, instrukcje i procedury określające zasady przetwarzania danych osobowych, zawarte umowy, w tym umowy powierzenia przetwarzania danych osobowych oraz opracowane formularze i kwestionariusze) 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, wszczynane jest postępowanie administracyjne lub kierowane jest do jednostki kontrolowanej pismo z informacją, że w zakresie objętym kontrolą nie stwierdzono uchybień. Ponadto, w przypadku stwierdzenia, że działanie lub zaniechanie kierownika jednostki kontrolowanej lub jej pracownika wyczerpuje znamiona przestępstwa określonego w ustawie o ochronie danych osobowych, do organu powołanego do ścigania przestępstw kierowane jest zawiadomienie o popełnieniu przestępstwa. Ustalenia kontrolne mogą także uzasadnić żądanie

wszczęcia przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień, np. postępowania dyscyplinarnego.

## **2.2. Kontrola przetwarzania danych osobowych w wybranych obszarach**

W 2010 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził łącznie **196 kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych.

### **1) Administracja publiczna**

W 2010 r. w ramach kontroli podmiotów sektora administracji publicznej, przeprowadzono **10 kontroli w urzędach kontroli skarbowej**<sup>4</sup>. Zakresem kontroli objęto zabezpieczenie danych osobowych przetwarzanych przez dyrektorów urzędów kontroli skarbowej.

Do najczęściej stwierdzanych w toku kontroli nieprawidłowości, należały uchybienia w zakresie niedostosowania systemów informatycznych wykorzystywanych do przetwarzania danych osobowych do wymogów rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W szczególności systemy te nie zapewniały dla każdej osoby, której dane osobowe były przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Liczne nieprawidłowości stwierdzono także w zakresie prowadzonej przez administratorów danych dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Uchybieniem było przede wszystkim niezawarcie w niej wszystkich elementów określonych w § 4 i § 5 wspomnianego rozporządzenia, tj. określających politykę bezpieczeństwa i instrukcję jej prowadzenia (np. brak było opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi). W pojedynczych przypadkach przeprowadzone kontrole wykazały, że administratorzy danych nie zastosowali odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w związku z brakiem rejestru pobranych i zdanych kluczy do pomieszczeń, w których przetwarzane są dane osobowe oraz rejestru wynoszonej poza obszar przetwarzania danych dokumentacji zawierającej dane osobowe. W jednym przypadku stwierdzono, że prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych nie spełniała wymagań określonych w art. 39 ust. 1 ustawy

---

<sup>4</sup> Np. kontrole DIS-K-421/97/10, DIS-K-421/103/10, DIS-K-421/122/10, DIS-K-421/125/10.

o ochronie danych osobowych<sup>5</sup>, tj. nie zawiera informacji o identyfikatorach użytkowników przetwarzających dane osobowe w systemach informatycznych.

W związku ze stwierdzonymi uchybieniami, wobec dyrektorów urzędów kontroli skarbowej wszczęte zostały postępowania administracyjne i wydane zostały decyzje nakazujące usunięcie uchybień<sup>6</sup>. W decyzjach tych Generalny Inspektor nakazał m.in. zapewnienie, aby system informatyczny służący do przetwarzania danych osobowych zapewniał dla każdej osoby, której dane osobowe były w tym systemie przetwarzane, odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Na podstawie ustaleń dokonanych w toku kontroli tych podmiotów, Generalny Inspektor skierował pismo do Ministra Finansów informujące o nieprawidłowościach dotyczących systemu informatycznego służącego do przetwarzania danych osób, które były poddawane kontroli podatkowej<sup>7</sup>. W odpowiedzi na ww. pismo Generalny Inspektor Kontroli Skarbowej wskazał, że system informatyczny został dostosowany do wymogów określonych w przepisach o ochronie danych osobowych. Do wszystkich urzędów kontroli skarbowej przekazano nową wersję systemu, która zapewnia automatyczne odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego te dane<sup>8</sup>. Podkreślić należy, że reakcja Ministra Finansów na wskazane nieprawidłowości była niezwłoczna i umożliwiła przywrócenie stanu zgodnego z prawem we wszystkich urzędach kontroli skarbowej znacznie przed upływem terminu wskazanego przez GODO w decyzjach nakazujących usunięcie uchybień.

## **2) Banki i inne instytucje finansowe**

W 2010 r. przeprowadzono **18 kontroli** zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w firmach inwestycyjnych prowadzących działalność maklerską<sup>9</sup>, w tym 16 kontroli przeprowadzono w ramach kontroli sektorowej<sup>10</sup>. Zakresem kontroli objęto zabezpieczenie danych osobowych. W toku 8 kontroli nie stwierdzono uchybień w procesie przetwarzania danych osobowych w zakresie objętym kontrolą.

Większość z przeprowadzonych kontroli wykazała nieprawidłowości w zakresie prowadzonej przez administratorów danych dokumentacji, opisującej sposób przetwarzania danych osobowych oraz

---

<sup>5</sup> 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.

<sup>6</sup> Np. decyzje DIS/DEC-1330/47863/10, DIS/DEC-1323/47590/10, DIS/DEC-1321/47592/10.

<sup>7</sup> Pismo z dnia 11 października 2010 r.

<sup>8</sup> Pisma z dnia 9 listopada 2010 r. KS3/0680/169/ROB/10/7411 oraz z dnia 7 grudnia 2010 r. KS2/066/123/BQS/10/ 7885.

<sup>9</sup> Art. 3 pkt 33 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowym, stanowi, że przez firmę inwestycyjną rozumie się dom maklerski, bank prowadzący działalność maklerską, zagraniczną firmę inwestycyjną prowadzącą działalność maklerską na terytorium Rzeczypospolitej Polskiej oraz zagraniczną osobę prawną z siedzibą na terytorium państwa należącego do OECD lub WTO, prowadzącą działalność maklerską na terytorium Rzeczypospolitej Polskiej. Dz. U. Nr 183, poz. 1538 z późn. zm.

środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Uchybienia te polegały m.in. na nieuwzględnianiu w opracowanych politykach bezpieczeństwa, takich elementów jak wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. W jednym przypadku stwierdzono także uchybienia w odniesieniu do instrukcji zarządzania systemem informatycznym, które polegały na niezawarcu w dokumentacji prowadzonej przez administratora danych m.in. procedur nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz niewskazanie osoby odpowiedzialnej za te czynności i stosowanych metod i środków uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem.

Do częstych uchybień stwierdzanych w toku kontroli firm inwestycyjnych prowadzących działalność maklerską należało także niezapewnianie przez administratora danych kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu były przekazywane. Uchybienia w ww. zakresie polegały w szczególności na nieodnotowywaniu faktu przekazywania dokumentacji zawierającej dane osobowe pomiędzy poszczególnymi jednostkami organizacyjnymi oraz na niezapewnieniu, aby dla każdej osoby, której dane osobowe były przetwarzane w systemie informatycznym, system ten zapewniał odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu. W pojedynczych przypadkach kontrole wykazały uchybienia polegające na niezastosowaniu środków kryptograficznych dla ochrony danych osobowych przesyłanych w sieci publicznej oraz niezawarcu w ewidencji osób upoważnionych do przetwarzania danych osobowych identyfikatora użytkownika w systemie informatycznym, w którym odbywa się przetwarzanie danych osobowych.

W wydanych decyzjach Generalny Inspektor Ochrony Danych Osobowych nakazał usunięcie ww. uchybień w procesie przetwarzania danych osobowych.

### **3) Internet**

Do najważniejszych kontroli przeprowadzonych w 2010 r. w sektorze komunikacji elektronicznej poprzez sieć Internet należy zaliczyć kontrolę przedsiębiorcy<sup>11</sup>, który w ramach prowadzonego portalu umożliwiał użytkownikom m.in. wyszukiwanie osób pełniących określone funkcje w podmiotach, które podlegają obowiązkowemu wpisowi do Krajowego Rejestru Sądowego. Do świadczenia przez przedsiębiorcę usług dostępnych we ww. portalu, wykorzystywane były dane

---

<sup>10</sup> Np. kontrole DIS-K-421/23/10, DIS-K-421/28/10, DIS-K-421/49/10 i DIS-K-421/77/10.

<sup>11</sup> DIS-K-421/105/10

pozyskane przez niego z Krajowego Rejestru Sądowego. Zasady współpracy pomiędzy ww. podmiotami uregulowane zostały w umowie o współpracy, w której w szczególności określono zakres danych, który może być udostępniany na portalu, środki techniczne i organizacyjne, jakie zobowiązany był zastosować właściciel portalu w związku z udostępnieniem danych oraz sposób postępowania w przypadku wystąpienia osoby, której dotyczą dane, z roszczeniem przeciwko właścicielowi portalu lub podmiotowi, który mu dane przekazał. Na podstawie zawartej umowy o współpracy właściciel portalu został zobowiązany do trwałego usunięcia przekazanych mu danych po zakończeniu współpracy z podmiotem, który przekazywał mu dane w celu ich publikowania na portalu. Ustalenia kontroli potwierdziły, że właściciel portalu przetwarza przekazane dane wyłącznie w granicach upoważnienia udzielonego mu w powołanej umowie o współpracy, tj. wyłącznie w celu ich udostępnienia (publikacji) użytkownikom portalu. W związku z dokonanymi w toku kontroli ustaleniami, rozstrzygnięcia w szczególności wymagała kwestia, który z ww. podmiotów jest administratorem danych przetwarzanych w ramach prowadzonego portalu. Po dokonaniu szczegółowej analizy umowy zawartej pomiędzy tymi podmiotami oraz po zbadaniu, który z tych podmiotów decyduje o celach i środkach przetwarzania danych osobowych, Generalny Inspektor uznał, że administratorem danych był podmiot, który przekazał dane przedsiębiorcy prowadzącemu portal internetowy, a jednostka kontrolowana podmiotem, któremu administrator danych powierzył ich przetwarzanie.

#### **4) Oświata i szkolnictwo wyższe**

W 2010 r. przeprowadzonych zostało w szkołach wyższych **31 kontroli** zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w tym 26 kontroli sektorowych<sup>12</sup>. Zakresem kontroli objęto zabezpieczenie danych osobowych przetwarzanych przez szkoły wyższe.

W oparciu o wyniki kontroli można stwierdzić, że szkoły wyższe najwięcej problemów miały z prawidłowym wykonaniem obowiązków związanych z przetwarzaniem danych osobowych przy użyciu systemów informatycznych. Do najczęściej spotykanych w tym zakresie naruszeń należało niezapewnianie przez systemy informatyczne służące do przetwarzania danych osobowych dla każdej osoby, której dane osobowe były przetwarzane w systemie informatycznym, odnotowania informacji o dacie pierwszego wprowadzenia danych do systemu i identyfikatorze użytkownika wprowadzającego te dane oraz sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 powołanego rozporządzenia<sup>13</sup>. Do częstych uchybień należało

---

<sup>12</sup> DIS-K-421/1/10, DIS-K-421/4/10, DIS-K-421/5/10, DIS-K-421/17/10, DIS-K-421/19/10, DIS-K-421/24/10, DIS-K-421/31/10, DIS-K-421/44/10, DIS-K-421/65/10, DIS-K-421/89/10.

<sup>13</sup> § 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

także ustawienie monitora komputera, na którym były przetwarzane dane osobowe, w sposób umożliwiający wgląd w te dane osobom nieupoważnionym oraz przesyłanie danych osobowych studentów za pośrednictwem poczty elektronicznej w formie niezaszyfrowanej i w postaci plików niezabezpieczonych hasłem, stosowanie haseł o mniejszej niż wymagana liczba znaków oraz ich zmienianie rzadziej niż co 30 dni. Krytycznie należy również ocenić zastosowane środki techniczne i organizacyjne w celu zabezpieczenia dokumentacji zawierającej dane osobowe. Stwierdzone w tym zakresie uchybienia polegały na przechowywaniu tej dokumentacji w szafach niewyposażonych w zamki lub na otwartym regale oraz na nieopracowaniu procedury dotyczącej przechowywania dokumentacji o charakterze archiwalnym i procedury regulującej sposób postępowania z kluczami do pomieszczeń, w których były przetwarzane dane osobowe.

Poddane kontroli szkoły wyższe miały problemy także z właściwym prowadzeniem dokumentacji dotyczącej przetwarzania danych osobowych. Część przeprowadzonych kontroli wykazała bowiem, że jednostki kontrolowane nie opracowały dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych lub nie zawierały w polityce bezpieczeństwa wszystkich elementów wskazanych w § 4 cytowanego rozporządzenia (m.in. informacji o wszystkich systemach informatycznych użytkowanych przez administratora danych; wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; opisu struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami). Ponadto w niektórych szkołach wyższych nie został wyznaczony administrator bezpieczeństwa informacji nadzorujący proces przetwarzania danych osobowych lub do przetwarzania danych osobowych dopuszczone zostały osoby, którym administrator danych nie nadał upoważnień. Odnotowano też przypadki, gdzie nie została opracowana ewidencja 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 (m.in. daty nadania i ustania upoważnienia). 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<sup>14</sup>.

---

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.

<sup>14</sup> Np. decyzje: DIS/DEC-653/21892/10, DIS/DEC-585/20169/10, DIS/DEC-703/23707/10, DIS/DEC-706/23841/10.



Kolejnym zagadnieniem badanym w toku kontroli przeprowadzonych w szkołach wyższych, było przetwarzanie danych osobowych studentów w związku z wydanymi im elektronicznymi legitymacjami studenckimi. Kontrole wykazały, że elektroniczne legitymacje studenckie posiadają dwa odseparowane fizycznie układy elektroniczne, tj. układ bezstykowy i układ stykowy. Układ bezstykowy wykorzystywany był przez przewoźnika do kodowania biletów komunikacji miejskiej na ww. legitymacjach. Natomiast układ stykowy wykorzystywany był przez uczelnie w celu zapisania danych osobowych studenta. Jak ustalono, przewoźnik nie posiadał dostępu do danych zapisanych w układzie stykowym. Współpraca pomiędzy szkołami wyższymi a przewoźnikiem w ww. zakresie odbywała się na podstawie zawartych porozumień, które określały m.in. zabezpieczenia danych przetwarzanych na elektronicznych legitymacjach studenckich.

Ponadto w wyniku jednej kontroli<sup>15</sup> skierowano wystąpienie do Ministra Edukacji Narodowej o podjęcie działań mających na celu zapewnienie, aby placówki oświatowe wskazane w rozporządzeniu Ministra Edukacji Narodowej z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. Nr 23, poz. 225 z późn. zm.), które korzystają z dzienników prowadzonych przy użyciu systemu informatycznego (tzw. e-dzienniki), prowadziły te dzienniki zgodnie z przepisami o ochronie danych osobowych<sup>16</sup>. W toku kontroli ustalono, iż placówki oświatowe powierzają dane osobowe uczniów, ich przedstawicieli ustawowych i nauczycieli podmiotowi oferującemu system informatyczny, który umożliwia prowadzenie dzienników w formie elektronicznej. Generalny Inspektor zwrócił uwagę Ministrowi Edukacji Narodowej na to, iż żadna ze wskazanych placówek, jako administrator danych ww. osób, nie zawarła z tym podmiotem umowy w formie pisemnej, o której mowa w art. 31 ustawy o ochronie danych osobowych, oraz że placówki te nie dokładają szczególnej staranności w zakresie upewnienia się, czy podmiot, któremu powierzają dane, przetwarza je zgodnie z wymogami określonymi w przepisach o ochronie danych osobowych.

## **5) Służba zdrowia**

W okresie sprawozdawczym skontrolowano podmiot prowadzący Krajowy Rejestr Nowotworów<sup>17</sup>. Do zadań tej placówki należało gromadzenie, przetwarzanie i analiza danych dotyczących zachorowań i zgonów z powodu nowotworów złośliwych na terenie Polski. Do Krajowego Rejestru Nowotworów raz w roku z wojewódzkich rejestrów nowotworów przesyłane są drogą elektroniczną dane o zachorowaniach na nowotwory złośliwe w poprzednim roku. Zasady przekazywania danych do ww. rejestrów nowotworów nie zostały jednak ujęte w regulacjach rangi

---

<sup>15</sup> DIS-K-421/56/10

<sup>16</sup> Pismo z dnia 23 lipca 2010 r. DIS-K-421/56/10/25558/10.

ustawowej, jak tego wymaga art. 27 ustawy o ochronie danych osobowych. Analiza stanu prawnego wykazała, iż stosownie do art. 18 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. Nr 88, poz. 439 z późn. zm.) w drodze rozporządzeń ustalane są przez Radę Ministrów, programy badań statystycznych statystyki publicznej. Każdego roku wydawane jest rozporządzenie zawierające program badań statystycznych statystyki publicznej na dany rok. Na przykład program badań na 2010 r. został określony w załączniku do Rozporządzenia Rady Ministrów z dnia 8 grudnia 2009 r. w sprawie programu badań statystycznych statystyki publicznej na rok 2010 (Dz. U. Nr 3, poz. 14). Jak wskazano w załączniku do rozporządzenia Rady Ministrów z dnia 27 listopada 2008 r. (Dz. U. Nr 221, poz. 1436), w ramach badań zachorowalności i leczonych na wybrane choroby, regionalne rejestry onkologiczne miały obowiązek przekazywania do dnia 30 czerwca 2010 r. do Centrum Onkologii (Krajowego Rejestru Chorób Nowotworowych) karty zgłoszeń nowotworu złośliwego (MZ/N-1a) za rok 2009, z terenu województwa, które dany rejestr obejmował. Taki obowiązek wynikał również z rozporządzeń wydanych w poprzednich latach i został także utrzymany w ww. rozporządzeniu Rady Ministrów z dnia 8 grudnia 2009 r. Wzory formularzy sprawozdawczych i objaśnienia, co do sposobu ich wypełniania oraz wzory kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej, określa Prezes Rady Ministrów w drodze rozporządzenia. W 2010 r. Prezes Rady Ministrów wydał rozporządzenie z dnia 28 kwietnia 2010 r. w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych, ustalonych w programie badań statystycznych statystyki publicznej na rok 2010 (Dz. U. Nr 106, poz. 676). Określił w nim m. in. wzór formularzy sprawozdawczych do badań statystycznych, ustalonych w programie badań statystycznych statystyki publicznej na rok 2010, prowadzonych przez ministra właściwego do spraw zdrowia, w tym - kartę zgłoszenia nowotworu złośliwego – MZ/N-1a. Biorąc za podstawę stan faktyczny ustalony w toku kontroli oraz obowiązujące przepisy prawa, Generalny Inspektor uznał, iż przetwarzanie danych w Krajowym Rejestrze Nowotworów oraz w wojewódzkich rejestrach nowotworów odbywa się bez podstawy prawnej, a tym samym narusza przysługujące każdej osobie konstytucyjne prawo do ochrony jej danych osobowych (wyrażone w art. 51 Konstytucji RP) i skonkretyzowane w ustawie o ochronie danych osobowych. Z uwagi na to, że korespondencja z Ministerstwem Zdrowia w ww. sprawie prowadzona jest od wielu lat, Generalny Inspektor po raz kolejny zwrócił się do Ministra Zdrowia o podjęcie działań mających na celu odpowiednie uregulowanie przetwarzania danych osobowych w ramach Krajowego Rejestru Nowotworów i wojewódzkich rejestrów nowotworów.<sup>18</sup> W odpowiedzi Generalny Inspektor został poinformowany o trwających pracach nad ustawą o systemie informacji w ochronie zdrowia, w której

---

<sup>17</sup> DIS-K-421/127/10

<sup>18</sup> Pismo z dnia 11 października 2010 r. DIS-K-421/127/10/39984,39987.

znajdą się m.in. przepisy określające zasady prowadzenia rejestrów medycznych, w tym Krajowego Rejestru Nowotworów i wojewódzkich rejestrów nowotworów<sup>19</sup>. Tym nie mniej w prowadzonych pracach legislacyjnych Minister Zdrowia wskazywał na konieczność uregulowania zakresu danych osobowych i zasad ich przetwarzania w wyżej wymienionym rejestrze w rozporządzeniu, co spotkało się z krytyką Generalnego Inspektora niezmiennie uznającego, że kwestie te powinny stanowić materię ustawową.

## **6) Ubezpieczenia społeczne, majątkowe i osobowe**

W okresie sprawozdawczym w towarzystwach ubezpieczeniowych przeprowadzono **12 kontroli** zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych<sup>20</sup>. Zakresem kontroli objęto udostępnianie przez towarzystwa ubezpieczeniowe danych osobowych klientów innym towarzystwom ubezpieczeniowym, pozyskiwanie danych osobowych klientów od innych towarzystw ubezpieczeniowych oraz zabezpieczenia zastosowane w procesie przetwarzania danych osobowych klientów. Należy podkreślić, że na 12 skontrolowanych towarzystw ubezpieczeniowych, w 6 przypadkach nie stwierdzono uchybień w procesie przetwarzania danych osobowych. Powyższe wskazuje, że podmioty te dokładają należytej staranności i dbałości w celu zapewnienia odpowiedniego zabezpieczenia przetwarzanych danych osobowych.

Przeprowadzone kontrole wykazały, że dane osobowe były przekazywane do innych towarzystw ubezpieczeniowych i otrzymywane od nich na podstawie art. 19 ust. 2 pkt 22 ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. z 2010 r. Nr 11, poz. 66 z późn. zm.)<sup>21</sup>. Przekazywanie i pozyskiwanie dokumentów zawierających dane osobowe następowało w związku z postępowaniem wyjaśniającym, będącym jednym z etapów rozpatrywania zgłoszonego roszczenia. Wymiana informacji pomiędzy towarzystwami ubezpieczeniowymi, w zamierzeniu miałyby zapobiegać przestępczości ubezpieczeniowej związanej np. z wyłudzeniem nienależnego odszkodowania lub odszkodowania od więcej niż jednego towarzystwa ubezpieczeniowego przez osobę do tego nieuprawnioną.

W toku kontroli towarzystw ubezpieczeniowych sprawdzonych zostało szesnaście systemów informatycznych wykorzystywanych do wymiany danych osobowych z innymi towarzystwami

---

<sup>19</sup> Pismo z dnia 2 listopada 2010 r. MZ-OZ-078-21628-39/N.Ż./10.

<sup>20</sup> Np. kontrole DIS-K-421/54/10, DIS-K-421/64/10, DIS-K-421/75/10, DIS-K-421/91/10, DIS-K-421/104/10.

<sup>21</sup> Art. 19 ust. 1. Zakład ubezpieczeń i osoby w nim zatrudnione lub osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia. Art. 19 ust. 2 pkt 22. Zakaz, o którym mowa w ust. 1, nie dotyczy informacji udzielanych na wnioski innego zakładu ubezpieczeń, w zakresie niezbędnym dla przeciwdziałania przestępczości ubezpieczeniowej lub stosowania taryfy w zależności od długości okresu bezszkodowego, lub ustalania proporcjonalnej odpowiedzialności, w przypadku zawarcia umów ubezpieczenia obowiązkowego na ten sam okres w co najmniej dwóch zakładach ubezpieczeń, lub dla potrzeb ustalenia odpowiedzialności, jeżeli ten sam przedmiot ubezpieczenia w tym samym czasie jest ubezpieczony od tego samego ryzyka w dwóch lub więcej zakładach ubezpieczeń na sumy, które łącznie przewyższają jego wartość ubezpieczeniową.

ubezpieczeniowymi. W większości przypadków systemy te opracowane zostały przez pracowników danego towarzystwa ubezpieczeniowego. Spotykano się również z wykorzystywaniem do powyższych celów takich narzędzi informatycznych jak edytory tekstu (pliki w formacie doc, PDF) i arkusze kalkulacyjne (skoroszyty, arkusze w formatach xls, ods) przetwarzanych z wykorzystaniem aplikacji pakietu MS Office, OpenOffice oraz Acrobat Reader. Proces pozyskiwania/udostępniania danych przetwarzanych w postaci elektronicznej, realizowany był za pośrednictwem teletransmisji danych z wykorzystaniem sieci Internet i/lub poprzez fizyczne przekazanie danych zapisanych na nośniku informatycznym (nośniku typu płyta CD). Proces pozyskiwania/udostępniania danych poprzez teletransmisję danych z wykorzystaniem sieci Internet, realizowany był przeważnie za pośrednictwem jednego z głównych systemów informatycznych, bądź za pośrednictwem poczty elektronicznej użytkowanej przez dane towarzystwo ubezpieczeniowe. Dla wszystkich skontrolowanych systemów informatycznych, z wyjątkiem jednego, zastosowane zostały środki bezpieczeństwa na poziomie wysokim. Nieprawidłowości występujące w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych wystąpiły w odniesieniu do dwóch administratorów danych, przy czym w jednym przypadku nieprawidłowości te dotyczyły nienależytego zabezpieczenia przesyłanych danych za pośrednictwem poczty elektronicznej.

Towarzystwa ubezpieczeniowe, w których odnotowano uchybienia w procesie przetwarzania danych osobowych, najwięcej problemów miały z prawidłowym wykonaniem podstawowych obowiązków dotyczących zabezpieczenia danych, określonych w przepisach o ochronie danych osobowych. W toku kontroli dwóch towarzystw ubezpieczeniowych stwierdzono, iż polityka bezpieczeństwa nie zawierała wszystkich niezbędnych elementów określonych 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 (m.in. wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz opisu sposobu przepływu danych pomiędzy poszczególnymi systemami), w toku trzech innych kontroli ustalono, że do prowadzonej ewidencji osób upoważnionych do przetwarzania danych osobowych nie wpisano wszystkich wymaganych informacji (m.in. zakresu upoważnienia do przetwarzania danych osobowych), natomiast w jednym przypadku do przetwarzania danych osobowych zostały dopuszczone osoby nieposiadające stosownego upoważnienia.

W związku ze stwierdzonymi uchybieniami wobec 6 towarzystw ubezpieczeniowych wszczęte zostały postępowania administracyjne i wydane zostały decyzje nakazujące ich usunięcie m.in. w zakresie uzupełnienia ewidencji osób upoważnionych do przetwarzania danych osobowych o zakres upoważnienia do przetwarzania danych osobowych oraz datę ustania upoważnienia oraz zapewnienia kryptograficznej ochrony danych przesyłanych pocztą elektroniczną do innych towarzystw

ubezpieczeniowych. Ponadto Generalny Inspektor nakazał uzupełnienie polityki bezpieczeństwa o: wykaz pomieszczeń i części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych zawierający informację o systemach służących do przetwarzania danych osobowych udostępnianych innym towarzystwom ubezpieczeniowym i otrzymywanych od innych towarzystw ubezpieczeniowych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także o sposób przepływu danych pomiędzy poszczególnymi systemami.<sup>22</sup>

## 7) Telekomunikacja

W 2010 r. przeprowadzono **15 kontroli u dostawców usług telekomunikacyjnych**, tj. o 8 więcej w stosunku do poprzedniego roku sprawozdawczego. Na 15 kontroli, którymi objęto przetwarzanie danych osobowych klientów usług telekomunikacyjnych, 14 przeprowadzono w ramach kontroli sektorowych<sup>23</sup>.

Stwierdzone w toku kontroli nieprawidłowości dotyczyły przede wszystkim składanych przez klientów oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych. Uchybienia w tym zakresie polegały w szczególności na niezapewnieniu osobom składającym oświadczenie, swobody przy składaniu tych oświadczeń, na łączeniu w jednym oświadczeniu zgód na różne cele przetwarzania danych (np. zgody na otrzymywanie informacji handlowej, przetwarzanie danych osobowych przez osoby trzecie w celach marketingowych, przetwarzanie danych transmisyjnych dla celów marketingowych, przetwarzanie danych związanych z przetwarzaniem usług drogą elektroniczną do celów reklamy, badania rynku, zachowań i preferencji usługobiorców) oraz niewskazaniu celu, w jakim będą przetwarzane. Ponadto, część dostawców usług telekomunikacyjnych pozyskiwała zgodę na przetwarzanie danych osobowych w celu marketingu ich własnych produktów i usług, pomimo iż w takich przypadkach zgoda osób, których dane dotyczą, nie jest wymagana. W pojedynczych przypadkach przeprowadzone kontrole wykazały, że operatorzy telekomunikacyjni nie realizowali w pełni ciążącego na nich obowiązku informacyjnego, wynikającego z art. 24 ust. 1 ustawy o ochronie danych osobowych<sup>24</sup> (m.in. brak informacji o aktualnym adresie siedziby administratora danych oraz

---

<sup>22</sup> Np. decyzje DIS/DEC-689/23129/10, DIS/DEC-958/2955/10, DIS/DEC-1021/32677/10.

<sup>23</sup> Np. kontrole DIS-K-421/81/10, DIS-K-421/92/10, DIS-K-421/98/10, DIS-K-421/108/10, DIS-K-421/130/10, DIS-K-421/133/10, DIS-K-421/161/10, DIS-K-421/163/10.

<sup>24</sup> 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.

o podstawie prawnej obowiązku podania danych), nie dopełnili obowiązku zgłoszenia do rejestracji wszystkich prowadzonych zbiorów danych osobowych (m.in. zbioru danych osób, które wypełniają tzw. formularze kontaktowe dostępne na stronie internetowej operatora) oraz zmian informacji zawartych w zgłoszeniu zbioru danych osobowych do rejestracji Generalnemu Inspektorowi.

Na podstawie wyników kontroli operatorom telekomunikacyjnym zarzucono również niedołożenie szczególnej staranności w celu ochrony interesów abonentów, a w szczególności niezapewnienie, aby dane te były przetwarzane zgodnie z prawem. Stwierdzane w tym zakresie nieprawidłowości dotyczyły pozyskiwania danych w zakresie szerszym (np. imion rodziców, miejsca i daty urodzenia), niż to wynika z przepisów § 6 ust. 2 pkt 1 oraz § 7 ust. 2 pkt 1 rozporządzenia Ministra Infrastruktury z dnia 17 czerwca 2009 r. w sprawie warunków korzystania z uprawnień w publicznych sieciach telefonicznych (Dz. U. Nr 97, poz. 810)<sup>25</sup> oraz pozyskiwania dodatkowych danych (np. adresu do korespondencji i adresu poczty elektronicznej) bez zgody klienta, o której mowa w art. 161 ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.)<sup>26</sup>.

Do nielicznych należały natomiast uchybienia związane z niedopełnieniem obowiązku zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Nieprawidłowości polegały w szczególności na niezastosowaniu środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej, na stosowaniu procedur, zgodnie z którymi hasła logowania do systemu informatycznego znane były także innym osobom niż użytkownicy, na użytkowaniu systemu informatycznego, który nie zapewniał dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie ww. informacje, a także na nieopracowaniu ewidencji osób upoważnionych do przetwarzania danych osobowych lub niezawarcia w niej wszystkich wymaganych elementów, określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych (m.in. zakresu upoważnienia do przetwarzania danych osobowych).

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

---

<sup>25</sup> § 6 ust. 2 pkt 1 oraz § 7 ust. 2 pkt 1. Wniosek o przeniesienie numeru powinien zawierać następujące dane osobowe: imię i nazwisko, numer PESEL, nazwę i numer dokumentu tożsamości (w przypadku osób nie posiadających numeru PESEL), adres korespondencyjny.

<sup>26</sup> Art. 161 ust. 3. Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer identyfikacji podatkowej NIP, numer konta bankowego lub karty płatniczej, adres

postępowania<sup>27</sup>. W wydanych decyzjach Generalny Inspektor nakazał m.in. zapewnienie klientom możliwości złożenia oświadczenia o niewyrażeniu zgody na przetwarzanie ich danych dodatkowych oraz opracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych.

## 8) Zatrudnienie

W 2010 r. skontrolowano działalność jednego z pracodawców<sup>28</sup>, który wykorzystywał dane biometryczne pracowników do rejestracji czasu pracy. Kontrola wykazała, że zastosowany przez jednostkę kontrolowaną system rejestracji czasu pracy obejmował czytniki linii papilarnych wraz z oprogramowaniem służącym do rejestracji wejść i wyjść w oparciu o rejestrowane obrazy cyfrowe linii papilarnych. Cyfrowy wzorec odcisku palca, odpowiednio zaszyfrowany w postaci zapisu cyfrowego (kod pięćdziesięciu punktów charakterystycznych wybranego palca), zapisywany był na karcie elektronicznej. Pracownik przykładł do czytnika kartę elektroniczną i palec w celu potwierdzenia swojej tożsamości. Obrazy linii papilarnych pobierane były z palców dłoni poprzez czytnik i po przetworzeniu do określonej postaci cyfrowej porównywane ze wzorcem, który zapisany był na karcie elektronicznej. W przypadku poprawnego porównania, zdarzenie było zapisywane w pamięci czytnika (zapisywany był numer ID oraz pierwsze trzy litery imienia i nazwiska pracownika), a z pamięci tymczasowej czytnika kasowany był obraz odczytanych linii papilarnych. W wyniku zestawienia kodu cyfrowego zapisanego na karcie pracownika z kodem cyfrowym wygenerowanym on-line przez oprogramowanie czytnika dla przyłożonego palca możliwe było potwierdzenie tożsamości pracownika i jego identyfikacja na podstawie zapisanego na karcie elektronicznej numeru ID.

W oparciu o dokonane ustalenia Generalny Inspektor uznał, że cyfrowe wzorce odcisków palców pracowników jednostki kontrolowanej, stanowią dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych. Co więcej, ich pozyskiwanie w celu rejestracji czasu pracy stanowi poszerzenie zakresu danych zbieranych od pracowników względem katalogu wskazanego w art. 22<sup>1</sup> Kodeksu pracy<sup>29</sup>. W celu przywrócenia stanu zgodnego z prawem wydana została decyzja nakazująca

---

korespondencyjny użytkownika, jeżeli jest on inny niż adres miejsca zameldowania na pobyt stały tego użytkownika, a także adres poczty elektronicznej oraz numery telefonów kontaktowych.

<sup>27</sup> Np. decyzje DIS/DEC-1212/41382/10, DIS/DEC-1244/43775/10, DIS/DEC-1375/49785/10.

<sup>28</sup> DIS-K-421/46/10

<sup>29</sup> Art. 22<sup>1</sup> § 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.

zaprzestanie zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników jednostki kontrolowanej<sup>30</sup>.

O ile wykorzystywanie metod biometrycznych dla kontroli stosowania zasad bezpieczeństwa na terenie zakładu pracy może w pewnych przypadkach zostać uznane za środek adekwatny do celu, jaki chce osiągnąć podmiot odpowiedzialny za bezpieczeństwo, o tyle stosowanie tych samych metod dla poświadczania zdarzeń związanych ze stosunkiem pracy nie znajduje podstaw w przepisach prawa pracy.

## 9) Komunalne jednostki organizacyjne

W okresie sprawozdawczym skontrolowano **18 komunalnych jednostek organizacyjnych**, w tym 16 przeprowadzono w ramach kontroli sektorowej<sup>31</sup>. W toku 3 kontroli nie stwierdzono uchybień w procesie przetwarzania danych osobowych.

Przeprowadzone kontrole wykazały, że komunalne jednostki organizacyjne najwięcej problemów miały z prawidłowym wykonaniem obowiązków wynikających z przepisów rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Uchybienia w tym zakresie polegały w szczególności na: wykorzystywaniu do przetwarzania danych osobowych systemów informatycznych niezapewniających dla każdej osoby, której dane osobowe są przetwarzane w tych systemach, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, zmianie haseł dostępu rzadziej niż co 30 dni oraz stosowaniu haseł nie zawierających wymaganej liczby znaków. Niektóre jednostki kontrolowane używały również systemów informatycznych, w których dostęp do danych osobowych nie wymagał wprowadzenia identyfikatora użytkownika i dokonywania uwierzytelnienia.

Krytycznie należy ocenić także sposób wykonania podstawowych obowiązków wynikających z przepisów ustawy o ochronie danych osobowych. Uchybienia w tym zakresie dotyczyły m.in. 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 niedopełnienia w pełnym zakresie wobec osób, których dane dotyczą, obowiązku informacyjnego wynikającego z art. 24 ust. 1 ustawy o ochronie danych osobowych, niezgłoszenia zmian informacji zawartych w zgłoszeniu zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz niezastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę

---

<sup>30</sup> Decyzja DIS/DEC-1133/37986/10.

<sup>31</sup> Np. kontrole DIS-K-421/131/10, DIS-K-421/157/10, DIS-K-421/160/10, DIS-K-421/166/10.



przetwarzanym danym osobowym (m.in. przechowywano dokumenty zawierające dane osobowe w szafach, które nie zostały wyposażone w zamki). W pojedynczych przypadkach kontrole wykazały, że podmioty kontrolowane przetwarzały dane szczególnie chronione dotyczące orzeczeń wydanych w postępowaniu sądowym, bez podstawy prawnej wynikającej z art. 27 ust. 2 ustawy o ochronie danych osobowych<sup>32</sup>.

Liczne zastrzeżenia co do prawidłowości wykonania obowiązków wynikających z przepisów o ochronie danych osobowych, odnosiły się także do dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumentacja ta najczęściej nie zawierała wszystkich wymaganych informacji, określonych w § 4 i § 5 ww. rozporządzenia (m.in. opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami i wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych). Nie wszystkie wymagane elementy, określone w art. 39 ust. 1 ustawy o ochronie danych osobowych, zawarte były również w ewidencji osób upoważnionych do przetwarzania danych osobowych (np. brak zakresu upoważnienia). Do rzadkich przypadków należało natomiast niewyznaczenie administratora bezpieczeństwa informacji oraz nienadanie upoważnień osobom dopuszczonym do przetwarzania danych osobowych.

Jednym z bardziej interesujących zagadnień, jakie wyniknęły w toku kontroli przeprowadzonych w komunalnych jednostkach organizacyjnych, była kwestia rozstrzygnięcia, komu przysługuje przymiot administratora danych przetwarzanych w związku z zaspakajaniem zbiorowych potrzeb wspólnoty samorządowej w Warszawie. Przeprowadzone w tych jednostkach kontrole wykazały, że na mocy nadanych im statutów są one jednostkami budżetowymi m.st. Warszawy, do

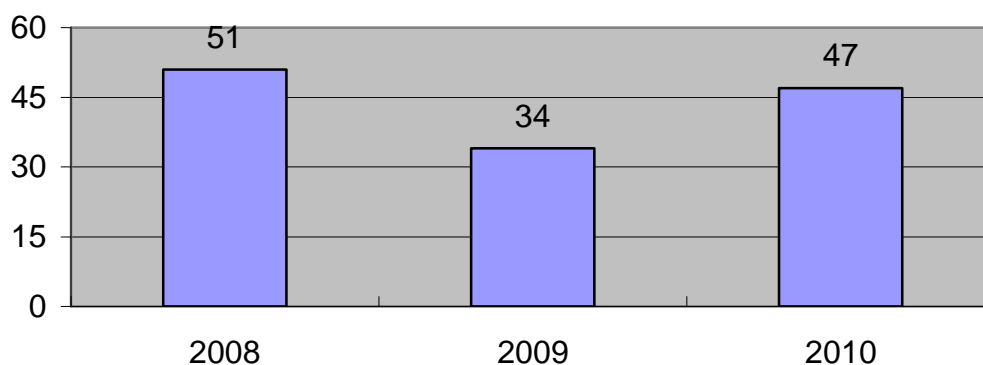
---

<sup>32</sup> Art. 27.2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli: 1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych, 2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony, 3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora, 4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych, 5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem, 6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie, 7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych, 8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą, 9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone, 10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

których zadań należy m.in. gospodarowanie w granicach zwykłego zarządu, w sposób i na zasadach określonych przepisami prawa oraz ustaleniami organów m.st. Warszawy, mieszkaniowym zasobem m.st. Warszawy, powierzonym zasobem nieruchomości m.st. Warszawy, a także wykonywanie innych zadań powierzonych przez organy m.st. Warszawy z zakresu zarządu mieszkaniowym zasobem i zasobem nieruchomości. Wymienione zadania wskazane jednostki wykonywały w oparciu o pełnomocnictwo udzielone przez Prezydenta m.st. Warszawy. Po dokonaniu analizy stanu faktycznego i prawnego Generalny Inspektor uznał, że administratorem danych przetwarzanych w związku z zaspakajaniem zbiorowych potrzeb wspólnoty samorządowej w m.st. Warszawie jest Prezydent m.st. Warszawy, a wskazane jednostki są podmiotami, które działają w jego imieniu.

## 10) Inne

W okresie sprawozdawczym w podmiotach nienależących do sektorów omówionych w poprzednich rozdziałach przeprowadzono **47 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych<sup>33</sup>. Grupa tych podmiotów była bardzo zróżnicowana i obejmowała m.in. podmioty wykonujące działalność gospodarczą w zakresie prowadzenia programów lojalnościowych, przewoźników, biura podróży, podmioty zajmujące się produkcją, handlem i usługami.



*Wykres 1: Zestawienie porównawcze liczby przeprowadzonych kontroli w podmiotach należących do sektora „Inne” w latach 2008–2010.*

Analizując wyniki kontroli należy stwierdzić, że jednostki kontrolowane miały problemy z prawidłowym wykonaniem podstawowych obowiązków wynikających z przepisów o ochronie danych osobowych. Uchybienia w tym zakresie dotyczyły m.in. naruszenia zasady adekwatności

<sup>33</sup> Np. kontrole DIS-K-421/11/10, DIS-K-421/57/10, DIS-K-421/80/10, DIS-K-421/115/10 i DIS-K-421/165/09.

przetwarzanych danych, jak również polegały na przechowywaniu danych w postaci umożliwiającej identyfikację osób, których dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Zdarzały się również przypadki niedopełnienia w pełnym zakresie wobec osób, których dane dotyczą, obowiązku informacyjnego wynikającego z art. 24 ust. 1 i art. 25 ust. 1 ustawy o ochronie danych osobowych<sup>34</sup> oraz niezgłoszenia zmian informacji zawartych w zgłoszeniu zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. 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 cytowanego rozporządzenia. W pojedynczych przypadkach stwierdzano także uchybienia polegające na niezawarcie w formie pisemnej umowy powierzenia przetwarzania danych osobowych lub nieokreśleniu w takiej umowie zakresu i celu przetwarzania powierzonych danych.

Przeprowadzone kontrole wykazały również, że administratorzy danych mają problemy z prawidłowym sformułowaniem treści oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych tak, aby wyrażona w taki sposób zgoda nie była domniemana lub dorozumiana z oświadczenia woli o innej treści. Uchybienia w tym zakresie stwierdzono w szczególności w toku kontroli przeprowadzonych w podmiotach uczestniczących w prowadzeniu programu lojalnościowego. Ustalono, że osoby zainteresowane przystąpieniem do programu lojalnościowego wypełniały formularz, w treści którego zawarte zostało oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych m.in. w celach marketingowych przez kilka podmiotów. Zawarcie wskazanej zgody w treści jednego oświadczenia bez jednoczesnego zapewnienia możliwości wyboru oznaczało, że osoba, której dane dotyczą, nie miała swobody w dysponowaniu swoimi danymi osobowymi, a w szczególności swobody w wyborze podmiotów, na rzecz których chciałaby wyrazić zgodę na przetwarzanie dotyczących jej danych osobowych. Tymczasem zgoda powinna być sformułowana w sposób wyraźny i jednoznaczny oraz wyróżniać się spośród innych pochodzących od tej osoby informacji i oświadczeń woli. W przypadku oświadczenia dotyczącego różnych celów przetwarzania, zgoda powinna być wyrażona wyraźnie pod każdym z tych celów przetwarzania<sup>35</sup>. Jednocześnie niezbędne jest umożliwienie osobie swobodnego wyrażenia woli w przedmiocie zgody na

---

<sup>34</sup> Art. 25. 1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, 3) źródle danych, 4) prawie dostępu do treści swoich danych oraz ich poprawiania, 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

<sup>35</sup> Por. wyrok Naczelnego Sądu Administracyjnego z dnia 11 kwietnia 2003 r. sygn. akt II SA 3942/02.

przetwarzanie jej danych, np. poprzez zapewnienie opcjonalności (możliwości wyboru) w klauzuli zgody na przetwarzanie danych osobowych, w szczególności wówczas, gdy dane mają być przetwarzane przez różne podmioty. Z uwagi na to, że oświadczenie o wyrażeniu zgody zawarte w treści formularza przystąpienia do programu lojalnościowego nie spełniało ww. warunków, Generalny Inspektor nakazał przywrócenie w tym zakresie stanu zgodnego z prawem poprzez sformułowanie przedmiotowego oświadczenia w taki sposób, aby zapewnić osobie wypełniającej ten formularz opcjonalność w kwestii wyrażenia zgody na przetwarzanie jej danych osobowych przez podmioty wymienione w jego treści<sup>36</sup>.

Kolejną sprawą badaną podczas kontroli była kwestia zatrzymywania dokumentów potwierdzających tożsamość klientów wypożyczających w hipermarketach „wózki – samochodziki” dla dzieci. Można określić te działania jako swoisty „zastaw” za wypożyczany przedmiot. Zatrzymywane dokumenty stanowiły np. legitymacje studenckie, prawa jazdy, elektroniczne karty ubezpieczeniowe (wydawane przez Śląski Oddział Narodowego Funduszu Zdrowia) i dowody rejestracyjne samochodów. Jak ustalono, podstawą prawną zatrzymywania dokumentów osób wypożyczających wózki, i tym samym przetwarzania danych osobowych ich posiadaczy, była zgoda ww. osób wyrażana poprzez dobrowolne pozostawienie dokumentu w punkcie wypożyczania wózków oraz umowa o wypożyczenie wózka zawierana w formie ustnej. Zakres danych osobowych pozyskiwanych od wskazanych osób wynikał z rodzaju dokumentu pozostawionego pod zastaw wózka.

W świetle dokonanych ustaleń oraz po przeprowadzeniu szczegółowej analizy przepisów określających zakres danych, jaki jest zawarty w treści poszczególnych dokumentów, które były zatrzymywane pod zastaw wózka, Generalny Inspektor uznał, że w związku z realizacją takiej umowy administrator danych pozyskiwał szerszy zakres danych niż ten, który był niezbędny dla realizacji ww. umowy, naruszając tym samym zasadę adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Konsekwencją była decyzja nakazująca przywrócenie stanu zgodnego z prawem poprzez zaprzestanie pozyskiwania danych osób wypożyczających wózki w zakresie szerszym, niż jest to niezbędne dla realizacji umowy wypożyczenia wózka<sup>37</sup>.

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 były przetwarzane w systemach informatycznych, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz zmiana haseł dostępu rzadziej niż co 30 dni).

---

<sup>36</sup> Np. decyzja DIS/DEC-1098/36246/10.

<sup>37</sup> DIS/DEC-651/21887/10

W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych przez jednostki kontrolowane, wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych w toku postępowania<sup>38</sup>. Generalny Inspektor w decyzjach nakazywał w szczególności dopełnianie wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych, zmodyfikowanie systemów informatycznych służących do przetwarzania danych osobowych w taki sposób, aby systemy te zapewniały dla każdej osoby, której dane osobowe są w nim przetwarzane, odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikator użytkownika wprowadzającego te dane oraz opracowanie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

### **2.3. Systemy informatyczne służące do przetwarzania danych osobowych**

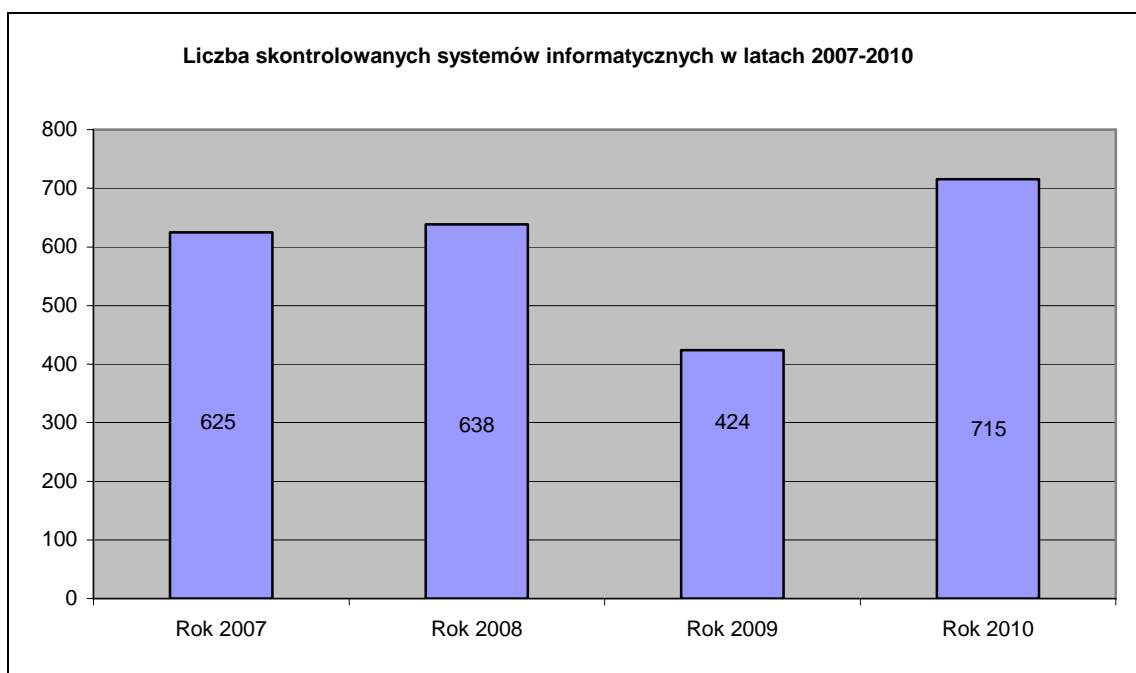
W ramach przeprowadzonych w 2010 r. kontroli, weryfikacji poddano **715 systemów informatycznych** wykorzystywanych do przetwarzania danych osobowych. Jest to najwyższa liczba od 4 lat, gdzie liczby przeprowadzonych kontroli, w tym systemów informatycznych przedstawiały się następująco:

rok 2007 = 161 kontroli, obejmujących 625 systemów informatycznych,  
rok 2008 = 201 kontroli, obejmujących 638 systemów informatycznych,  
rok 2009 = 220 kontroli, obejmujących 424 systemy informatyczne,  
rok 2010 = 196 kontroli, obejmujących 715 systemów informatycznych.

Wzrost liczby systemów informatycznych poddanych kontroli jest zjawiskiem naturalnym – związanym z coraz częstszym przetwarzaniem danych w środowisku elektronicznym w miejsce kartotek, skrówidzów, ksiąg, wykazów i w innych zbiorów ewidencyjnych prowadzonych w postaci papierowej. Należy zwrócić uwagę na zdecydowanie większy nakład pracy inspektorów z Biura GODO przeznaczany na każdą z kontroli, która obejmuje wiele systemów informatycznych prowadzonych przy użyciu różnego oprogramowania. Dalsze zwiększenie liczby kontrolowanych systemów nie będzie możliwe bez zwiększenia nakładów finansowych przeznaczonych na szkolenie pracowników Biura w zakresie nowych technologii przetwarzania danych i bez zwiększenia nakładów finansowych na same kontrole.

---

<sup>38</sup> Np. decyzje DIS/DEC-1152/39023/10, DIS/DEC-843/26172/10, DIS/DEC-1206/40994/10, DIS/DEC-651/21887/10, DIS/DEC-1376/49787/10 i DIS/DEC-1053/35065/10.



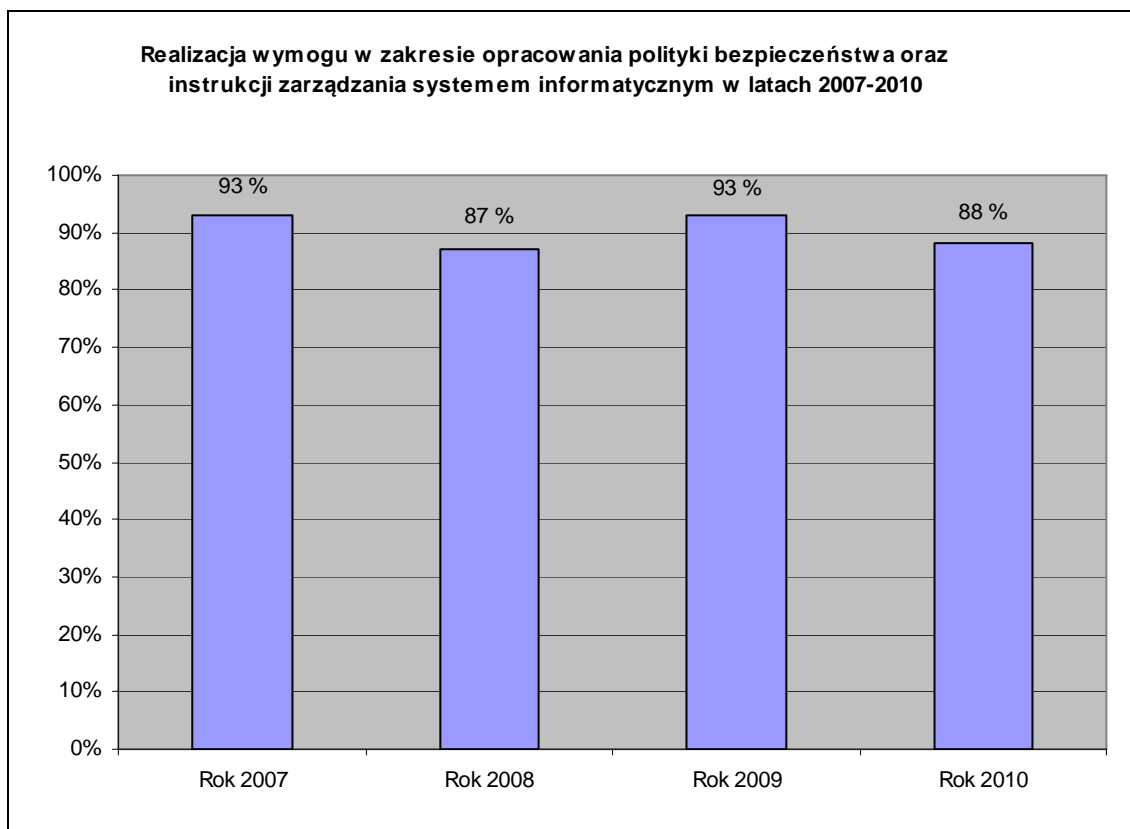
*Wykres 2: Zestawienie porównawcze liczby skontrolowanych systemów informatycznych w latach 2007–2010.*

#### **2.4. Wyniki kontroli w zakresie wypełnienia obowiązków formalnych i organizacyjnych**

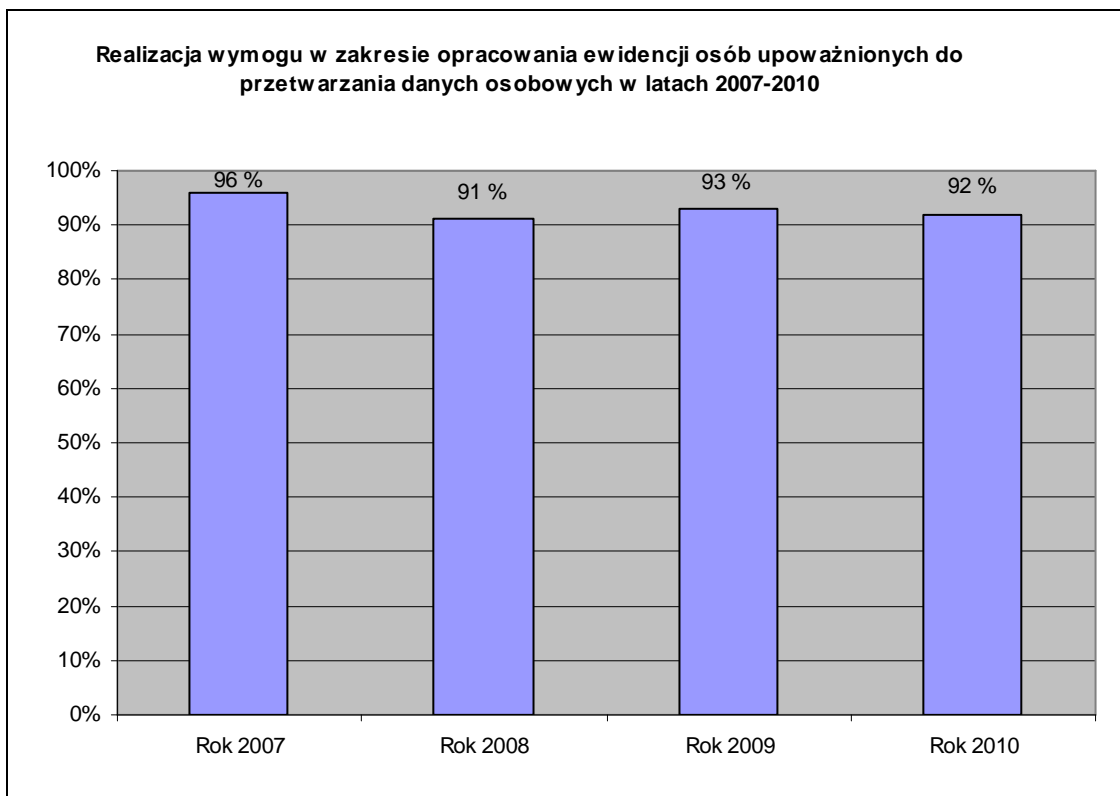
Realizacja w latach 2007-2010 wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie o ochronie danych osobowych i rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zobrażona została poniżej w formie diagramów. Wykresy pokazują procentowe wyniki kontroli w odniesieniu do ogólnej liczby kontroli w danym roku lub ogólnej liczby kontrolowanych w danym roku systemów informatycznych. Warunki odnoszące się do wymaganych funkcjonalności systemów informatycznych oceniane były w skali procentowej do liczby systemów objętych kontrolą. Pozostałe wymogi natomiast, odnoszące się np. do dokumentacji procesu przetwarzania, czy też obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, oceniano w skali procentowej w stosunku do liczby kontrolowanych podmiotów.

Proces przetwarzania danych w zakresie wymogów formalno-organizacyjnych uznawano za prawidłowy, gdy kontrolowana jednostka opracowała wymagane dokumenty (takie jak polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania

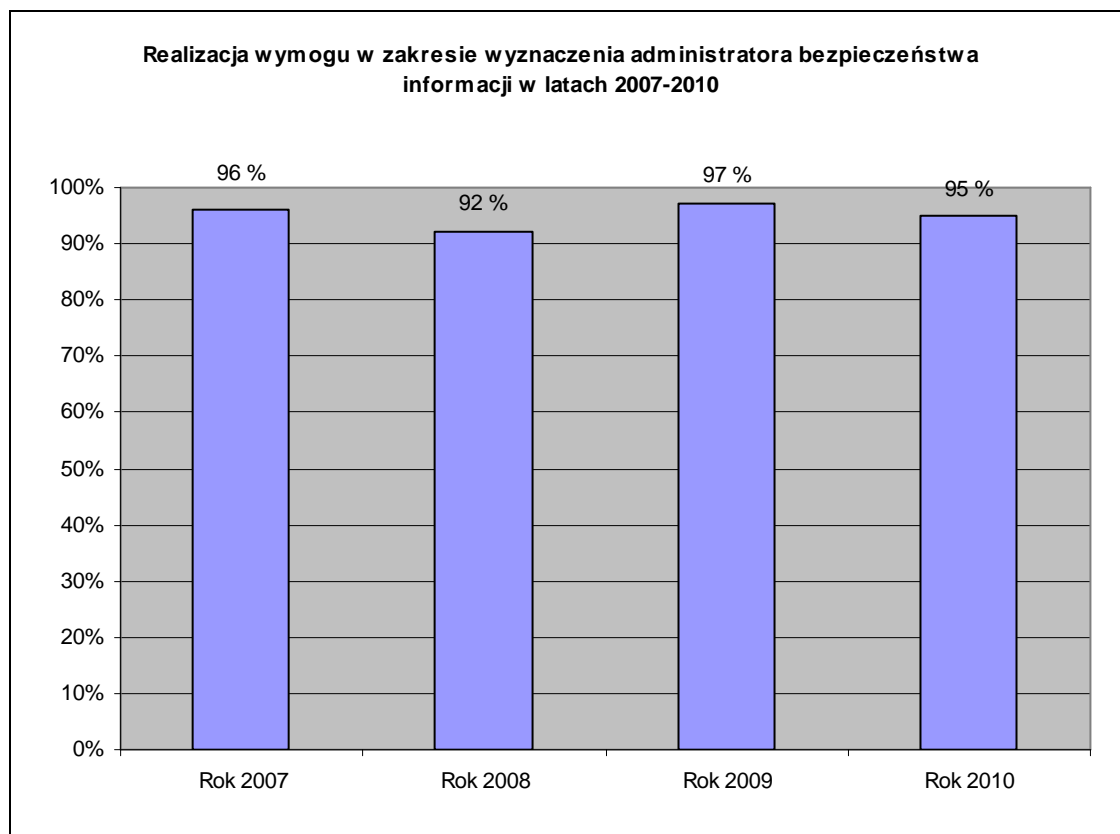
danych osobowych), prowadziła ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wdrożyła opisane w tej dokumentacji procedury. Ponadto sprawdzano, czy wyznaczony został administrator bezpieczeństwa informacji oraz, czy osoby dopuszczone do przetwarzania danych posiadały stosowne upoważnienia. Stopień wykonania przez kontrolowane podmioty ww. warunków w latach 2007-2010 przedstawiono na poniższych diagramach (Wykresy: 3, 4, 5).



**Wykres 3: Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych (polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych) w latach 2007–2010.**



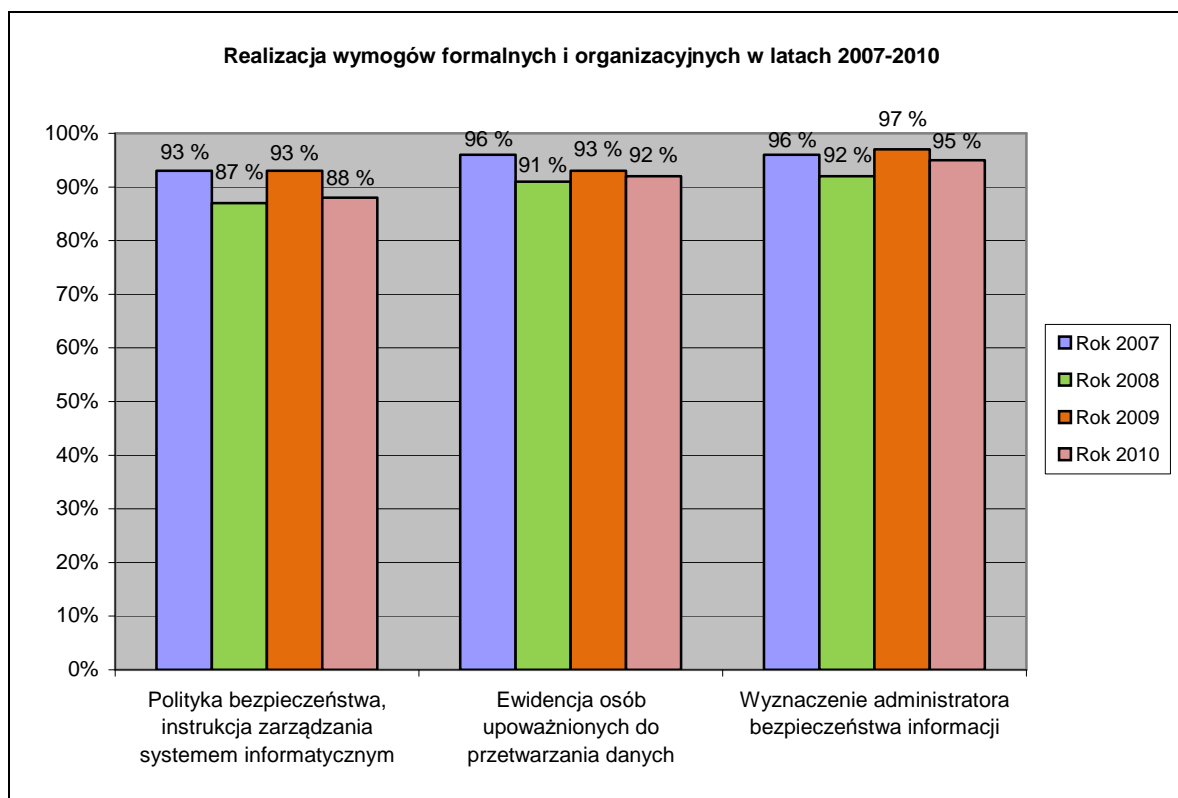
**Wykres 4: Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w latach 2007–2010.**



**Wykres 5: Stopień realizacji obowiązku wyznaczenia administratora bezpieczeństwa informacji w latach 2007-2010.**



Zbiorne zestawienie wypełnienia wymogów formalnych i organizacyjnych w zakresie dotyczącym prowadzenia dokumentacji przetwarzania danych osobowych oraz wyznaczenia administratora bezpieczeństwa informacji w latach 2007-2010 zestawiono na poniższym diagramie (Wykres 6).



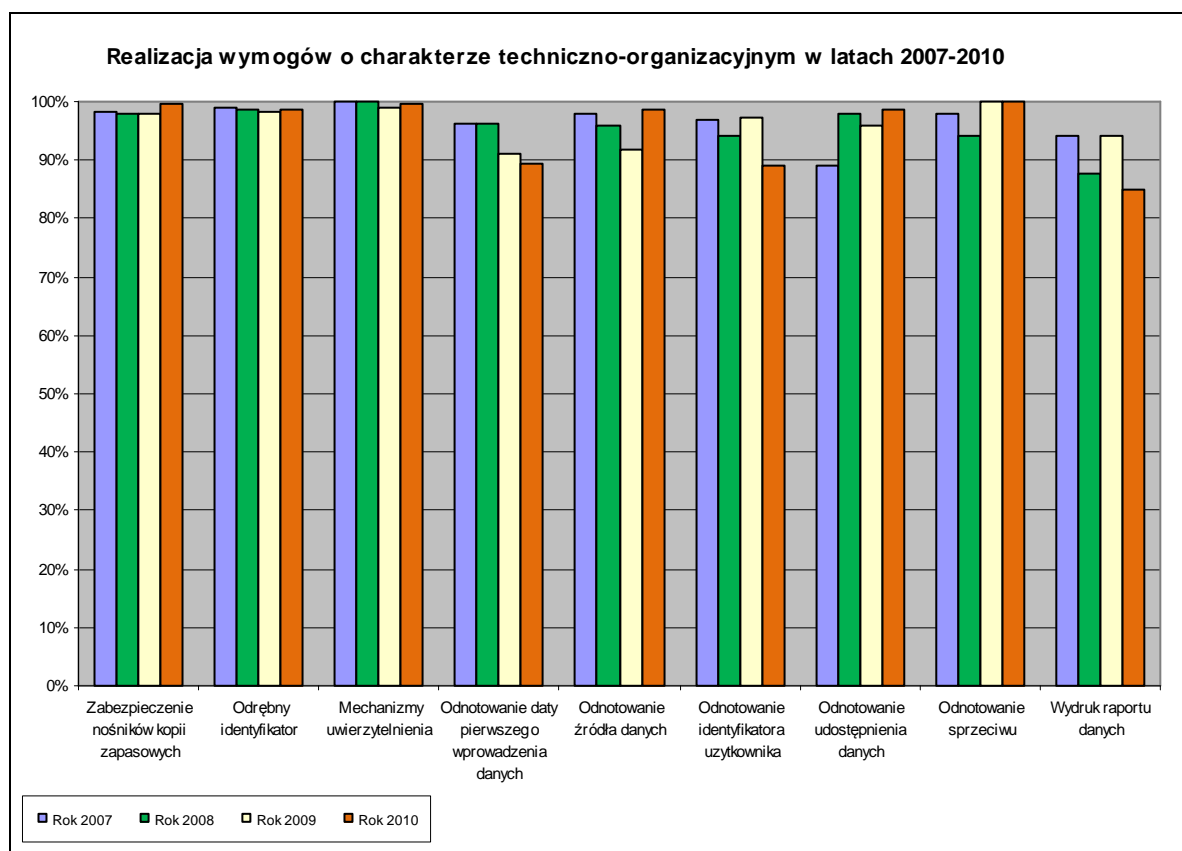
Wykres 6: *Stopień realizacji obowiązku prowadzenia dokumentacji stanowiącej politykę bezpieczeństwa, instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wypełnienie obowiązku wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji w latach 2007–2010.*

## 2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych

W 2010 r. skontrolowano **715 systemów informatycznych** służących do przetwarzania danych osobowych. Były to systemy o bardzo różnorodnych rozwiązaniach technologicznych, od najprostszych, gdzie zbiory danych osobowych przetwarzane były z wykorzystaniem powszechnie dostępnych aplikacji biurowych (edytorów tekstu, arkuszy kalkulacyjnych) po najbardziej rozbudowane oparte o zaawansowane mechanizmy bazodanowe.

Jako jednostkę statystyczną w zestawieniach odnoszących się do stopnia realizacji technicznych warunków przetwarzania danych, przyjęto kontrolowany system informatyczny.

Gdy system informatyczny posiadał wymaganą funkcjonalność lub funkcjonalność ta była realizowana przy użyciu dedykowanych modułów programowych, zgodnie z warunkami określonymi w § 7 ust. 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, poszczególne warunki uznawano dla systemu objętego kontrolą jako wypełnione. Stopień realizacji wymogów o charakterze techniczno-organizacyjnym dla systemów informatycznych objętych kontrolą w roku 2010 na tle lat 2007-2009, przedstawiono na poniższym diagramie (Wykres 7).



**Wykres 7: Stopień realizacji wymogów technicznych i organizacyjnych w latach 2007-2010.**

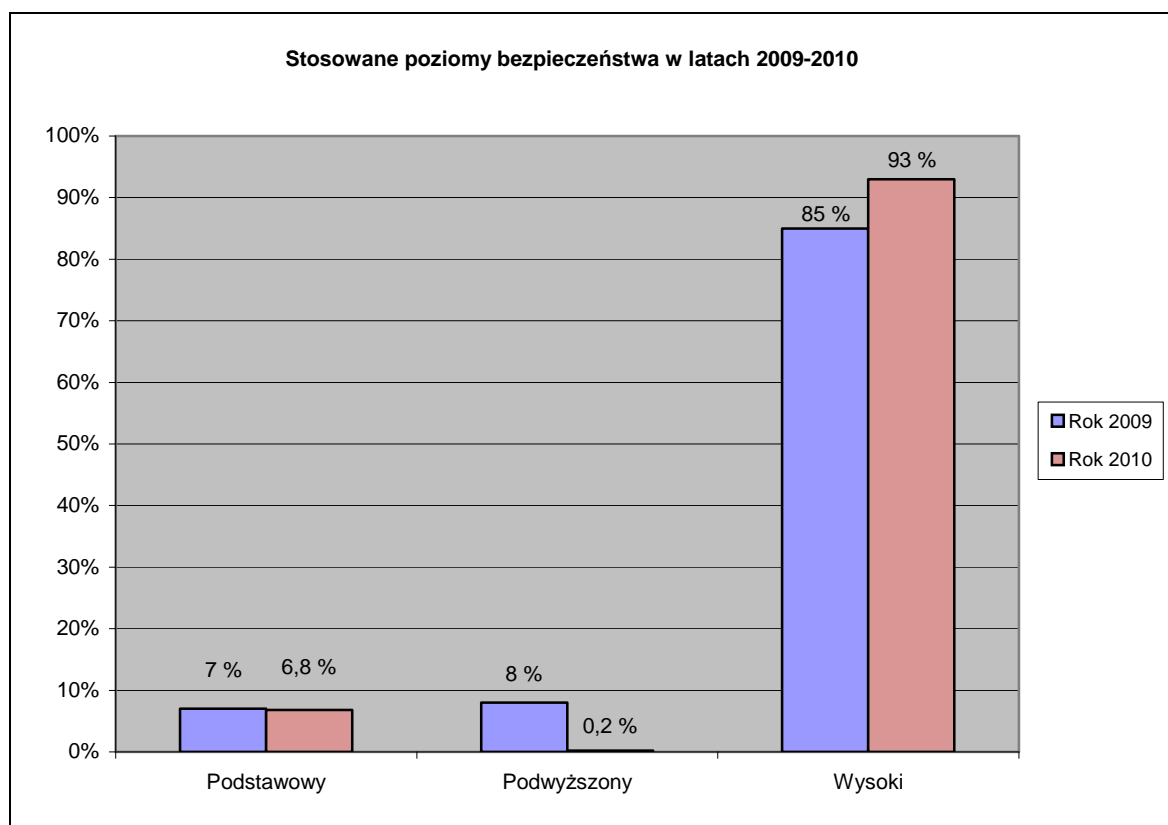
Jak wynika z przedstawionego wykresu, liczba systemów informatycznych objętych kontrolą w roku 2010 była większa niż w latach poprzednich. Spowodowane było to tym, że przeprowadzane w 2010 r. kontrole sektorowe obejmowały m.in. urzędy kontroli skarbowej, towarzystwa ubezpieczeniowe, szkoły wyższe, firmy inwestycyjne prowadzące działalność maklerską oraz komunalne jednostki organizacyjne, w których do przetwarzania danych osobowych używanych było od kilku do kilkunastu systemów informatycznych. W znacznym stopniu liczba ta wynika również z ukierunkowania niektórych kontroli na zagadnienia związane z procesami wymiany danych pomiędzy różnymi instytucjami, jak np. w przypadku urzędów kontroli skarbowej, gdzie prawie

w każdym urzędzie kontrolowanych było od kilku do kilkunastu systemów, z których każdy służył do wymiany danych z inną instytucją. Podobnie było w sektorze ubezpieczeniowym, gdzie kontrole ukierunkowane były na weryfikację systemów służących do wymiany danych pomiędzy różnymi podmiotami. Specyfika ta zwiększyła wydatnie liczbę sprawdzanych systemów informatycznych. Jednocześnie zauważono trend polegający na stosowaniu do przetwarzania danych osobowych wyspecjalizowanych systemów informatycznych, które często służą do przetwarzania kilku różnych zbiorów danych osobowych.

Przeprowadzone czynności kontrolne pokazują również, że niemal 100% kontrolowanych jednostek przetwarza dane osobowe z wykorzystaniem systemów informatycznych. Przypadki przetwarzania danych osobowych wyłącznie w formie tradycyjnej (papierowej) dotyczyły jedynie kilku skontrolowanych podmiotów.

### 2.5.1. Ocena poziomu bezpieczeństwa

W odniesieniu do skontrolowanych w 2010 r. systemów informatycznych podział na poziomy bezpieczeństwa przedstawiony został na poniższym diagramie (Wykres 8).



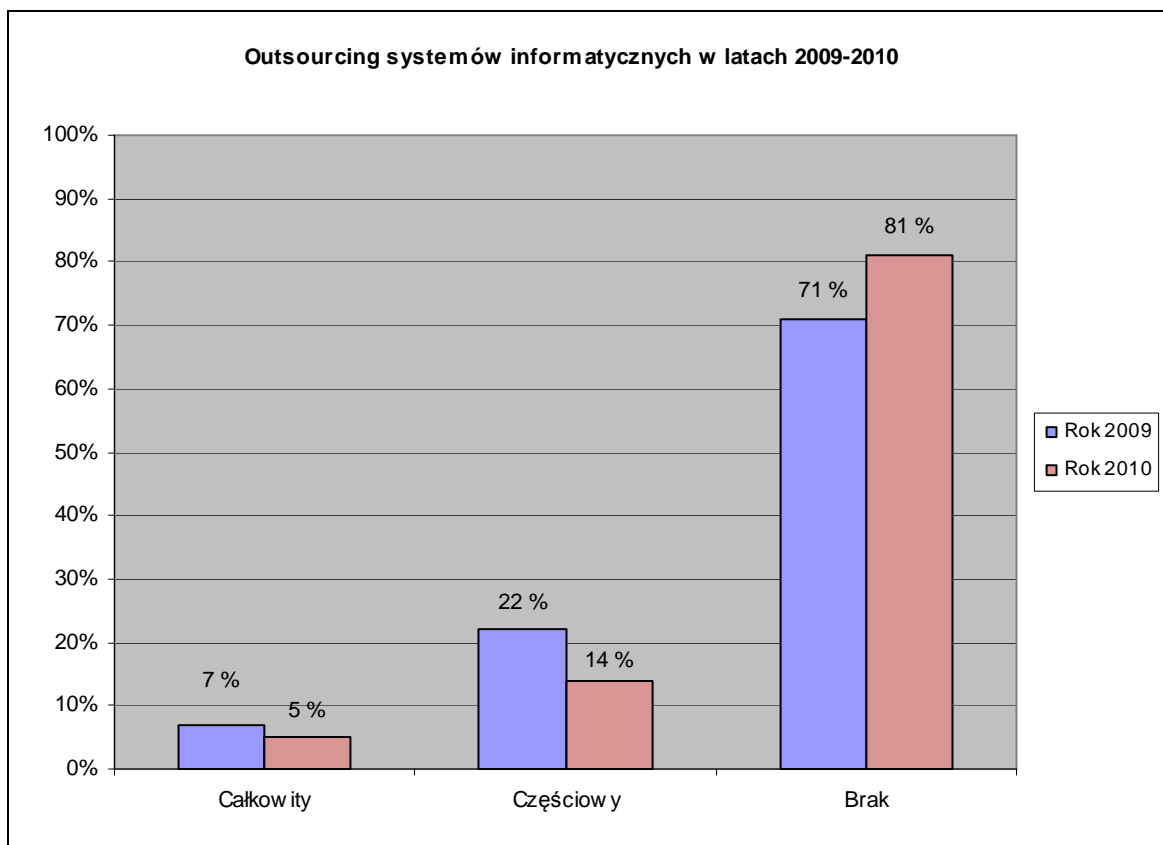
Wykres 8: *Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych skontrolowanych w latach 2009-2010.*

Jak wynika z ww. podziału, 93 % podmiotów skontrolowanych w 2010 r. zastosowało wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Jest to w głównym stopniu związane z tym, że coraz więcej systemów informatycznych posiada dostęp do publicznej sieci Internet, skutkujący koniecznością stosowania zabezpieczeń na poziomie wysokim. Zauważono również tendencję do zwiększania poziomu bezpieczeństwa z podwyższonego na wysoki. Natomiast procentowy udział zabezpieczeń na poziomie podstawowym pozostał praktycznie bez zmian.

### **2.5.2. Outsourcing i kolokacja danych**

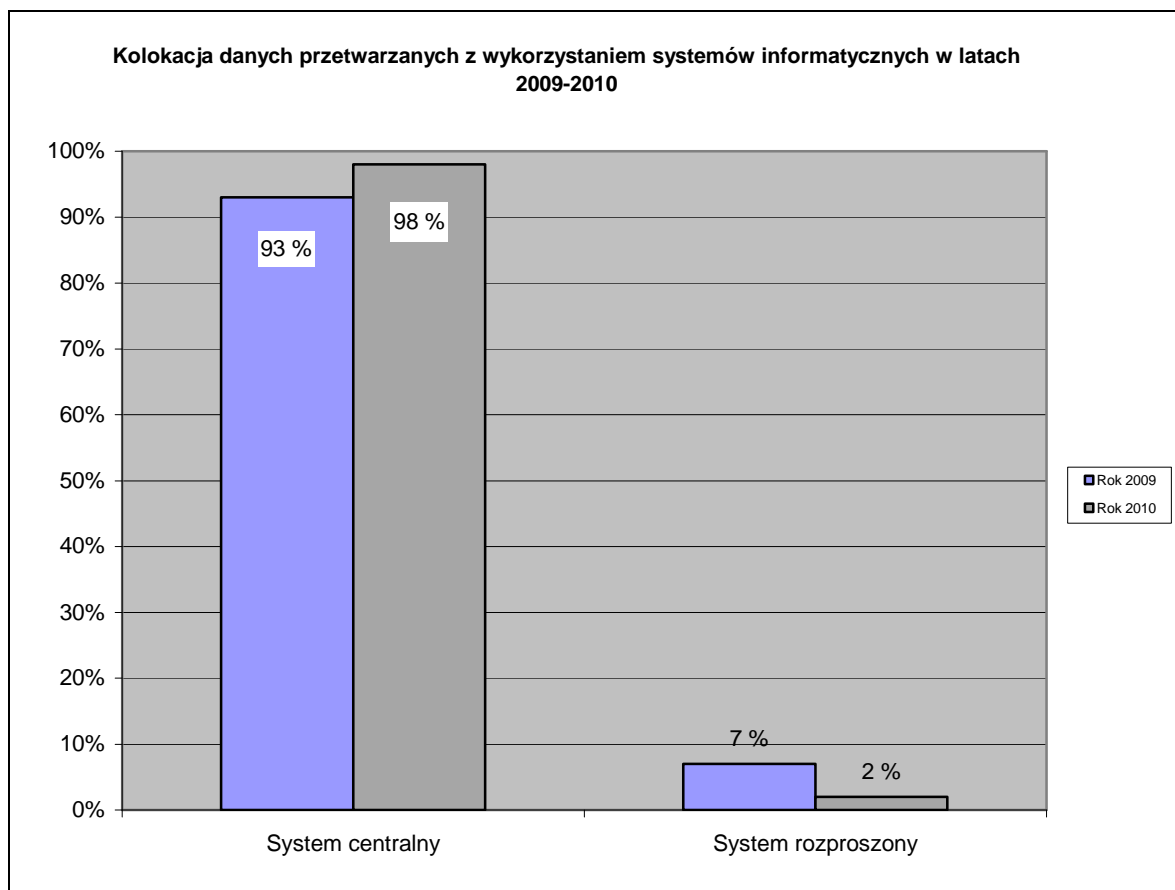
W 2010 r. około 5 % skontrolowanych systemów informatycznych użytkowanych było na zasadzie całkowitego outsourcingu, gdzie proces przetwarzania danych osobowych, jak również oprogramowanie i sprzęt teleinformatyczny, administrator danych powierzył w całości do administrowania podmiotom zewnętrznym. W 81 % systemów informatycznych, jakie poddano kontroli w 2010 r., przetwarzaniem danych osobowych w tych systemach, ich obsługą techniczną i administracją zajmowali się pracownicy administratora danych. Zmniejszyła się natomiast w porównaniu do 2009 r. liczba systemów objętych częściowym outsourcingiem, gdzie podmiotom zewnętrznym powierzano tylko niektóre aspekty związane z utrzymywaniem systemu typu kolokacja maszyn stanowiących platformę sprzętową dla użytkowanych systemów informatycznych, czy wykonywanie czynności administracyjnych, typu zarządzanie bazą danych, wykonywanie kopii zapasowych, itp. Outsourcing częściowy stosowany był w 14% skontrolowanych w 2010 r. systemów.

Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2009-2010 przedstawiono na poniższym diagramie (*Wykres 9*). Opisywane zmiany parametrów nie muszą jednak oddawać tendencji rynkowych i mogą być związane z charakterem podmiotów poddanych kontroli w 2010 r.



**Wykres 9: Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2009-2010.**

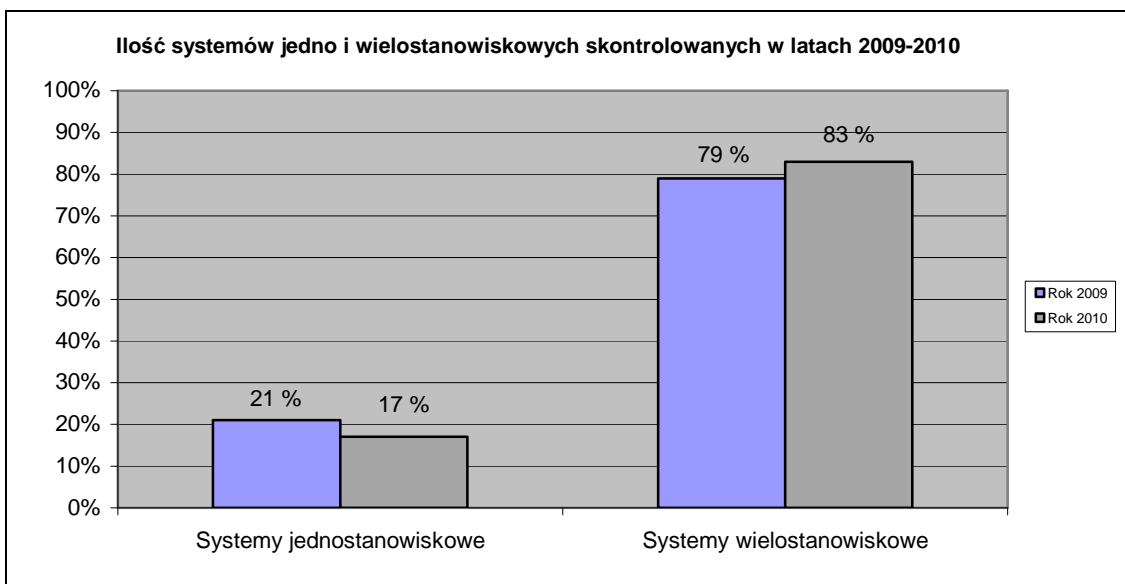
Analiza przetwarzania danych osobowych pod kątem fizycznej lokalizacji danych wykazała, że u większości skontrolowanych podmiotów dane osobowe zapisywane były w jednym, centralnym miejscu, np. na serwerze/serwerach znajdujących się w jednym budynku, zazwyczaj w siedzibie kontrolowanego podmiotu. Tylko w nielicznych przypadkach zastosowano zabezpieczenia odnoszące się do ciągłości przetwarzania i bezpieczeństwa danych poprzez stosowanie zapasowych centrów przetwarzania zlokalizowanych w odrębnej lokalizacji. Poniżej przedstawiono diagram (Wykres 10) ilustrujący stopień stosowania przez kontrolowane podmioty rozwiązań technicznych opartych o systemy centralne i rozproszone.



*Wykres 10: Ilościowy udział centralnego i rozproszonego przetwarzania danych w systemach informatycznych objętych kontrolą w latach 2009-2010.*

### **2.5.3. Systemy sieciowe i wielostanowiskowe**

Jak przedstawiono na poniższym diagramie (*Wykres 11*), w 2010 r. w porównaniu z rokiem 2009 zwiększyła się liczba wielostanowiskowych systemów informatycznych (około 98 %). Rozwiązania oparte o systemy jedno stanowiskowe stanowiły zaledwie 2 % skontrolowanych systemów informatycznych. Zastosowanie systemów jedno stanowiskowych w większości przypadków dotyczyło przestarzałych rozwiązań informatycznych. Zauważyć jednak należy, że systemy jedno stanowiskowe stosowano również w przypadkach, gdy wymagały tego zwiększone względy bezpieczeństwa, np. przetwarzanie danych niejawnych.



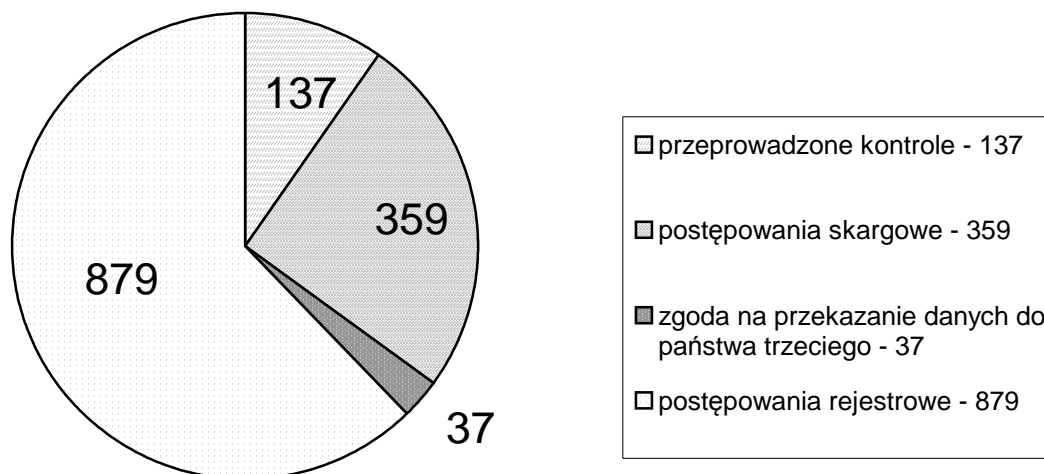
Wykres 11: *Procentowy udział systemów informatycznych jedno- i wielostanowiskowych wśród systemów objętych kontrolą w latach 2009-2010.*

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

#### 3.1. Wydawanie decyzji

Postępowanie wszczęte przez Generalnego Inspektora z urzędu lub na wniosek osoby zainteresowanej dotyczące naruszenia ustawy o ochronie danych osobowych, toczy się według przepisów Kodeksu postępowania administracyjnego. Postępowanie to może zakończyć się wydaniem decyzji administracyjnej nakazującej administratorowi danych przywrócenie stanu zgodnego z prawem poprzez usunięcie uchybień, uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie albo usunięcie danych osobowych, zastosowanie dodatkowych środków zabezpieczających zgromadzone dane, wstrzymanie przekazania ich za granicę, zabezpieczenie danych lub przekazanie ich innym podmiotom.

W 2010 r. Generalny Inspektor wydał **1412 decyzji administracyjnych**, tj. o 64 więcej w stosunku do roku 2009, w którym wydanych było 1348 decyzji. Spośród 1412 decyzji wydanych w 2010 r. **879** dotyczyło postępowań rejestrowych, **137** zostało wydanych w związku z przeprowadzonymi kontrolami, **359** wydano na skutek postępowania zainicjowanego skargą, zaś **37** dotyczyło zgody na przekazanie danych do państwa trzeciego.



Wykres 12: *Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2010 r.*

### 3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa

W analizowanym roku sprawozdawczym 2010 Generalny Inspektor Ochrony Danych Osobowych skierował do organu powołanego do ścigania przestępstw **23 zawiadomienia o podejrzeniu popełnienia przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych**. Niezmiennie najwięcej zawiadomień złożonych zostało w związku z informacjami przekazanymi Generalnemu Inspektorowi Ochrony Danych Osobowych przez podmioty indywidualne - **18 zawiadomień**. Należy tutaj podkreślić, że na tę ogólną liczbę 18 zawiadomień skierowanych do organów ścigania, 10 z nich dotyczyło podejrzenia popełnienia przestępstwa z użyciem Internetu<sup>39</sup>. Pozostałe 8 przypadków dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego w art. 49 ust. 1 ustawy, przetwarzania danych osobowych przez podmioty nieuprawnione. Ponadto w jednym z przypadków dodatkową przyczyną złożenia zawiadomienia było udostępnienie danych osobowych podmiotom nieuprawnionym (art. 51 ust. 1 ustawy). W pozostałych przypadkach przedmiotem zawiadomień uczyniono podejrzenie popełnienia przestępstwa bezpodstawnego przetwarzania danych osobowych w celach marketingowych<sup>40</sup>, próbę sprzedaży zbioru danych towarzystwu emerytalnemu zawierającego informacje o osobach fizycznych, które nie wybrały jeszcze obowiązkowego funduszu emerytalnego<sup>41</sup> oraz udostępnienie osobom

<sup>39</sup> DOLiS/ZAW-3/10, DOLiS/ZAW-7/10, DOLiS/ZAW-11/10, DOLiS/ZAW-12/10, DOLiS/ZAW-15/10, DOLiS/ZAW-16/10, DOLiS/ZAW-17/10, DOLiS/ZAW-18/10, DOLiS/ZAW-3/10/2645, DOLiS/ZAW-15/10/29889.

<sup>40</sup> Zawiadomienie z dnia 17 lutego 2010 r. DOLiS/ZAW-5/10/6815.

<sup>41</sup> Zawiadomienie z dnia 11 stycznia 2010 r. DOLiS/ZAW-2/917/10.



nieupoważnionym danych osobowych poprzez zamieszczenie ich na tablicach ogłoszeń znajdujących się na terenie ogrodu działkowego<sup>42</sup>.

Natomiast **5 zawiadomień miało związek z przeprowadzonymi kontrolami**. W dwóch przypadkach zawiadomienia dotyczyły przestępstwa wskazanego w art. 49 ustawy o ochronie danych osobowych<sup>43</sup>. W toku kontroli ustalono, że jednostki kontrolowane przetwarzały dane osobowe, do przetwarzania których nie były uprawnione. W jednym z ww. przypadków kontrola wykazała, że podmiot występujący jako agencja pracy tymczasowej, przetwarzał bez podstawy prawnej dane osobowe kandydatek na matki zastępcze (surogatki) oraz dane osób zainteresowanych ich wynajęciem. W opinii organu ds. ochrony danych osobowych tego typu działalność nie może być kwalifikowana jako świadczenie usług w zakresie pracy tymczasowej. Natomiast drugi przypadek dotyczył przetwarzania danych osobowych pacjentów przez podmiot, który nie został wpisany do rejestru zakładów opieki zdrowotnej. Brak tego wpisu oznaczał, że wskazany podmiot nie był uprawniony do przetwarzania danych dotyczących stanu zdrowia ww. osób.

W jednym przypadku ustalenia kontrolne uzasadniły złożenie zawiadomienia o podejrzeniu popełnienia przestępstwa określonego w art. 52 ustawy o ochronie danych osobowych<sup>44</sup>. Zawiadomienie to dotyczyło niezabezpieczenia przez pracodawcę dokumentacji zawierającej dane osobowe pracowników. W innym przypadku Generalny Inspektor stwierdził wypełnienie znamion czynu zabronionego wskazanego w art. 53 ustawy o ochronie danych osobowych, tj. niezgłoszenia do rejestracji Generalnemu Inspektorowi zbioru danych użytkowników serwisu internetowego<sup>45</sup>.

Na skutek przeprowadzonych czynności kontrolnych w jednym z podmiotów stwierdzono wypełnienie znamion czynów zabronionych określonych w art. 49, 52, 53 i 54 ustawy o ochronie danych osobowych<sup>46</sup>. Uchybienia uzasadniające skierowanie zawiadomienia o popełnieniu ww. przestępstw polegały m.in. na przetwarzaniu przez pracodawcę bez podstawy prawnej danych osobowych pracowników dotyczących informacji o nałogach, karalności, stanie zdrowia, zachowaniu w miejscu pracy, komunikatywności, a także na braku dokumentacji stanowiącej politykę bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, niezgłoszeniu do rejestracji zbioru danych osobowych pracowników innych podmiotów (usługobiorców) oraz niedopełnieniu wobec osób, których dane osobowe dotyczą, obowiązku poinformowania o ich prawach lub przekazania tym osobom informacji umożliwiających korzystanie z praw przyznanych im w ustawie o ochronie danych osobowych.

---

<sup>42</sup> Zawiadomienie z dnia 4 stycznia 2010 r. DOLiS/ZAW-1/10/91.

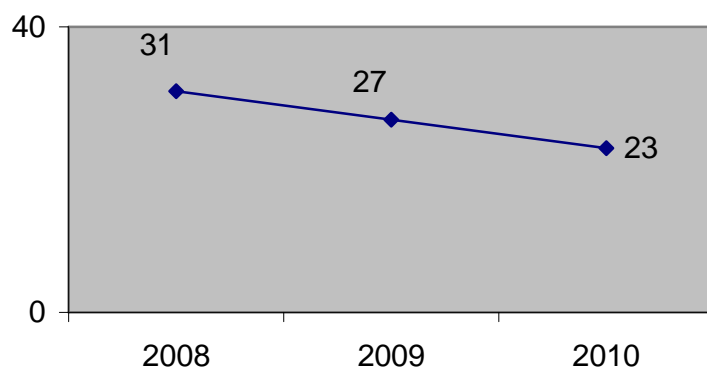
<sup>43</sup> DIS/ZAW-9/14956/10 i DIS/ZAW-14/24571/10.

<sup>44</sup> DIS/ZAW-6/7473/10

<sup>45</sup> DIS/ZAW-4/4295/10

<sup>46</sup> DIS/ZAW-8/11530/10

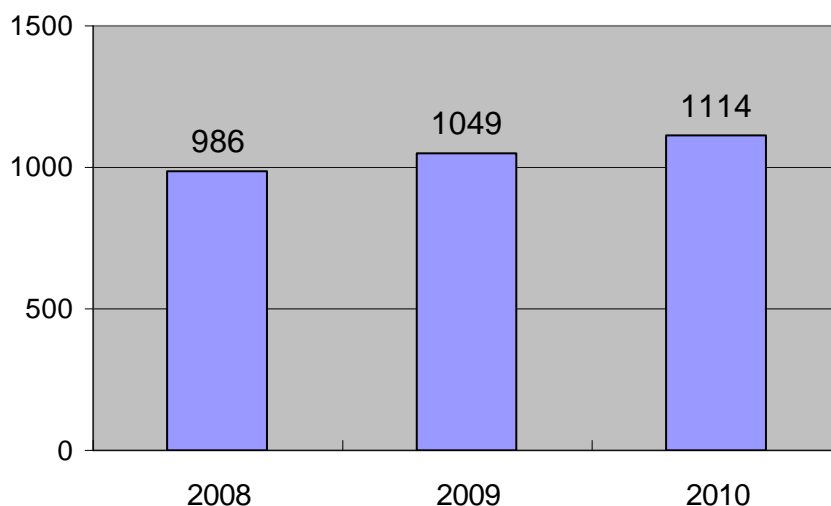
Liczbę **zawiadomień o podejrzeniu popełnienia przestępstwa** składanych przez Generalnego Inspektora w latach 2008–2010 przedstawia Wykres 13.



Wykres 13: *Porównanie liczby zawiadomień o podejrzeniu popełnienia przestępstwa kierowanych przez GODO w latach 2008–2010.*

### 3.3. Rozpatrywanie skarg

W 2010 r. do Departamentu Orzecznictwa, Legislacji i Skarg wpłynęło **1114 skarg** dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2009 liczba skarg uległa zwiększeniu o 65, co przedstawia Wykres 14.

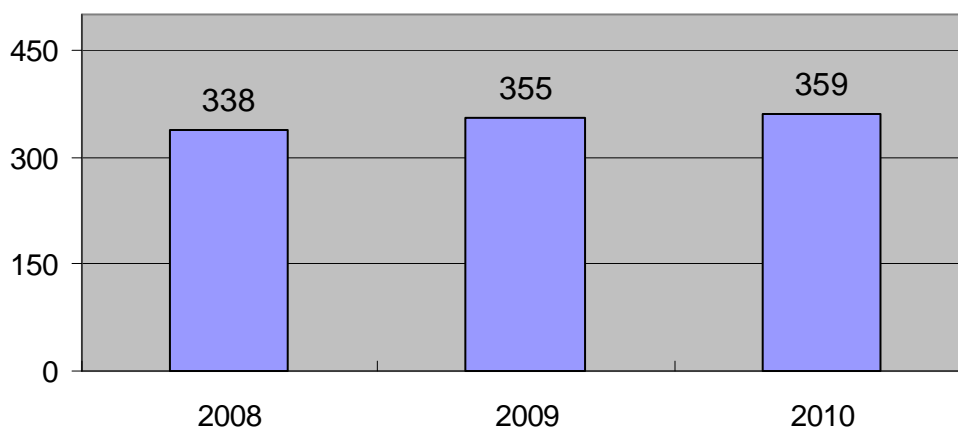


Wykres 14: *Zestawienie porównawcze liczby skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008–2010.*

Każda ze skarg analizowana była na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego. W przypadku tych, które je

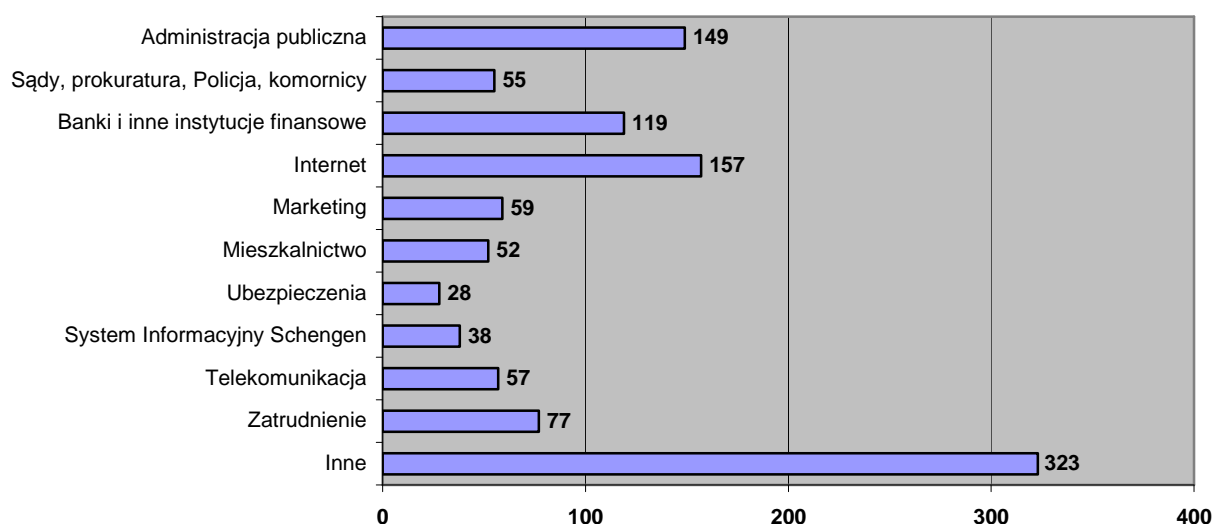
spełniały, GIODO inicjował postępowania administracyjne. Jeżeli w ich toku stwierdzał naruszenie przepisów ustawy o ochronie danych osobowych, wydawał decyzje administracyjne i zgodnie z art. 18 ustawy nakazywał przywrócenie stanu zgodnego z prawem, a w szczególności: 1) usunięcie uchybień, 2) uzupełnienie, 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.

W postępowaniach zainicjowanych tymi skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych z urzędu, wydanych zostało **359 decyzji administracyjnych**, z których **40** zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie [WSA]. (zał. 4). W porównaniu z rokiem 2009, w którym 45 decyzji zostało zaskarżonych, oznacza to spadek o 8,9 %.



*Wykres 15: Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2010 w związku z rozpatrywanymi skargami.*

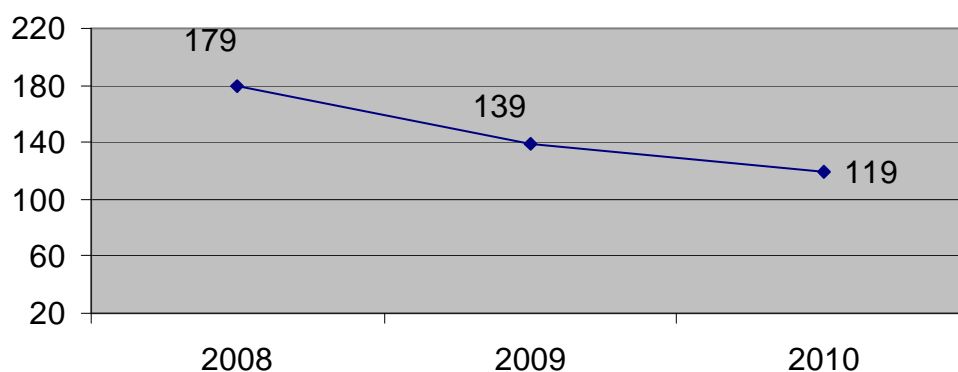
Analizując treść skarg wyróżnić należy 11 kategorii, w zależności od zagadnień, których dotyczyły. Wśród nich znalazły się: 1) administracja publiczna, 2) sądy, prokuratura, Policja, komornicy, 3) banki i inne instytucje finansowe, 4) Internet, 5) marketing, 6) mieszkalnictwo, 7) ubezpieczenia społeczne, majątkowe i osobowe, 8) System Informacyjny Schengen, 9) telekomunikacja, 10) zatrudnienie i 11) inne.



Wykres 16: *Zestawienie porównawcze liczby skarg, które wpłynęły do Biura GODO w 2010 r. w określonych sektorach.*

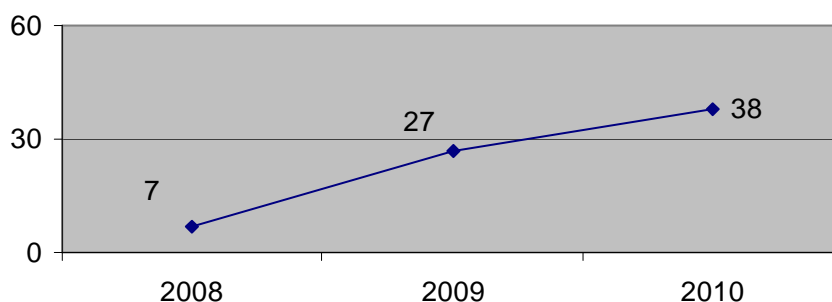
Porównanie liczby skarg w ww. sektorach na przestrzeni lat 2008-2010 pozwala zauważyć dwa interesujące trendy. Pierwszym z nich był znaczący wzrost liczby skarg w sektorze odnoszącym się do Internetu. Dla porównania, w roku 2009 wpłynęło 88 skarg dotyczących działalności podmiotów z tego sektora, zaś w analizowanym 2010 – **157**, czyli o 69 więcej.

Natomiast drugim zauważalnym trendem był stopniowy spadek liczby skarg na podmioty z sektora banków i innych instytucji finansowych. O ile w 2008 r. skarg tych było 179, w 2009 – 139, to w 2010 r. wpłynęło ich już zaledwie 119. W porównaniu do 2008 r. oznacza to spadek liczby skarg o 66 %.



Wykres 17: *Zestawienie porównawcze liczby skarg dotyczących sektora bankowości, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2010.*

Ponadto stale wzrasta liczba skarg na przetwarzanie danych osobowych w Systemie Informacyjnym Schengen, co przedstawia poniższy Wykres 18.



Wykres 18: *Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych osobowych w Systemie Informacyjnym Schengen w latach 2008-2010.*

Z chwilą przystąpienia Polski w dniu 21 grudnia 2007 r. do strefy Schengen, organ ds. ochrony danych rozpoczął sprawowanie kontroli prawidłowości przetwarzania danych osobowych w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej<sup>47</sup>. Wspomniana kontrola odbywa się na zasadach uregulowanych w ustawie o ochronie danych osobowych. Generalny Inspektor Ochrony Danych Osobowych czuwa nad tym, aby przetwarzanie danych gromadzonych w tych systemach nie naruszało praw osób, których dane dotyczą. W sprawach skarg z tego sektora skarżący najczęściej żądali usunięcia dotyczących ich danych osobowych, ponieważ w ich ocenie zostały one bezpodstawnie zamieszczone w tym systemie.

Poniżej przedstawione zostaną przykłady innych skarg, które w 2010 r. wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych. Wśród nich były skargi zawierające zarzut przetwarzania nieaktualnych danych osobowych przez proboszczów **parafii Kościoła Katolickiego**<sup>48</sup>. Skarżący wskazywali w nich, iż pomimo złożenia oświadczenia o wystąpieniu z Kościoła Katolickiego, nie została o tym fakcie zamieszczona stosowna adnotacja w księdze chrztów. Generalny Inspektor Ochrony Danych Osobowych zwracał się w poszczególnych sprawach o wyjaśnienia do odpowiednich podmiotów przetwarzających dane członków lub byłych członków Kościoła Katolickiego. Po uzyskaniu wyjaśnień, z których wynikało, że osoby skarżące są wciąż członkami Kościoła Katolickiego Generalny Inspektor umarzał postępowania administracyjne w takich sprawach wskazując w oparciu o przepis art. 43 ust. 2 ustawy o ochronie danych osobowych na brak swojej kognicji do wydania merytorycznej decyzji administracyjnej w tym względzie<sup>49</sup>. W związku bowiem

<sup>47</sup> 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.

<sup>48</sup> DOLiS-440-588/10, DOLiS-440-632/10, DOLiS-440-693/10, DOLiS-440-663/10, DOLiS-440-771/10, DOLiS-440-793/10, DOLiS-440-810/10, DOLiS-440-845/10, DOLiS-440-858/10, DOLiS-440-859/10, DOLiS-440-872/10, DOLiS-440-973/10, DOLiS-440-884/10, DOLiS-440-954/10, DOLiS-440-958/10, DOLiS-440-985/10.

<sup>49</sup> Decyzja GODO z dnia 15 grudnia 2010 r. DOLiS/DEC-1373/10/49651, 49658, decyzja GODO z dnia 29 grudnia 2010 r. DOLiS/DEC-1402/10/51399,51405, decyzja GODO z dnia 31 grudnia 2010 r. DOLiS/DEC-1425/10/51817,51818, decyzja GODO z dnia 14 stycznia 2011 r. DOLiS/DEC-21/11/1560,1570, decyzja GODO z dnia 20 stycznia 2011 r.

z treścią powołanego przepisu, organ nie może prowadzić postępowania wyjaśniającego ukierunkowanego na wydanie merytorycznej decyzji administracyjnej ani przeprowadzać czynności kontrolnych odnośnie przetwarzania danych osobowych na potrzeby Kościoła Katolickiego, z wyłączeniem prawa żądania złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwania osób w zakresie niezbędnym do ustalenia stanu faktycznego.

W omawianym roku 2010, Generalny Inspektor Ochrony Danych Osobowych - podobnie jak w latach poprzednich – najwięcej wystąpień kierował do podmiotów z sektora **administracji publicznej**, sygnalizując w nich uchybienia, których się dopuścili, np. udostępniając dane osobie nieupoważnionej, poprzez umożliwienie jej wglądu do akt postępowania administracyjnego. GODO podejmował również działania dostosowujące proces przetwarzania danych osobowych w rejestrach publicznych do wymogów określonych przepisami ustawy o ochronie danych osobowych. W tym celu organ wystąpił do Ministra Spraw Wewnętrznych i Administracji o podjęcie działań zapewniających lepszą jakość danych osobowych przetwarzanych w centralnej ewidencji pojazdów, w szczególności ich merytoryczną poprawność<sup>50</sup>.

GODO zwracał się także do Ministra Spraw Wewnętrznych i Administracji o rozważenie zasadności podjęcia działań legislacyjnych mających na celu zmianę przepisów regulujących przetwarzanie danych osobowych w Krajowym Systemie Informacyjnym Policji. Nowelizacja ta miałaby obejmować wprowadzenie do ww. regulacji precyzyjnie określonych okresów, w których Policja może przetwarzać w Krajowym Systemie Informacyjnym Policji pozyskane dane osobowe<sup>51</sup> oraz określających kryteria weryfikacji danych osobowych zawartych w tym systemie<sup>52</sup>. Minister Spraw Wewnętrznych i Administracji bronił poglądu o niezbędności przetwarzania danych osobowych w Krajowym Systemie Informacyjnym Policji w dotychczasowym zakresie. Wskazywane przez Generalnego Inspektora wątpliwości sugerują jednak rozważenie zmian legislacyjnych w najbliższej przyszłości.

Kolejnym obszarem pod względem liczby wystąpień Generalnego Inspektora Ochrony Danych Osobowych spowodowanych uchybieniami w procesie przetwarzania danych osobowych, była działalność **spółdzielni mieszkaniowych i wspólnot mieszkaniowych**. Pomimo sygnalizowania tym podmiotom przez organ w poprzednich latach, konieczności respektowania w ich działalności przepisów ustawy o ochronie danych osobowych, nadal wywieszają one na klatkach schodowych listy dłużników oraz pisma zawierające dane osobowe członków, jak również doręczają korespondencję przez osoby nieposiadające upoważnienia do przetwarzania danych osobowych adresatów.

---

DOLiS/DEC-33/11/2429,2430, decyzja GODO z dnia 25 stycznia 2011 r. DOLiS/DEC-44/11/3079,3082, decyzja GODO z dnia 25 stycznia 2011 r. DOLiS/DEC-45/11/3167,3170.

<sup>50</sup> Pismo GODO z dnia 27 stycznia 2010 r. DOLiS-440-373/09/3742/10.

<sup>51</sup> Pismo GODO z dnia 25 czerwca 2010 r. DOLiS-440-20/10/25634, pismo GODO z dnia 22 września 2010 r. DOLiS-440-696/10/37853.

Liczne były również wystąpienia Generalnego Inspektora Ochrony Danych Osobowych w związku z nieprawidłowościami w przetwarzaniu danych osobowych w celach **marketingowych**. Ich adresatami były przede wszystkim banki oraz operatorzy telekomunikacyjni. Najpowszechniejszym uchybieniem popełnianym przez pracowników banków i operatorów telekomunikacyjnych był brak niezwłocznego odnotowania sprzeciwu podmiotu danych wobec przetwarzanych dotyczących go danych osobowych. Organ ds. ochrony danych osobowych wystąpił również w związku z praktyką prowadzenia przez banki akcji marketingowych, polegających na przesyłaniu swoim klientom niezamawianych przez nich, spersonalizowanych, nieaktywnych kart kredytowych. W sprawie tej GODO zwrócił się do Przewodniczącego Komisji Nadzoru Finansowego o zajęcie stanowiska w sprawie zgodności przedstawionej praktyki z odpowiednimi przepisami prawa<sup>53</sup>. W odpowiedzi Przewodniczący Komisji Nadzoru Finansowego wskazał, iż fakt przesyłania klientowi przez bank karty kredytowej bez zawarcia umowy o kartę kredytową, daje podstawę do stwierdzenia, że bank naruszył art. 21 ustawy o elektronicznych instrumentach płatniczych<sup>54</sup>.

W 2010 r. stałym przedmiotem wystąpień Generalnego Inspektora Ochrony Danych Osobowych było nienależyte dopełnianie obowiązku informacyjnego wynikającego z art. 33 ustawy o ochronie danych osobowych, głównie przez **banki oraz operatorów telekomunikacyjnych**. Administratorzy danych nie przestrzegali 30 dniowego terminu do udzielenia żądanych informacji. Jako drastyczny przykład zaniechania w tym względzie należy wskazać dopełnienie przedmiotowego obowiązku przez jeden z banków po blisko dwóch latach i to wyłącznie na skutek działań podjętych przez Generalnego Inspektora Ochrony Danych Osobowych<sup>55</sup>.

Generalny Inspektor Ochrony Danych Osobowych podejmował również działania mające na celu zapewnienie zgodności treści różnego rodzaju formularzy z regulacjami ustawy o ochronie danych osobowych. Uchybienia w tym obszarze polegały między innymi na niewłaściwym spełnieniu obowiązku informacyjnego z art. 24 ustawy o ochronie danych osobowych albo braku jego spełnienia, niewłaściwym formułowaniu klauzuli zgody na przetwarzanie danych osobowych oraz pozyskiwaniu danych osobowych w zbyt szerokim zakresie. Jednocześnie należy zaznaczyć, iż w omawianym okresie na skutek wystąpień organu ds. ochrony danych osobowych podejmowanych z urzędu, jeden z dostawców paliwa gazowego dostosował treść stosowanych przez niego wzorców formularzy, w tym umowy kompleksowej dostarczania paliwa gazowego, do wymogów ustawy o ochronie danych osobowych poprzez dodanie informacji o braku obligatoryjności podania przez osoby nie prowadzące działalności gospodarczej numeru NIP, adresu do korespondencji, numeru telefonu, adresu poczty

---

<sup>52</sup> Pismo GODO z dnia 1 września 2010 r. DOLiS-440-696/10/34865.

<sup>53</sup> Pismo GODO z dnia 9 marca 2010 r. DOLiS-440-705/09/9960/10.

<sup>54</sup> Pismo KNF z dnia 25 marca 2010 r. DPP-WNB/023/586/2/10/AJ.

<sup>55</sup> Pismo GODO z dnia 27 maja 2010 r. DOLiS-440-23/10/21879.

elektronicznej oraz numeru konta bankowego<sup>56</sup>. Podjęcie z urzędu działań przez Generalnego Inspektora Ochrony Danych Osobowych wobec tego podmiotu było jak najbardziej zasadne ze względu na znaczną liczbę osób fizycznych korzystających z jego usług.

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

Jednym z podstawowych zadań Generalnego Inspektora Ochrony Danych Osobowych jest prowadzenie ogólnokrajowego, jawnego rejestru zbiorów danych osobowych. Z zadaniem tym skorelowany jest obowiązek zgłaszania zbiorów danych osobowych przez administratorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych<sup>57</sup>. Wskazane powyżej zadanie realizowane jest w Departamencie Rejestracji Zbiorów Danych Osobowych Biura GODO. Nałożenie na administratorów danych obowiązku zgłoszenia zbioru danych do rejestracji umożliwia Generalnemu Inspektorowi Ochrony Danych Osobowych sprawowanie kontroli zgodności procesu przetwarzania danych osobowych w zgłoszonych zbiorach z zasadami przyjętymi w ustawie. Informacje uzyskane w toku postępowania rejestracyjnego stanowią dla organu podstawowe źródło wiedzy na temat administratorów danych, prowadzonych przez nich zbiorów danych oraz warunków przetwarzania danych w tych zbiorach. Posiadanie wymienionych informacji pozwala zdefiniować problemy występujące w procesie przetwarzania danych w określonych obszarach i podjąć działania zmierzające do przywrócenia stanu zgodnego z prawem.

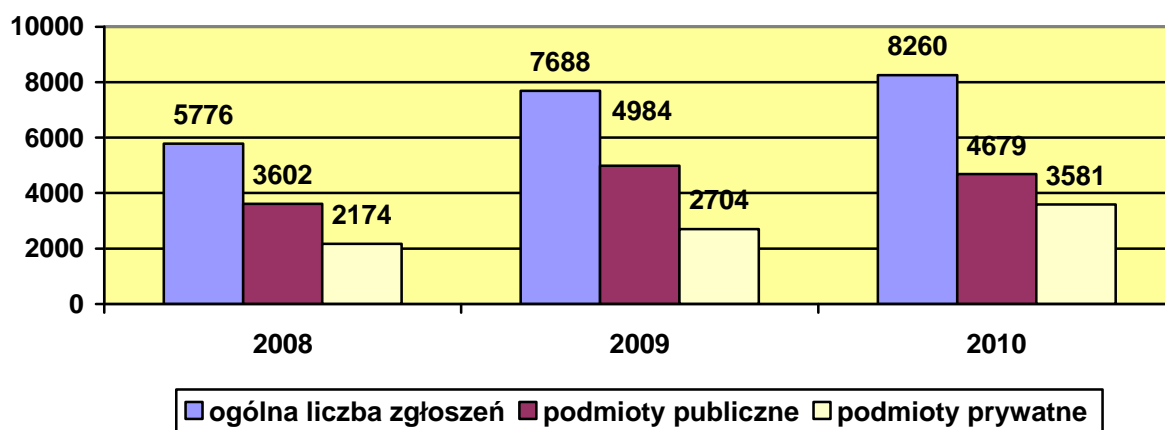
W roku 2010 r. administratorzy danych zgłosili do rejestracji **8260 zbiorów**, z czego podmioty z sektora administracji publicznej zgłosiły 4679 zbiorów, co stanowi 57 % ogólnej liczby zgłoszeń dokonanych w tym okresie, zaś podmioty z sektora prywatnego 3581 zbiorów, co stanowi 43 % ogólniej liczby zgłoszonych zbiorów.

---

<sup>56</sup> DOLiS-440-269/09

<sup>57</sup> 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 19: *Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2008 -2010.*

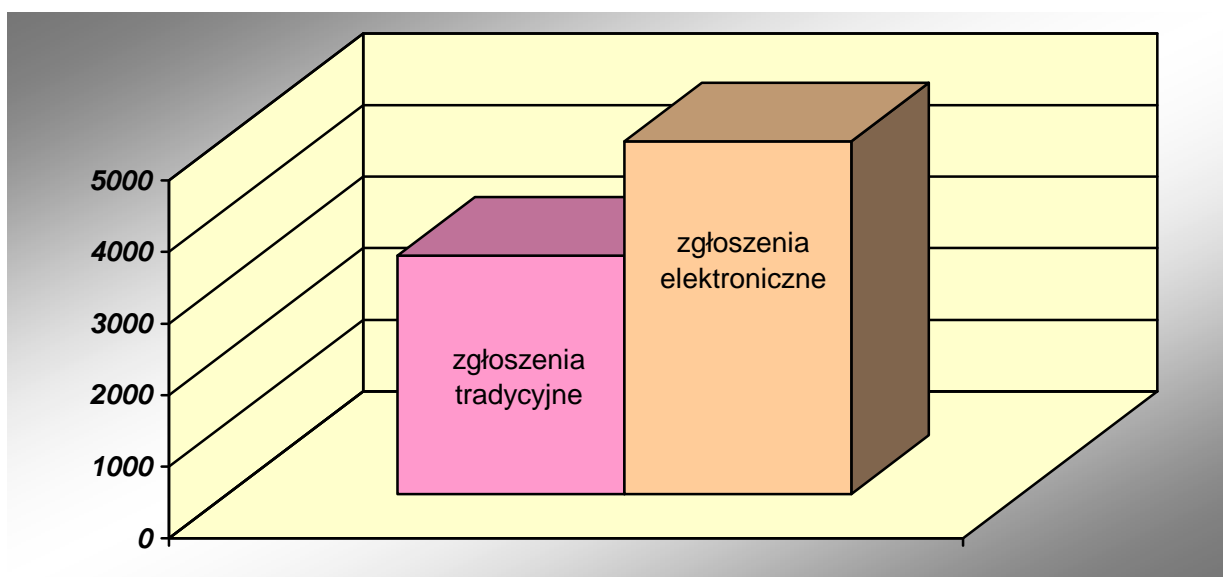
Analizując przedstawione powyżej zestawienie, oprócz stale rosnącej ogólnej liczby zgłoszeń, zauważyć należy wzrost liczby zgłoszeń dokonanych przez podmioty prywatne. Wynika to przede wszystkim z rozwoju świadomości prawnej społeczeństwa w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych, w tym także obowiązku rejestracji zbiorów danych osobowych. Na taki stan rzeczy niewątpliwie zasadniczy wpływ miała działalność edukacyjna Generalnego Inspektora. Ponadto, dzięki możliwości realizacji obowiązku rejestracji drogą elektroniczną, zgłaszanie zbiorów stało się łatwiejsze i szybsze.

Wśród podmiotów z sektora publicznego najwięcej zbiorów zgłosiły do rejestracji, podobnie jak w latach ubiegłych, jednostki samorządu terytorialnego (gminy, powiaty), a także podmioty realizujące zadania z zakresu pomocy społecznej (ośrodki pomocy społecznej, powiatowe centra pomocy rodzinie) oraz jednostki oświatowe (przedszkola, szkoły). Natomiast wśród podmiotów prywatnych, tak jak w poprzednich latach, najwięcej zbiorów zgłosiły te, które do przetwarzania danych osobowych wykorzystują sieć Internet.

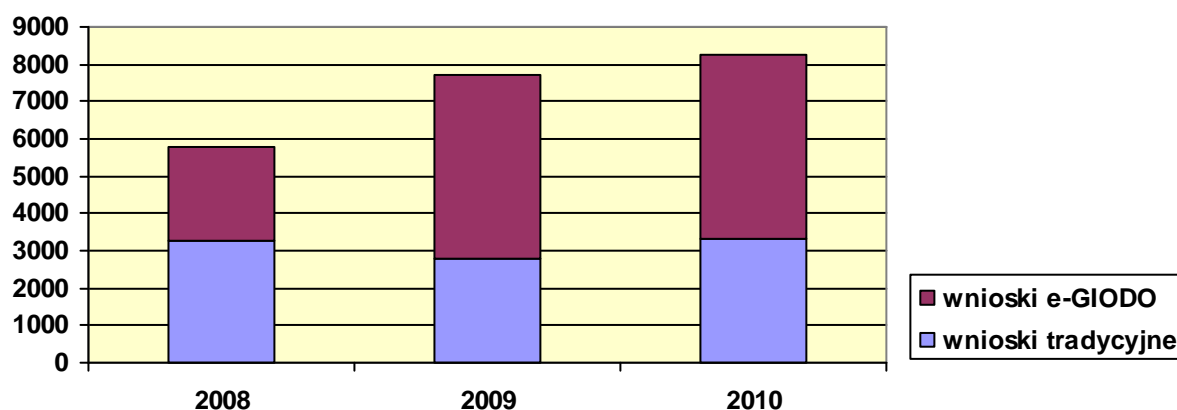
Jak wspomniano powyżej systematycznie rośnie liczba zgłoszeń, które wpływają do Biura Generalnego Inspektora Ochrony Danych Osobowych. W zrealizowaniu obowiązku rejestracji niewątpliwie pomocny jest program komputerowy służący do prawidłowego wypełnienia zgłoszenia zbioru danych do rejestracji, udostępniony na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych. Program ten, wraz z internetową wersją rejestru zbiorów danych osobowych, funkcjonuje w ramach systemu „Elektroniczna platforma komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych” (w skrócie e-GIODO). Program ten został opracowany na podstawie dotychczasowych doświadczeń Departamentu Rejestracji Zbiorów Danych Osobowych Biura GIODO, z uwzględnieniem najczęstszych błędów popełnianych przez wnioskodawców przy wypełnianiu zgłoszenia. Celem programu jest wyeliminowanie - dzięki systemowi podpowiedzi i komunikatów -

możliwości popełnienia tych błędów. Istotą programu jest to, że wymusza podanie wszystkich informacji, które zgodnie z przepisami prawa powinno zawierać zgłoszenie oraz ogranicza możliwość podania informacji nieprecyzyjnych lub sprzecznych. Po wypełnieniu formularza wnioskodawca ma możliwość przesłania zgłoszenia zbioru danych osobowych do rejestracji GIODO drogą elektroniczną również wtedy, gdy nie dysponuje bezpiecznym podpisem elektronicznym. Jednakże w takim przypadku powinien opatrzyć wydruk zgłoszenia przesłanego elektronicznie podpisem i pieczętą, a następnie przesać pocztą lub złożyć w siedzibie Generalnego Inspektora. Liczba zgłoszeń wypełnianych za pomocą ww. programu systematycznie rośnie. W roku sprawozdawczym większość administratorów skorzystała z takiego sposobu zgłaszania zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

W omawianym okresie **4929** zgłoszeń dokonano drogą elektroniczną, tj. przy użyciu ww. programu (co stanowi 60 % ogólnej liczby zgłoszeń), w tym **873** zgłoszenia opatrzone były podpisem elektronicznym, co stanowi 18 % wszystkich zgłoszeń przesłanych elektronicznie i 11 % ogólnej liczby zgłoszeń nadesłanych do rejestracji w 2010 r.

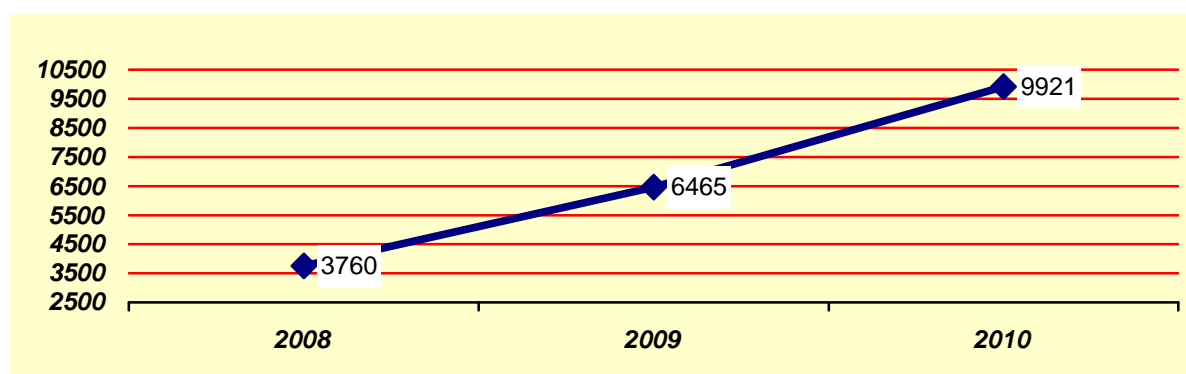


Wykres 20: *Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonywanych w 2010 r. w formie tradycyjnej i elektronicznej.*



Wykres 21: Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2008-2010 w formie tradycyjnej i przy użyciu programu wspomagającego, udostępnionego na stronie [www.giodo.gov.pl](http://www.giodo.gov.pl)

W okresie sprawozdawczym do ogólnokrajowego jawnego rejestru zbiorów danych osobowych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych zostało wpisanych 9921 zbiorów danych.



Wykres 22: Zestawienie porównawcze liczby zarejestrowanych zbiorów danych osobowych w latach 2008 - 2010.

Należy zauważyć, że w roku 2010 zostało zarejestrowanych więcej zbiorów danych osobowych, niż w latach poprzednich. Było to możliwe dzięki temu, iż zgłoszenia nie zawierały aż tak dużej liczby błędów, jak to miało miejsce w latach ubiegłych. Niewątpliwie na taki rezultat wpływ miały dwa czynniki. Pierwszym z nich była przeprowadzona przez Generalnego Inspektora modyfikacja programu komputerowego wspomagającego wypełnianie formularza zgłoszenia, drugim zaś – wprowadzenie od 10 lutego 2009 r. nowego wzoru zgłoszenia.

Dzięki modyfikacji ww. programu administrator może wysłać zgłoszenie drogą elektroniczną również wtedy, gdy nie dysponuje bezpiecznym podpisem elektronicznym. Zmiana ta doprowadziła do

znacznego wzrostu liczby zgłoszeń wypełnianych za pomocą ww. programu. Co więcej, dzięki mechanizmom, w oparciu o które zbudowany jest ten program, udaje się unikać typowych błędów w procesie wypełniania wniosku do rejestracji, co z kolei pozwala szybciej zakończyć postępowania bez konieczności prowadzenia postępowań wyjaśniających. Ponadto informacje zawarte we wnioskach przesłanych elektronicznie trafiają automatycznie do systemu obsługującego ogólnokrajowy rejestr zbiorów danych osobowych, bez konieczności ręcznego wprowadzania danych, co także wpłynęło na przyspieszenie procesu rejestracji.

Również zgłoszenia dokonywane tradycyjnie zawierały mniej błędów niż w latach ubiegłych. Zgłoszenia były bowiem dokonywane na nowym, uproszczonym wzorze. Nowy wzór zgłoszenia, 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<sup>58</sup>. Głównym celem zmiany tego wzoru było uproszczenie części E zgłoszenia dotyczącej informacji o środkach technicznych i organizacyjnych zastosowanych w celu zabezpieczenia danych. Po pełnym roku stosowania nowego wzoru zgłoszenia można stwierdzić, iż cel ten został osiągnięty. Głównym przejawem tego jest wyraźne zmniejszenie liczby nieprawidłowo wypełnionych zgłoszeń – głównie w części E, co z kolei przekłada się na przyspieszenie postępowania rejestracyjnego.

W ramach postępowania prowadzonego w związku ze zgłoszeniem zbioru do rejestracji dokonywana jest szczegółowa analiza i ocena treści zgłoszenia. Należy przede wszystkim ustalić, czy zgłoszenie faktycznie dotyczy zbioru danych, czy zbiór został zgłoszony przez podmiot uprawniony do dokonania takiego zgłoszenia, tj. przez administratora danych, czy ustawa o ochronie danych osobowych ma zastosowanie ze względu na informacje objęte zgłoszeniem oraz podmiot zgłaszający zbiór, a ponadto czy zgłoszony do rejestracji zbiór podlega obowiązkowi rejestracji, tj. czy nie występują przesłanki zwolnienia z obowiązku rejestracji określone w art. 43 ust. 1 ustawy.

Jeśli w trakcie postępowania w sprawie zgłoszenia zbioru do rejestracji stwierdzone zostanie, iż zachodzi jedna z wyżej wymienionych sytuacji uniemożliwiająca zarejestrowanie zbioru danych, wówczas Generalny Inspektor Ochrony Danych Osobowych kieruje do wnioskodawcy pismo informujące o braku podstaw do dokonania wpisów w rejestrze. W roku sprawozdawczym zostało wysłanych **712 takich pism**, w tym **303 pisma** informujące administratorów danych o braku obowiązku rejestracji zbioru, wynikającym z jednej z przesłanek określonych w art. 43 ust. 1 ustawy oraz **409 pism** informujących o braku podstaw do dokonania wpisów w rejestrze z innych przyczyn, niż wynikające z powołanego powyżej przepisu. Pisma te dotyczyły zgłoszeń dokonanych przez podmioty nie będące administratorami danych lub zgłoszeń obejmujących więcej niż jeden zbiór

danych osobowych, a także zgłoszeń dotyczących danych, w stosunku do których przepisy ustawy nie mają zastosowania. Pisma kierowane do administratorów w związku z wystąpieniem przesłanek zwolnienia z obowiązku rejestracji, określonych w art. 43 ust. 1 ustawy, najczęściej dotyczyły zgłoszeń zbiorów pracowników lub osób ubiegających się o zatrudnienie u administratora danych. Wnioskodawcy, którzy nie byli administratorami danych, to zazwyczaj podmioty, którym administratorzy danych powierzyli przetwarzanie danych na podstawie art. 31 ustawy.

Zgłoszenia dotyczące więcej niż jednego zbioru często obejmowały wszystkie zbiory prowadzone w związku z działalnością administratora, np. zbiór danych klientów przetwarzanych w celu realizacji umów oraz zbiór danych pracowników prowadzony w związku z wykonywaniem obowiązków pracodawcy wynikających z Kodeksu pracy<sup>59</sup>. Tymczasem każdy ze zbiorów powinien zostać zgłoszony na odrębnym formularzu zgłoszenia, co wynika wprost z art. 41 ust. 1 ustawy. Zgłoszenia dotyczące danych, do których przetwarzania przepisy ustawy o ochronie danych osobowych nie miały zastosowania, dotyczyły przede wszystkim danych identyfikujących przedsiębiorców w obrocie gospodarczym, ściśle związanych z prowadzoną przez nich działalnością gospodarczą.

Jeżeli zgłoszenie pozytywnie przejdzie opisaną powyżej wstępną weryfikację, to w następnej kolejności w postępowaniu rejestracyjnym ustala się, czy nie zachodzi przesłanka odmowy rejestracji zgłoszonego zbioru. Generalny Inspektor Ochrony Danych Osobowych odmawia bowiem rejestracji zgłoszonego zbioru danych<sup>60</sup>, jeżeli zgłoszenie nie zawiera wszystkich wymaganych informacji, przetwarzanie danych naruszałoby określone w ustawie o ochronie danych osobowych zasady, a ponadto gdy urządzenia i systemy informatyczne służące do przetwarzania zbioru danych nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w rozporządzeniu wykonawczym do ustawy<sup>61</sup>. Zatem w postępowaniu rejestracyjnym ocenie poddawany jest w szczególności zakres przetwarzanych danych, tj. czy jest on adekwatny w stosunku do celu, w jakim prowadzony jest zbiór. Administrator danych zobowiązany jest bowiem gromadzić tylko takiego rodzaju dane, które są niezbędne ze względu na cel ich przetwarzania. Badaniu podlega też legalność przetwarzania danych. W tym celu należy m.in. dokonać analizy przepisów prawa regulujących zadania lub działalność, w związku z realizacją których administrator przetwarza dane osobowe

---

<sup>58</sup> Dz. U. Nr 229, poz. 1536

<sup>59</sup> Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.

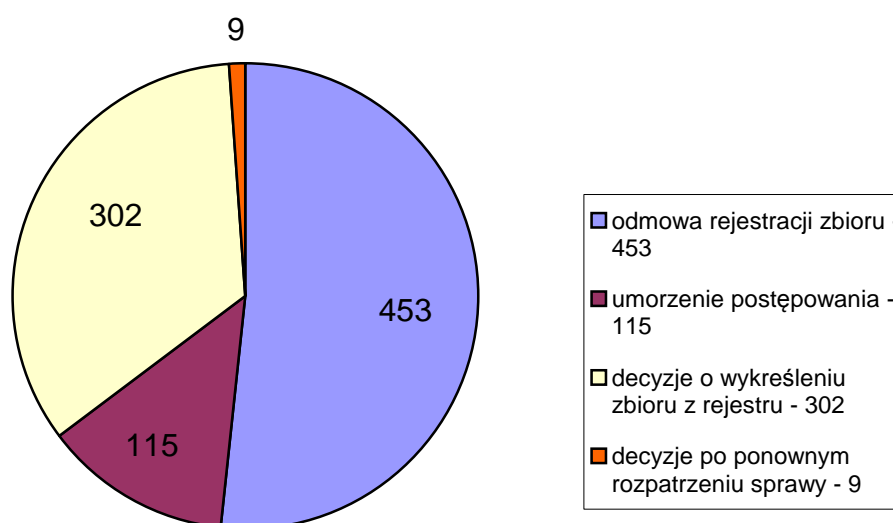
<sup>60</sup> Zgodnie z art. 44 ust. 1 ustawy Generalny Inspektor Ochrony Danych Osobowych odmawia, w drodze decyzji administracyjnej, rejestracji zgłoszonego zbioru danych, jeżeli: nie zostały spełnione wymogi określone w art. 41 ust. 1 ustawy, przetwarzanie naruszałoby zasady określone w art. 23-30 ustawy, urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a ustawy.

<sup>61</sup> 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).

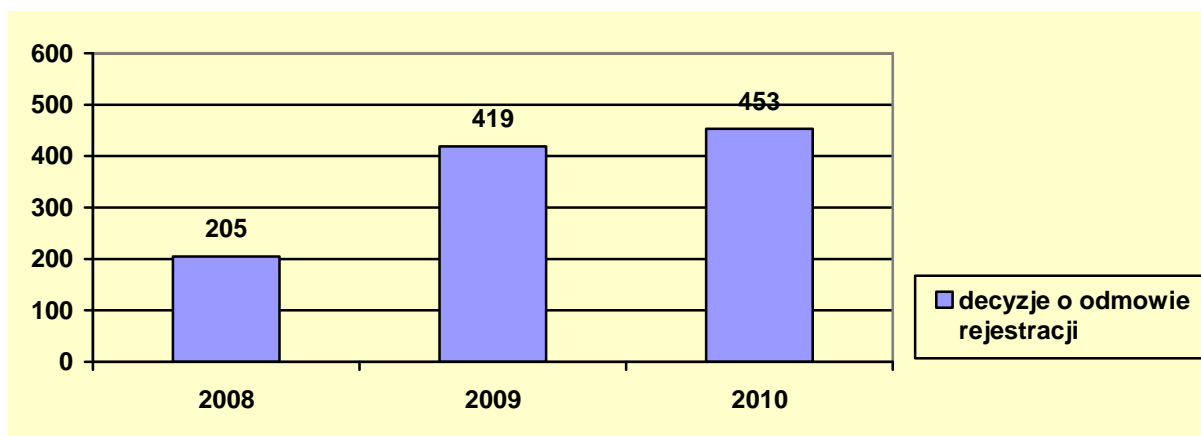
w zbiorze.

Wraz z odmową rejestracji zbioru Generalny Inspektor nakazuje ograniczenie przetwarzania danych wyłącznie do ich przechowywania lub zastosowanie innych środków, określonych w art. 18 ustawy, np. usunięcie uchybień, zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe, a nawet usunięcie danych osobowych. Zatem skutki odmowy rejestracji mogą mieć negatywny wpływ na całą działalność wnioskodawcy, często wręcz uniemożliwiając jej kontynuowanie. Zagrożenie negatywnymi konsekwencjami związanymi z odmową rejestracji zbioru danych niewątpliwie mobilizuje administratorów danych do tego, aby przed zgłoszeniem dokonali oceny, czy spełnione są wszystkie wymagania przewidziane w ustawie o ochronie danych osobowych.

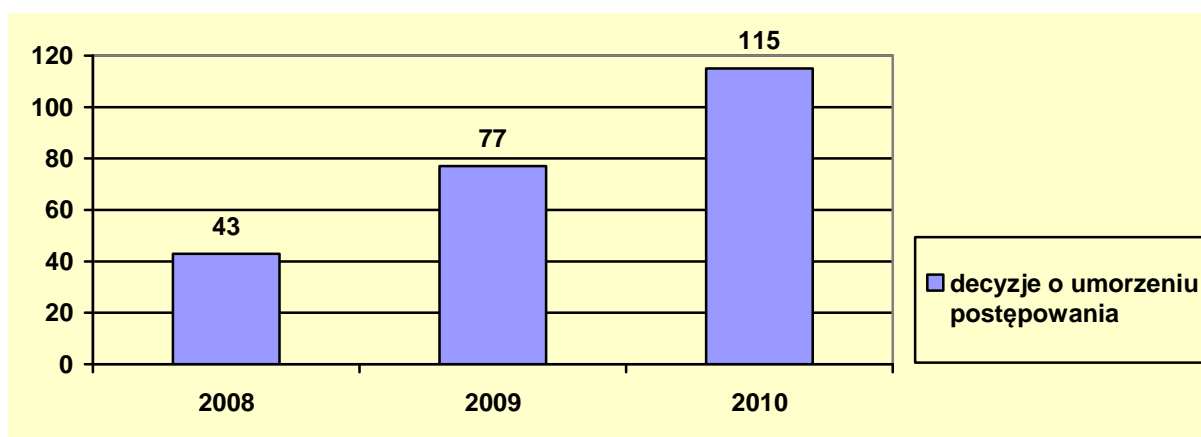
W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **453 decyzje o odmowie rejestracji zbioru danych, 115 decyzji o umorzeniu postępowania, 302 decyzje o wykreśleniu zbioru danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych oraz 9 decyzji po ponownym rozpatrzeniu sprawy** dotyczącej odmowy rejestracji zbioru.



**Wykres 23: Liczbowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2010 r.**



Wykres 24: Zestawienie porównawcze decyzji o odmowie rejestracji zbioru wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2010.



Wykres 25: Zestawienie porównawcze decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2010.

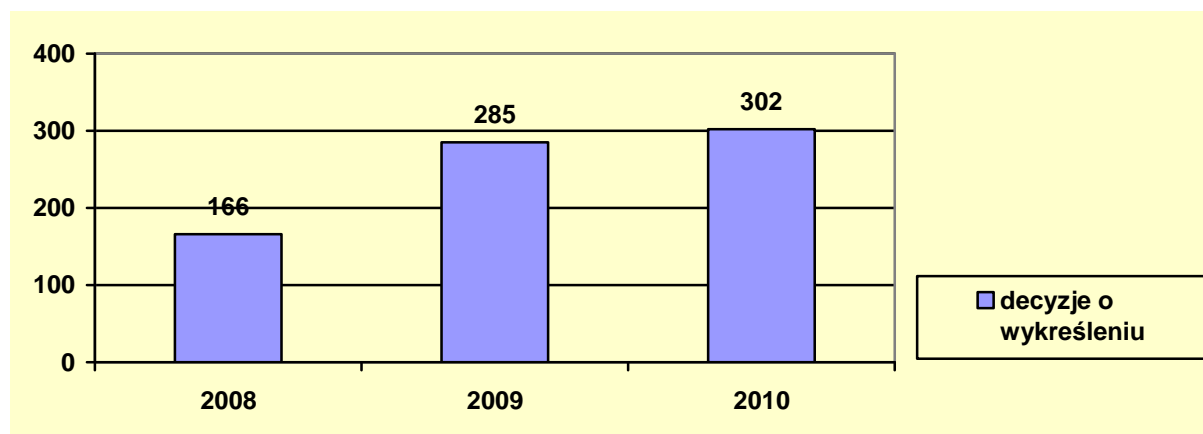
Należy zauważyć, że nie zawsze informacje zawarte w zgłoszeniu pozwalają na zakończenie sprawy bez przeprowadzenia postępowania wyjaśniającego. Wówczas Generalny Inspektor Ochrony Danych Osobowych zwraca się do wnioskodawcy o złożenie dodatkowych wyjaśnień lub dowodów.

W 2010 roku w toku postępowań rejestracyjnych do wnioskodawców skierowano **1828 pism**, w których Generalny Inspektor Ochrony Danych Osobowych zwracał się o złożenie pisemnych wyjaśnień lub informował o przesłankach odmowy rejestracji zbioru danych oraz o uprawnieniach strony przed wydaniem decyzji administracyjnej. Ponadto w 2010 roku skierowano do wnioskodawców, na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego, **1267 wezwań** do uzupełnienia w zgłoszeniu braku podpisu lub braku potwierdzenia umocowania wnioskodawcy do reprezentowania administratora danych.

Rejestr zbiorów danych osobowych spełnia przypisane mu funkcje tylko wówczas, gdy jest

zgodny ze stanem rzeczywistym, a zatem zawiera aktualne informacje o istniejących zbiorach. Aktualności rejestru służy zarówno nałożony na administratorów obowiązek zgłaszania Generalnemu Inspektorowi Ochrony Danych Osobowych każdej zmiany informacji, o których mowa w art. 41 ust. 1 ustawy<sup>62</sup>, jak również instytucja wykreślenia. Obie te instytucje stwarzają możliwość porządkowania rejestru, zgodnie ze zmieniającymi się okolicznościami przetwarzania danych.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **302 decyzje o wykreśleniu** zbioru danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych. Wnioski o wykreślenie były kierowane w związku z zaprzestaniem przetwarzania danych osobowych. Zgodnie z art. 44a pkt 1 ustawy wykreślenie z rejestru jest dokonywane w drodze decyzji administracyjnej, jeżeli zaprzestano przetwarzania danych w zarejestrowanym zbiorze. Nie wszystkie kierowane przez administratorów wnioski o wykreślenie zbioru były zasadne, bowiem wielu administratorów danych mylnie interpretując pojęcie przetwarzania danych występowało o wykreślenie zbioru, w którym nadal przetwarzane były dane osobowe w celach archiwalnych. Tymczasem przechowywanie danych jest zgodnie z definicją ustawową jedną z form przetwarzania danych.



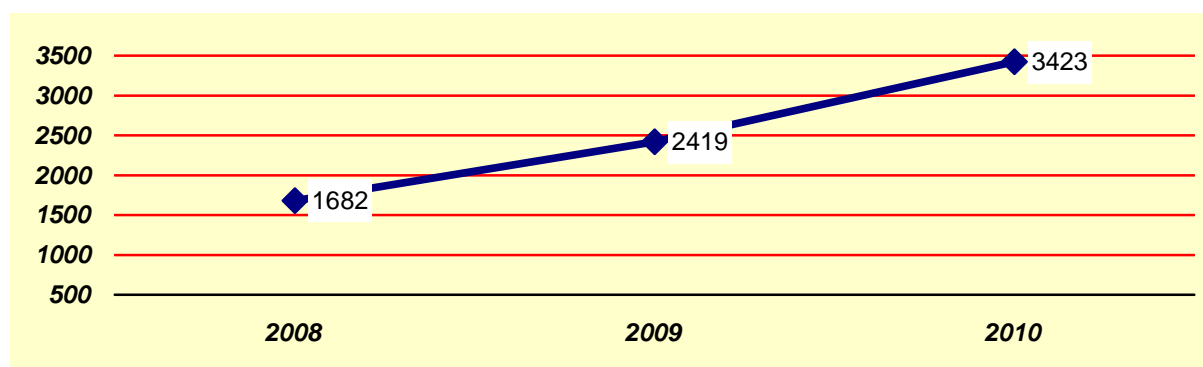
*Wykres 26: Zestawienie porównawcze decyzji o wykreśleniu zbioru z rejestru zbiorów danych osobowych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2010.*

W 2010 r. Generalny Inspektor Ochrony Danych Osobowych rozpatrzył **3423 zgłoszenia aktualizacyjne** dokonane przez administratorów danych w trybie art. 41 ust. 2 ustawy o ochronie danych osobowych. Podobnie jak w poprzednich okresach sprawozdawczych aktualizacje te najczęściej dotyczyły zmiany siedziby administratora danych, zmiany zakresu przetwarzanych danych, a także zmian dotyczących środków technicznych i organizacyjnych zastosowanych w celu ochrony

<sup>62</sup> Zgodnie art. 41 ust. 2 administrator danych obowiązany jest zgłaszać każdą zmianę informacji zawartych w zgłoszeniu rejestracyjnym w terminie 30 dni od dnia dokonania zmiany w zbiorze danych.



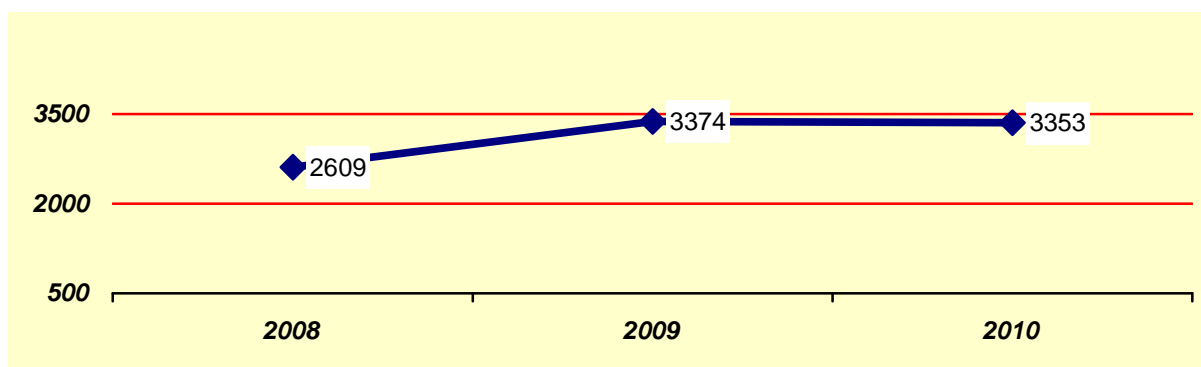
przetwarzanych danych osobowych.



Wykres 27: *Zestawienie porównawcze zgłoszeń aktualizacyjnych rozpatrzonych w latach 2008 - 2010.*

Należy zauważyć, iż w roku 2010, w porównaniu z poprzednimi latami, zostało rozpatrzonych zdecydowanie więcej zgłoszeń aktualizacyjnych. Tak jak w przypadku zgłoszeń zbiorów danych osobowych rozpatrzonych w 2010 r. osiągnięcie takiego wyniku było możliwe ze względu na to, iż nadsyłane aktualizacje nie zawierały takiej ilości błędów, jak to miało miejsce w latach ubiegłych. Powodów poprawy jakości zgłoszeń, z punktu widzenia spełniania wymogów ustawowych, należy upatrywać w tych samych przyczynach, które odnoszą się do zgłoszeń zbiorów danych, a mianowicie w rozszerzeniu możliwości wykorzystania programu komputerowego wspomagającego wypełnianie zgłoszenia oraz uproszczeniu wzoru zgłoszenia.

Zadaniem Generalnego Inspektora Ochrony Danych Osobowych jest także udzielanie informacji o zarejestrowanych zbiorach, w szczególności wydawanie zaświadczeń o zarejestrowaniu zbioru danych osobowych. W omawianym okresie Generalny Inspektor Ochrony Danych Osobowych wydał **3353 zaświadczenia o zarejestrowaniu zbioru**. Generalny Inspektor wydaje zaświadczenia o zarejestrowaniu zgłoszonego zbioru danych na żądanie administratora. Jednakże w przypadku zarejestrowania zbioru danych, w którym przetwarzane są dane osobowe szczególnie chronione, określone w art. 27 ust. 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych wydaje zaświadczenie z urzędu, niezwłocznie po dokonaniu rejestracji takiego zbioru.

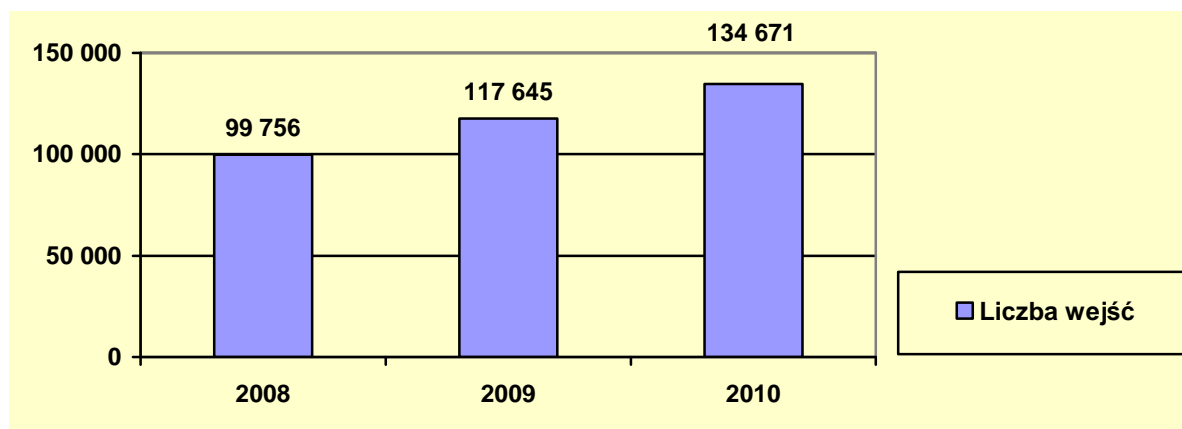


Wykres 28: Zestawienie liczby zaświadczeń o zarejestrowaniu zbioru danych osobowych wydanych w latach 2008 - 2010.

W okresie od stycznia do grudnia 2010 roku, poza korespondencją prowadzoną w związku z postępowaniami rejestracyjnymi, wysłano **46 odpowiedzi na zapytania** dotyczące problematyki rejestracji zbiorów danych osobowych.

Celem rejestracji jest także upublicznienie informacji o zbiorach zarejestrowanych w ogólnokrajowym jawnym rejestrze zbiorów danych osobowych. Każdy, korzystając z prawa do przeglądania rejestru, może uzyskać ogólne informacje o administratorach danych i prowadzonych przez nich zbiorach. Umożliwia to osobom, których dane mogą być przetwarzane w takich zbiorach, sprawowanie indywidualnej kontroli przetwarzania danych wynikającej z art. 32 ustawy. Informacje zawarte w rejestrze udostępniane są na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych ( [www.giodo.gov.pl](http://www.giodo.gov.pl) ) w ramach platformy e-GIODO. Wyszukanie ksiąg rejestrowych dotyczących zbiorów wpisanych do ogólnokrajowego rejestru zbiorów danych osobowych możliwe jest według różnych kryteriów, m.in. nazwy administratora danych, miejscowości, czy też nazwy zbioru danych.

W roku 2010 w elektronicznej wersji rejestru odnotowano **134 671 wejść** do poszczególnych ksiąg rejestrowych.

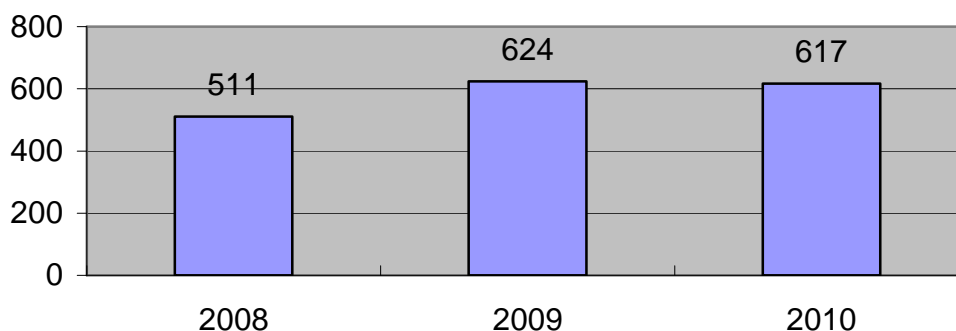


Wykres 29: *Liczbowe zestawienie wejść do poszczególnych ksiąg rejestrowych w rejestrze zbiorów danych osobowych w ramach platformy e-GIODO w latach 2008 - 2010.*

## 5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych

Na wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych już na etapie procesu tworzenia prawa, pozwala uprawnienie Generalnego Inspektora nadane mu mocą art. 12 ust. 4 ustawy o ochronie danych osobowych. Stosownie do treści tego przepisu, do zadań Generalnego Inspektora należy opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych.

W roku 2010 do Biura GIODO wpłynęło do zaopiniowania **617 projektów aktów prawnych**, a zatem odnotować należy nieznaczny spadek w tej kategorii względem roku poprzedniego, co przedstawia Wykres 30.



Wykres 30: *Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2010.*

Należy zwrócić uwagę, że w roku 2010, mocą przepisów *ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw* (Dz. U. Nr 229, poz. 1497) zakończony został trwający od 2007 roku proces legislacyjny, mający na celu wprowadzenie zmian w przepisach ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Generalny Inspektor uzyskał uprawnienia w postaci nakładania grzywien, jako środka egzekucyjnego, w celu przymuszenia, jak również wprost sformułowane zostało jego prawo występowania do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Ponadto podmioty, do których zostało skierowane przez GODO wystąpienie lub wnioski będą zobowiązane ustosunkować się do nich w terminie 30 dni od daty jego otrzymania. W nowelizowanych przepisach ustawy o ochronie danych osobowych wprowadzony zostanie nowy rodzaj przestępstwa, jakim będzie uniemożliwianie bądź utrudnianie kontroli GODO. Kara za ten czyn w postaci grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2, będzie mogła być nałożona nie tylko na administratora danych, ale także na każdą osobę, która uczestnicząc w kontroli uniemożliwia bądź utrudnia jej przeprowadzenie. Dla kontrolowanych podmiotów istotne znaczenie mają nowe przepisy precyzujące, co powinny zawierać wystawiane kontrolerom imienne upoważnienie i sporządzany przez nich protokół. Dodać można też, że ustawa o zmianie ustawy o ochronie danych osobowych zawiera także przepisy o charakterze porządkującym rozwiązania już istniejące w obowiązującej ustawie o ochronie danych osobowych. Uchylony został art. 29, regulujący udostępnianie danych osobowych w celach innych niż włączenie do zbioru. Po nowelizacji ustawy o ochronie danych osobowych jedynymi przesłankami przetwarzania, a więc także udostępniania danych osobowych, pozostaną te wymienione w art. 23 ustawy odnośnie danych zwykłych i art. 27 ustawy odnośnie danych szczególnie chronionych.

Zaznaczyć również trzeba, że zmiany w ustawie o ochronie danych osobowych wprowadza też nowa *ustawa o ochronie informacji niejawnych*<sup>63</sup>. Zmiany te dotyczą kwestii rejestracji zbiorów, odmowy udostępnienia danych i obowiązku informacyjnego. I tak, z obowiązku rejestracji zbioru danych zwolnieni będą administratorzy danych, których zbiory zawierają informacje niejawne, administrator danych będzie mógł odmówić udostępnienia danych, jeśli ich ujawnienie spowodowałoby ujawnienie wiadomości zawierających informacje niejawne, a także nie będzie informował osoby o tym, skąd pozyskał jej dane, jeśli te informacje objęte będą tajemnicą informacji niejawnych lub tajemnicą zawodową.

---

<sup>63</sup> DOLiS-033-244/09, ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Dz. U. Nr 182, poz. 1228.

Opiniując projekt *ustawy o systemie informacji w ochronie zdrowia* (element tzw. pakietu zdrowotnego), organ do spraw ochrony danych osobowych zgłosił w trakcie prac legislacyjnych szereg istotnych zastrzeżeń do przedmiotowego projektu, które – na etapie prac rządowych – w znacznej części nie zostały uwzględnione. Organ do spraw ochrony danych osobowych nie zanegował samej potrzeby tworzenia zintegrowanego systemu teleinformatycznego służącego do zarządzania zadaniami w zakresie ochrony zdrowia, ani konieczności wprowadzenia skutecznych mechanizmów kontroli sposobu świadczenia usług publicznych w ochronie zdrowia. Jednakże jako podmiot stojący na straży praw osobistych gwarantowanych przez Konstytucję Rzeczypospolitej Polskiej podjął starania dla zapewnienia, by przyjmowane nowe rozwiązania prawne gwarantowały jak najwyższy poziom ochrony szczególnie wrażliwych danych, jakimi są dane o stanie zdrowia. Generalny Inspektor Ochrony Danych Osobowych wskazał zagrożenia dla prawa do prywatności i prawa do ochrony danych osobowych wynikające z regulacji zawartych w przedstawionym do zaopiniowania projekcie.

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych podstawowe kryteria oceny zbioru, jego zawartości, zasad przetwarzania danych (w tym danych osobowych) oraz technicznych metod zabezpieczenia tych danych przed nieuprawnionym przetwarzaniem powinny być zdeterminowane faktem, iż zaprojektowana baza danych - pod względem swojej zawartości - będzie jedną z największych w Polsce. W uzasadnieniu do projektu ustawy wskazano, że w trakcie analizy systemów informacyjnych obsługujących system ochrony zdrowia, zidentyfikowano 69 rejestrów i ewidencji, dla których podstawę prawną funkcjonowania stanowią przepisy o randze ustawy. Co więcej, stwierdzono, iż analiza ta nie uwzględnia rejestrów, ewidencji i innych uporządkowanych zbiorów informacji w ochronie zdrowia funkcjonujących na podstawie umów lub porozumień zawieranych przez organy publiczne w celu wykonania zadań publicznych, rejestrów i ewidencji funkcjonujących w oparciu o normy zwyczajowe lub prowadzonych na podstawie nieobowiązujących już aktów prawnych na zasadach historycznych oraz rejestrów prowadzonych bez jakichkolwiek podstaw prawnych. W opinii GODO niepokojącym był również fakt uwzględniania w ramach projektowanego systemu, rejestrów funkcjonujących bez podstawy wynikającej z powszechnie obowiązujących przepisów prawa (na przykład tzw. rejestry rakowe).

Generalny Inspektor Ochrony Danych Osobowych opiniując przedmiotowy projekt podkreślił, iż każde przedsięwzięcie związane z przetwarzaniem danych powinno odbywać się z poszanowaniem zasad przetwarzania danych osobowych wynikających z przepisów prawa powszechnie obowiązującego, w tym z ustawy o ochronie danych osobowych oraz jej przepisów wykonawczych. Planowany niniejszym projektem ustawy system informacji w ochronie zdrowia swoim zakresem obejmować powinien wyłącznie te rejestry oraz ewidencje, które tworzone będą w oparciu o przepisy obowiązującego prawa. W ocenie organu niedopuszczalne jest przetwarzanie danych osobowych, w tym danych szczególnie chronionych, w zbiorach (rejestrach, ewidencjach) funkcjonujących na

podstawie innej niż przepisy powszechnie obowiązujące, ani też próba zalegalizowania takiego stanu rzeczy poprzez ogólne sformułowania analizowanego projektu. Niezależnie od powyższego GIODO zgłosił do projektu również wiele uwag szczegółowych odnośnie niezgodności projektowanych przepisów z regulacjami ustawy o ochronie danych osobowych, bądź ich niejasności interpretacyjnej. W odniesieniu do tego projektu GIODO zamierza nadal podejmować działania celem zmiany rozwiązań zaakceptowanych przez Sejm.

W roku 2010 GIODO kontynuował prace legislacyjne nad *projektem założeń projektu ustawy o systemie informacji oświatowej*. Opiniując założenia, a następnie projekt przepisów ustawy GIODO wskazał, że kwestia tworzenia tak rozbudowanych zbiorów, jak projektowana przez Ministerstwo Edukacji Narodowej megabaza danych osobowych, zawierająca miliony danych osobowych – w tym przypadku informacje o około 5 milionach uczniów, 900 tysiącach przedszkolaków, 600 tysiącach słuchaczy i 600 tysiącach nauczycieli, zawsze była i pozostawać będzie przedmiotem szczególnego zainteresowania organu do spraw ochrony danych osobowych.

Pomimo prowadzonych w trakcie dotychczasowego procesu legislacyjnego konsultacji, zawarta w przedmiotowym projekcie propozycja utworzenia przy ministrze właściwym ds. oświaty i wychowania systemu teleinformatycznego obsługującego scentralizowany zbiór danych, nadal budziła istotne wątpliwości organu do spraw ochrony danych osobowych. Nie przekonywała bowiem prezentowana dotychczas przez Ministerstwo Edukacji Narodowej argumentacja, zgodnie z którą zgromadzenie w bazie danych administrowanej przez ministra właściwego ds. oświaty i wychowania wielkiej ilości danych osobowych jest niezbędne dla prawidłowej realizacji polityki oświatowej oraz zarządzania oświatą. GIODO wskazał także na niebezpieczeństwo bezprawnego ujawnienia zgromadzonych danych, jak i pokusę ich wykorzystania dla innych celów, aniżeli te, dla których pierwotnie zostały zebrane.

Do projektu zgłoszone zostały także uwagi szczegółowe, jak np. ta, że nie został zrealizowany – sygnalizowany przez Generalnego Inspektora już na etapie prac ministerialnych – postulat określenia w projektowanej *ustawie o systemie informacji oświatowej*, zamkniętego katalogu danych zamieszczanych we wniosku o udzielenie upoważnienia do dostępu do bazy danych SIO. Ponadto w projekcie opisane zostały procedury nadawania i odbierania upoważnień do dostępu do bazy danych SIO, jednakże zaniechano wskazania podmiotu odpowiedzialnego za prowadzenie ewidencji osób upoważnionych do dostępu do tej bazy. Nieracjonalne – w opinii Generalnego Inspektora – było również rozwiązanie, zgodnie z którym rodzice ucznia składają w placówce oświatowej, prowadzącej zalecaną dla ucznia formę kształcenia, opinię lub orzeczenie, a następnie placówka ta na podstawie numeru i daty tego dokumentu pozyskuje z bazy danych SIO dane o tej opinii lub orzeczeniu. Projekt omawianej ustawy skierowany został do Sejmowej Komisji Edukacji, Nauki i Młodzieży oraz Komisji Samorządu Terytorialnego i Polityki Regionalnej.

GIODO opiniując powyższe projekty podkreślał, iż w toku dotychczasowych prac nie została rozstrzygnięta wątpliwość, czy zaproponowana koncepcja funkcjonowania tych systemów nie będzie prowadziła do naruszenia zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich będą one przetwarzane. Generalny Inspektor sygnalizował autorom wymienionych projektów, że nie należy również wykluczać takiej zmiany prawa w przyszłości, która dopuści wykorzystywanie danych zgromadzonych w megabazach w celu innym, niż wskazany pierwotnie. Tym bardziej, iż dane te posiadać będą znaczną wartość rynkową. Zwrócił także uwagę na inne istotne zagadnienie, jakim będzie możliwość łączenia w przyszłości systemów teleinformatycznych obsługujących projektowane megabazy, z innymi, już istniejącymi systemami teleinformatycznymi (na przykład w odniesieniu do systemu informacji o ochronie zdrowia - z systemami obsługiwanymi przez ePUAP<sup>64</sup>, czy GUS), bądź z systemami planowanymi do utworzenia w przyszłości, np. w szkolnictwie wyższym w odniesieniu do systemu informacji oświatowej. Wobec powyższego, ewentualne uchybienia popełnione dziś przy tworzeniu podstaw prawnych dla przetwarzania danych w systemie informacji w ochronie zdrowia czy systemie informacji oświatowej mogą w przyszłości zaważyć nad działaniem innych systemów w naszym kraju<sup>65</sup>.

Kolejna projektowana megabaza przedstawiona została w dokumencie *Założenia do projektu ustawy o zmianie ustawy o zasadach ewidencji i identyfikacji podatników i płatników oraz o zmianie niektórych innych ustaw*. Pomimo ustaleń poczynionych na konferencji uzgodnieniowej, dokument ten wciąż budził zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych, ponieważ projektowana megabaza będzie wykorzystywać informacje pochodzące ze zbioru PESEL.

Opiniując powyższy dokument GIODO podniósł, że przedstawiona przez Ministerstwo Finansów propozycja wykorzystania administracyjnego numeru identyfikacyjnego PESEL, jako identyfikatora osób fizycznych w ich kontaktach z administracją podatkową, nie jest rozwiązaniem powszechnie przyjętym w ustawodawstwach państw europejskich. Wykorzystywanie we wszystkich kontaktach z administracją publiczną jednego numeru identyfikacyjnego obywatela stanowiłoby bowiem nadmierną ingerencję w jego prywatność.

Nie negując prawa projektodawcy do zmiany istniejącego stanu prawnego, Generalny Inspektor Ochrony Danych Osobowych czuł się zobligowany do wskazania, że zaproponowane przez Ministerstwo Finansów wykorzystanie numeru PESEL, jako identyfikatora w kontaktach z administracją podatkową dla podatników będących osobami fizycznymi nieprowadzącymi

---

<sup>64</sup> 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 realizowanych drogą elektroniczną. Informacje zawarte na portalu odnoszą się do formy organizacyjno-prawnej, możliwości systemu, sposobu korzystania oraz innych kwestii związanych z platformą.

<sup>65</sup> Uwagi zgłoszone przez GIODO zostały w większości uwzględnione, co nastąpiło w styczniu 2011 r.

działalności gospodarczej, skutkować może zmniejszeniem poziomu ochrony tej danej osobowej. Logiczną konsekwencją potraktowania numeru PESEL jako identyfikatora podatkowego jest bowiem wyłączenie go spod zakresu tajemnicy skarbowej. Przypomniano także, iż art. 37 ust. 1 ustawy o swobodzie działalności gospodarczej, uznaje numer PESEL przedsiębiorcy będącego osobą fizyczną za daną tak ściśle powiązaną z tą osobą, że zasługującą na szczególną ochronę i – w konsekwencji – niepodlegającą udostępnieniu za pośrednictwem Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Organ do spraw ochrony danych osobowych nie mógł także pominąć, iż przyjęcie propozycji Ministerstwa Finansów przedstawionej w projekcie założeń, umożliwia ministrowi właściwemu do spraw finansów publicznych, jako organowi prowadzącemu Centralny Rejestr Podmiotów - Krajową Ewidencję, dokonywanie unifikacji w oparciu o jeden identyfikator zbiorów danych prowadzonych przez różne podmioty publiczne. Nakłada to na Ministra Finansów obowiązek dołożenia wyjątkowej staranności w celu ochrony praw osób, których dane będzie przetwarzał, w szczególności zaś do uniemożliwienia dokonywania, także w przyszłości, istotnie ingerującego w te prawa profilowania osób.

Z punktu widzenia zasad ochrony danych osobowych, wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budziła zwłaszcza przedstawiona w projekcie założeń koncepcja przekształcenia Krajowej Ewidencji Podatników w Centralny Rejestr Podmiotów – Krajową Ewidencję Podatników (CRP KEP). Krajowa Ewidencja Podatników zawiera dane ze zgłoszeń identyfikacyjnych i aktualizacyjnych podatników, tj. osób fizycznych, osób prawnych lub jednostek organizacyjnych niemających osobowości prawnej, podlegających na mocy ustaw podatkowych obowiązkowi podatkowemu wynikającemu z art. 7 §1 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60 z późn. zm.). Tymczasem projekt założeń przewiduje **automatyczne** zapisywanie w CRP KEP imienia, nazwiska i numeru PESEL **każdej osoby posiadającej numer PESEL**. Tym samym zbiór nazwany w projekcie założeń Centralnym Rejestrem Podmiotów – Krajową Ewidencją Podatników, będzie w istocie obejmować swoim zakresem również osoby niebędące jeszcze podatnikami, na przykład noworodki czy osoby o polskim obywatelstwie pozostające na stałe za granicą. W grupie tych podmiotów mogą się więc znaleźć nawet takie osoby, które nigdy podatnikami się nie staną. GODO uznał, że tworzenie takiego zbioru nie wydaje się prawidłowe w świetle zasad ochrony danych osobowych, jak również stanowi dublowanie, utworzonego na podstawie ustawy o ewidencji ludności i dowodach osobistych i mającego wejść w życie od 1 sierpnia 2011 roku na podstawie ustawy o ewidencji, zbioru (rejestru) PESEL.

Nie negując prawa administracji podatkowej do prowadzenia bazy danych osób, w stosunku do których zaistniało jakiekolwiek zdarzenie skutkujące powstaniem obowiązku podatkowego, czyli bazy podatników, organ do spraw ochrony danych osobowych pozostawił pod rozważę autorów projektu



założeń kwestię zakresu pozyskiwanych danych. Proponowany w zmianie katalog tych danych wydaje się bowiem nadmiernie szeroki w stosunku do deklarowanego celu tworzenia takiej bazy. Zauważono też, że problematyka właściwego określenia okresu retencji danych w zbiorach danych, jak również zagadnienie konieczności dokonywania przeglądu posiadanych danych pod kątem ich przydatności do realizacji deklarowanych celów istnienia konkretnego zbioru danych, jest w chwili obecnej przedmiotem szczególnego zainteresowania ze strony organów Unii Europejskiej. Tymczasem przedstawiony projekt założeń pomija te kwestie milczeniem i dlatego wciąż jeszcze wymaga dalszych uzgodnień i konsultacji z organem do spraw ochrony danych osobowych. Z uwagi na wskazane wyżej liczne wątpliwości, Generalny Inspektor Ochrony Danych Osobowych zamierza aktywnie uczestniczyć w pracach dotyczących przedmiotowego projektu założeń i zwrócił się do projektodawcy o przesyłanie zarówno kolejnych wersji samego projektu założeń, jak i projektu ustawy, po ich sporządzeniu. Organ do spraw ochrony danych osobowych – podobnie jak w przypadkach innych doniosłych projektów – zastrzegł sobie przy tym prawo do zgłaszania uwag do tych projektów na każdym etapie prac legislacyjnych, zwłaszcza w oparciu o dokonaną analizę ich konkretnych unormowań, nie zaś sformułowanych w sposób ogólny założeń, czy propozycji<sup>66</sup>.

Na oddzielne omówienie zasługuje także tzw. **pakiet ustaw zdrowotnych**. Jest to popularna nazwa szeregu projektów legislacyjnych. W prace nad tymi projektami organ do spraw ochrony danych był zaangażowany ze względu na zawarte w nich istotne rozwiązania prawne dotyczące przetwarzania danych osobowych, w tym danych wrażliwych. W początkowej fazie pakiet ten składał się z 12 projektów ustaw. Po odrzuceniu *projektu ustawy o zakazie zapłodnienia pozaustrojowego i manipulacji ludzką informacją genetyczną* przez Sejm RP w I czytaniu, liczba projektowanych aktów prawa zmniejszyła się do jedenastu. Poniżej przedstawionych zostało dziesięć projektów wchodzących w skład pakietu ustaw zdrowotnych, ponieważ charakterystyka jednego z nich, a mianowicie projektu ustawy o systemie informacji w ochronie zdrowia, została już wcześniej przedstawiona.

Pierwsze uwagi do trzech projektów, a mianowicie: *ustawy o ochronie genomu ludzkiego i embrionu ludzkiego oraz Polskiej Radzie Bioetycznej i zmianie innych ustaw, ustawy o zmianie ustawy o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów, ustawy o zmianie ustawy Kodeks rodzinny i opiekuńczy*, Generalny Inspektor Ochrony Danych Osobowych zgłosił w roku 2009.

Opiniując powyższe projekty GIODO podkreślił, iż istotą ochrony danych osobowych jest ochrona prywatności osoby, której dane dotyczą. Źródło tej ochrony wynika przede wszystkim z przepisów Konstytucji Rzeczypospolitej Polskiej. Zgodnie natomiast z utrwalonym orzecznictwem Trybunału Konstytucyjnego, wkroczenie w prywatność jednostki jest działaniem konstytucyjnym, o ile

---

<sup>66</sup> Rada Ministrów przyjęła założenia do omawianego projektu założeń podczas posiedzenia w dniu 15 lutego 2011 r.

jest konieczne dla osiągnięcia wskazanych w zapisach ustawy zasadniczej celów. I tylko te cele są władne uzasadnić naruszenie praw i wolności jednostki<sup>67</sup>. Dlatego też GIODO zwrócił się do projektodawców o rozważenie, czy rozwiązania istniejące w aktualnym stanie prawnym i utrzymywane mocą przepisów przedłożonych projektów, w istocie wyczerpują warunki wskazane w przepisach konstytucyjnych. W 2010 roku Sejm RP kontynuował prace dotyczące pakietu ustaw regulujących problematykę zapłodnienia pozaustrojowego (in vitro), ochrony genomu ludzkiego i embrionu ludzkiego oraz pobierania, przechowywania i przeszczepiania komórek, tkanek i narządów. Projekty te zostały skierowane do Komisji Polityki Społecznej i Rodziny oraz Komisji Zdrowia. W związku z tym GIODO poinformował przewodniczących tych komisji<sup>68</sup>, że zagadnienia regulowane przepisami tych aktów – jako że dotyczą przetwarzania danych szczególnie chronionych – pozostają przedmiotem szczególnego zainteresowania organu do spraw ochrony danych osobowych.

Opiniując projekt *ustawy o działalności leczniczej* Generalny Inspektor podniósł, że jego zastrzeżenia wzbudziła dyspozycja przewidująca wyposażenie pacjentów szpitali w znaki identyfikacyjne zawierające ich imiona i nazwiska. W uzasadnieniu projektu brak jest bowiem wskazania przyczyn wprowadzenia takiego unormowania. W ocenie Generalnego Inspektora Ochrony Danych Osobowych wprowadzenie tego zapisu może godzić w prawo pacjentów do prywatności, a nawet w statuowane ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta - prawo pacjentów do intymności. Generalny Inspektor Ochrony Danych Osobowych wskazał także na brak racjonalnych powodów, dla których projektodawcy zdecydowali się narazić pacjentów na takie niedogodności. Rozumiejąc jednak potrzebę sprawnej identyfikacji pacjentów szpitali przez uprawnionych pracowników służby zdrowia, zwrócił się o przyjęcie w projekcie takich rozwiązań, które nie będą prowadziły do naruszenia konstytucyjnie gwarantowanych praw pacjentów.

GIODO pozytywnie natomiast ocenił określone w projekcie zasady prowadzenia rejestru podmiotów wykonujących działalność leczniczą. Z drugiej jednak strony wskazał, iż sposób, w jaki regulacja ta została ujęta, rodzi dwie wątpliwości. Po pierwsze, nie ma jasności z jakich źródeł organ prowadzący rejestr ma pozyskiwać informacje nieznajdujące się we wnioskach o wpis do przedmiotowego rejestru, po drugie zaś – jaki zakres informacji miałby być w rzeczywistości zamieszczony w rejestrze podmiotów wykonujących działalność leczniczą.

Nie umknął uwadze organu do spraw ochrony danych osobowych fakt pominięcia w projekcie zasad udostępniania danych z rejestru. Dodatkowo sposób rozwiązania przez autorów projektu kwestii jawności, bądź powszechnej dostępności danych zawartych w rejestrze, rzutować także będzie w sposób bezpośredni na ocenę GIODO w odniesieniu do zagadnienia adekwatności danych zamieszczanych w tym rejestrze.

---

<sup>67</sup> Wyrok Trybunału Konstytucyjnego z dnia 20 listopada 2002 r. o sygn. K. 41/2002.

<sup>68</sup> DOLiS-070-19/10

W przedstawionym do zaopiniowania projekcie *ustawy o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta*, zastrzeżenia GODO wzbudził brak unormowania nakładającego na członków wojewódzkich komisji do spraw orzekania o błędach medycznych, obowiązku zachowania w tajemnicy informacji i danych osobowych uzyskanych podczas wydawania orzeczeń, w tym również po ustaniu członkostwa w takiej komisji. W opinii Generalnego Inspektora Ochrony Danych Osobowych konieczność wprowadzenia przedmiotowej regulacji nie ulega wątpliwości.

Zgłaszając uwagi do *ustawy o zmianie ustawy o zawodach lekarza i lekarza dentysty* Generalny Inspektor podniósł, że w świetle określonych w ustawie o ochronie danych osobowych zasad ochrony tych danych (zwłaszcza zasady adekwatności), zachodzi potrzeba określenia zakresu danych zawartych w zaświadczeniach, o którym mowa jest w projektowanych przepisach. Generalny Inspektor wskazał ponadto, że jeśli w zaświadczeniu nie miałyby się znajdować dane szczególnie chronione w rozumieniu wspomnianej ustawy, możliwym rozwiązaniem mogłoby być określenie wzoru tego zaświadczenia w rozporządzeniu wykonawczym do ustawy o zawodach lekarza i lekarza dentysty.

Zastrzeżenia organu do spraw ochrony danych osobowych wzbudziły również projektowane unormowania nakładające na organy prowadzące postępowanie kwalifikacyjne oraz Państwową Komisję Egzaminacyjną (lub wydzielony spośród jej członków zespół egzaminacyjny) obowiązek sporządzenia listy lekarzy zakwalifikowanych i niezakwalifikowanych do rozpoczęcia danego szkolenia specjalizacyjnego oraz listy lekarzy dopuszczonych do Państwowego Egzaminu Specjalizacyjnego. Nie sprecyzowano bowiem, wbrew wymaganiom wynikającym z ustawy o ochronie danych osobowych, jakie dane osobowe winny zawierać przedmiotowe listy. Podkreślić należy, że niewskazanie zakresu danych osobowych lekarzy przetwarzanych na potrzeby przygotowania powyższych list, godzi bezpośrednio w prawo tych osób do ochrony dotyczących ich danych osobowych oraz rodzi realne niebezpieczeństwo naruszenia zasady adekwatności przetwarzanych danych w stosunku do celów ich przetwarzania.

W opinii do *projektu ustawy o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych* Generalny Inspektor zwrócił uwagę, że nie zawierał on określenia katalogu danych zawartych w deklaracji o braku konfliktu interesów, a dotyczących danych osoby składającej oświadczenia oraz danych jej małżonka, wstępnych i zstępnych. Po raz kolejny Generalny Inspektor zmuszony był zwrócić uwagę, że ustawa o ochronie danych osobowych wymaga, aby dane osobowe były adekwatne w stosunku do celów ich przetwarzania, a zatem swym rodzajem i swą treścią nie powinny wykraczać poza potrzeby wynikające z celu zbierania.

Zastrzeżenia budził także sposób oznaczenia w projektowanych przepisach osoby „wnioskodawcy” między innymi poprzez podanie jego adresu. Zgodnie z aktualnie obowiązującym

stanem prawnym, dane dotyczące osoby fizycznej prowadzącej działalność gospodarczą nie podlegają ochronie przewidzianej przepisami ustawy o ochronie danych osobowych, jeśli są powiązane ściśle z prowadzoną działalnością gospodarczą. GODO zaproponował zatem, aby w opiniowanym projekcie dokonano takiego zredagowania terminu „adres”, aby oczywistym było, iż podawany jest adres zamieszkania osoby fizycznej prowadzącej działalność gospodarczą jedynie w przypadku, gdy adres i miejsce wykonywania tej działalności są tożsame. GODO nie zaakceptował również praktyki posługiwania się przez projektodawcę sformułowaniem „w szczególności” dla określenia elementów, jakie zawierać będzie umowa na realizację recept, jak również umowa upoważniająca do wystawiania recept na refundowane leki, środki spożywcze specjalnego przeznaczenia żywieniowego oraz wyroby medyczne. Treść projektowanych przepisów prawa nie powinna bowiem budzić jakichkolwiek wątpliwości interpretacyjnych.

W chwili obecnej nad **projektami ustawy o refundacji leków, ustawy o Urzędzie Rejestracji Produktów Leczniczych**<sup>69</sup>, który nie wpłynął do zaopiniowania przez GODO oraz **ustawy Prawo Farmaceutyczne**<sup>70</sup>, do którego GODO nie zgłosił uwag, trwają prace w sejmowej podkomisji Nadzwyczajnej. Zaznaczyć jednak trzeba, że jeszcze na etapie prac ministerialnych nad tymi projektami, uwagi GODO uwzględnione zostały w satysfakcjonujący sposób. Aktualnie trwają prace parlamentarne nad tymi projektami.

Poniżej przedstawione zostały projekty innych aktów prawnych przesłanych Generalnemu Inspektorowi Ochrony Danych Osobowych w 2010 r. do zaopiniowania, które również zwróciły jego uwagę ze względu na podejmowane w nich istotne kwestie związane z regulacjami zawartymi w ustawie o ochronie danych osobowych, jak i samej Konstytucji RP oraz prawie Unii Europejskiej.

Analiza **projektu ustawy o kredycie konsumenckim**<sup>71</sup> wzbudziła zasadnicze wątpliwości GODO w przedmiocie poważnego rozszerzenia katalogu danych osobowych w ustawie Prawo bankowe<sup>72</sup>. Konstrukcja tego katalogu umożliwia udostępnianie bardzo szerokiemu kręgowi kredytodawców (także tym mającym siedzibę na terytorium innych państw członkowskich UE), informacji stanowiących tajemnicę bankową w zakresie, w jakim są one niezbędne do oceny ryzyka kredytowego. Generalny Inspektor zaoponował przeciwko rozszerzeniu art. 105 ust. 4 Prawa bankowego o kolejne podmioty, które mogą uzyskiwać od instytucji utworzonych na podstawie tego przepisu informacje będące tajemnicą bankową. Utworzenie instytucji informacji kredytowej miało na celu ułatwienie uzyskiwania informacji i jej „przepływ” w sektorze bankowym<sup>73</sup>. Tymczasem

---

<sup>69</sup> DOLiS-033-361/10

<sup>70</sup> DOLiS-033-249/09

<sup>71</sup> DOLiS-033-201 i DOLiS-033-450.

<sup>72</sup> Art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe. Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.

<sup>73</sup> W literaturze przedmiotu wskazuje się, iż, cyt.: „(...) Funkcjonowanie takiej instytucji będzie wygodniejsze dla banków niż uzyskiwanie informacji bezpośrednio od konkretnego banku lub instytucji (...)” zob. Bączyk M., Góral L., Fojcik–

w rozumieniu spornego przepisu projektu, kredytodawcą miałyby być przedsiębiorca w rozumieniu przepisów ustawy Kodeks cywilny<sup>74</sup>, który w zakresie swojej działalności gospodarczej lub zawodowej, udziela lub daje przyrzeczenie udzielenia konsumentowi kredytu. Powyższe oznaczałoby, że dostęp do objętych tajemnicą bankową danych o zobowiązaniach olbrzymiej grupy osób, uzyskałaby znacznie większa, niż obecnie, liczba podmiotów. GIODO uznał za niedopuszczalne uczynienie z informacji o zobowiązaniach osób fizycznych wiedzy niemal powszechnie dostępnej, wskazując przy tym, że praktyka taka stanowi naruszenie zasad demokratycznego państwa prawa.

Za celowe GIODO uznał także zwrócenie uwagi na zapisy ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz. U. Nr 81, poz. 530), które mają na celu usprawnienie systemu wymiany informacji gospodarczych, poprawę warunków funkcjonowania biur informacji gospodarczych, a także zapewnienie lepszej ochrony wierzycieli. Do jednej z najważniejszych zmian, jakie przewiduje ta ustawa w stosunku do uprzedniego stanu prawnego, należy otwarcie katalogu podmiotów uprawnionych do przekazywania informacji gospodarczych, a także uzyskiwania wiedzy na temat wiarygodności. Zdaniem GIODO przepisy tej ustawy będą bardzo pomocne w ocenie ryzyka kredytowego przez kredytodawcę.

W odniesieniu do innych postanowień *projektu ustawy o kredycie konsumenckim* Generalny Inspektor Ochrony Danych Osobowych wskazał, że brak było w jego treści doprecyzowania, jakiego rodzaju dane osobowe konsumenta zamieszczane miałyby być w projekcie umowy o kredyt konsumencki. Informacji na temat zakresu „podstawowych” danych osobowych konsumenta, przetwarzanych w związku z procesem udzielania kredytu konsumenckiego, nie było także w pozostałych przepisach projektu. GIODO wskazał, że celem uniknięcia wątpliwości interpretacyjnych, jakiego rodzaju dane osobowe konsumenta mają być przetwarzane w treści umowy, niezbędne jest wprowadzenie odpowiednich przepisów do przedłożonego projektu.

Na podstawie analizy projektu ustawy przekazanego do prac w Komisji sejmowej ustalono, że powyższe uwagi GIODO, skupione zasadniczo wokół proponowanych zmian obowiązujących przepisów ustawy Prawo bankowe, zostały uwzględnione. Podczas trwających obecnie prac legislacyjnych nad tym projektem w Sejmowej Komisji Gospodarki, GIODO wniósł zastrzeżenia do sposobu sformułowania art. 30 ust. 1 ww. projektu. Określony w tym przepisie katalog informacji, które zawierać miałyby umowa o kredyt konsumencki, poprzedzony został formułą „co najmniej” i zyskał w ten sposób charakter otwarty. Przy takim ujęciu opiniowanej regulacji konsument mógłby być zobligowany do podawania przy zawieraniu umowy o kredyt konsumencki dowolnych swoich

---

Mastalska E. (red.), Pisuliński J., Pyziół W.: *Najnowsze wydanie: Prawo bankowe. Komentarz*. Wyd. V, Warszawa 2007, Wydawnictwo Prawnicze LexisNexis, s. 840.

<sup>74</sup> Zgodnie z art. 43<sup>1</sup> ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny, przedsiębiorcą jest osoba fizyczna, osoba prawna i jednostka organizacyjna, o której mowa w art. 33<sup>1</sup> § 1, prowadząca we własnym imieniu działalność gospodarczą lub zawodową. Dz. U. Nr 16, poz. 93 z późn. zm.

danych osobowych, co stwarza niebezpieczeństwo pozyskiwania przez kredytodawców danych zbędnych, w nadmiarze, i – w konsekwencji – naruszenia jednej z podstawowych zasad przetwarzania danych osobowych, to jest zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane. Identyczną uwagę zgłoszono wobec zaproponowanego brzmienia art. 35 ust. 1 zdanie wstępne projektu. Tematem aktualnym w pracach komisji sejmowej jest również dokonanie ww. zmian w Prawie bankowym. Sejmowa Komisja Gospodarki rozpatrzyła projekt tej ustawy, a zatem trwają dalsze prace legislacyjne nad tym projektem.

Po przeprowadzeniu analizy *projektu założeń projektu ustawy o zmianie ustawy o księgach wieczystych i hipotece*<sup>75</sup> GODO wskazał, że wymaga dogłębnego rozważenia prezentowane przez projektodawcę stanowisko, jakoby udostępnianie w sieci Internet wszystkich danych zawartych w księgach wieczystych (w tym danych osobowych w rozumieniu ustawy o ochronie danych osobowych) stanowiło właściwą realizację zasady jawności ksiąg wieczystych, statuowanej w art. 2 ustawy z dnia 6 lipca 1982 roku o księgach wieczystych i hipotece (Dz. U. z 2001 r. Nr 124, poz. 1361 z późn. zm.). Generalny Inspektor Ochrony Danych Osobowych w swojej dotychczasowej praktyce zawsze stanowczo występował przeciwko utożsamianiu pojęć „jawność” i „powszechna dostępność” w odniesieniu do udostępniania danych osobowych<sup>76</sup>. Organ do spraw ochrony danych osobowych zwrócił także uwagę na kwestię proporcjonalności i niezbędności zaproponowanego rozwiązania w stosunku do celu, który za jego pomocą projektodawca chce osiągnąć (zwłaszcza wobec zakresu danych, jaki na być publikowany za pomocą sieci Internet), a także na pominięte w projekcie założeń kwestie rozwiązań technicznych i organizacyjnych, jakie będą zastosowane przez Ministra Sprawiedliwości dla zapewnienia bezpieczeństwa Centralnej Bazy Danych Ksiąg Wieczystych. W szczególności jej ochrony przed nieuprawnionym dostępem osób trzecich, zniszczeniem oraz utratą danych.

GODO zamierza nadal aktywnie uczestniczyć w pracach dotyczących przedmiotowego projektu założeń i w procesie opiniowania tworzonych przepisów prawa regulujących udostępnianie ksiąg wieczystych w Internecie. W związku z tym zwrócił się do projektodawcy o przesyłanie zarówno kolejnych wersji samego projektu założeń, jak i projektu ustawy o zmianie ustawy o księgach wieczystych i hipotece oraz projektu rozporządzenia wykonawczego do tej ustawy, po ich sporządzeniu. GODO zastrzegł sobie przy tym prawo do zgłaszania uwag do tych projektów na każdym etapie prac legislacyjnych.

W roku sprawozdawczym 2010, Generalny Inspektor Ochrony Danych Osobowych poddał analizie prawnej *Umowę między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych*

---

<sup>75</sup> DOLiS-033-51/10

*Ameryki Północnej o współpracy w zwalczaniu przestępczości, w szczególności przestępczości zorganizowanej*<sup>77</sup>. W opinii do projektu tej ustawy poinformował, że wiążące Rzeczpospolitą Polską na mocy Traktatu o przystąpieniu do Unii Europejskiej przepisy prawa europejskiego, w zwłaszcza dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 23.11.1995, s. 31 z późn. zm.), nakładają na niezależny organ do spraw ochrony danych osobowych obowiązek szczególnego kontrolowania umów międzynarodowych zawieranych przez Rzeczpospolitą Polską, w szczególności tych, przewidujących przekazywanie danych osobowych do państw trzecich. Uwzględniając fakt, że Stany Zjednoczone są państwem trzecim, które na swoim obszarze nie daje gwarancji ochrony danych osobowych takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, przedmiotowa umowa będzie miała wyjątkowo istotny charakter z punktu widzenia problematyki ochrony danych osobowych, a co za tym idzie – jej postanowienia muszą podlegać wnikliwej analizie Generalnego Inspektora. Projektowana *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki Północnej o współpracy w zwalczaniu przestępczości, w szczególności przestępczości zorganizowanej*, powinna zawierać w swojej treści unormowania, które zapewnią wysoki i adekwatny do charakteru przetwarzanych danych osobowych, poziom ich ochrony. Jest to szczególnie istotna kwestia, jeśli zauważyć, iż umowa ta ma być ratyfikowana za uprzednią zgodą wyrażoną w ustawie, a zatem w przypadku kolizji jej przepisów z postanowieniami ustaw polskich (w tym również ustawy o ochronie danych osobowych) będzie miała ona pierwszeństwo i będzie wyłączać stosowanie polskich regulacji. Kontynuując korespondencję w sprawie, GODO podtrzymał opinię, że zamieszczenie w projekcie umowy węższego niż w polskiej ustawie o ochronie danych osobowych, katalogu danych podlegających szczególnej ochronie, wpłynie negatywnie na poziom ochrony przekazywanych na jej podstawie danych dotyczących skazań oraz informacji o kodzie genetycznym.

W tym miejscu dodać można, że analogicznie jak w latach poprzednich, jednym z przykładów projektów opiniowanych przez Generalnego Inspektora Ochrony Danych Osobowych były również umowy bilateralne zawierane przez Rząd Rzeczypospolitej Polskiej o wzajemnej ochronie informacji niejawnych<sup>78</sup>.

Przeprowadzona szczegółowa analiza *projektu ustawy o dowodach osobistych* pozwoliła stwierdzić, iż unormowania w nim przyjęte stanowią niemal dosłowne powtórzenie rozwiązań

---

<sup>76</sup> Na praktyczne aspekty tego problemu wskazywał Minister Sprawiedliwości w piśmie z dnia 28 czerwca 2010 roku (znak: DL-P-II-4105-7/10) skierowanym do GODO niedługo po uruchomieniu Podsystemu Dostępu do Centralnej Bazy Danych Ksiąg Wieczystych.

<sup>77</sup> DOLiS-033-134/10 i DOLiS-033-234/10.

<sup>78</sup> Np. projekt wniosku o udzielenie przez Radę Ministrów zgody na podpisanie umowy między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o wzajemnej ochronie informacji niejawnych (DOLiS-033-115/10),

zaproponowanych w dokumencie *Projekt założeń projektu ustawy o dowodach osobistych (pl. ID)*, który był uzgadniany z organem do spraw ochrony danych osobowych w 2009 r. W związku z udziałem w opiniowaniu projektu tej ustawy również w 2010 r., GODO wystąpił o zwrócenie szczególnej uwagi na konieczność uwzględniania organu do spraw ochrony danych osobowych w procedurze uzgodnień międzyresortowych, co zaowocowało inicjatywą MSWiA wystąpienia do Kancelarii Prezesa Rady Ministrów o zmianę uchwały – Regulamin pracy Rady Ministrów. Zmiana przedmiotowej uchwały dotyczyła zapewnienia organowi do spraw ochrony danych osobowych udziału we wszystkich pracach legislacyjnych dotyczących projektów mogących mieć wpływ na problematykę ochrony danych osobowych. W toku prac prowadzonych w 2009 r. Generalny Inspektor Ochrony Danych Osobowych nie zgłosił uwag do tego projektu. Wyraził jednak opinię w przedmiocie utworzenia przez Ministerstwo Spraw Wewnętrznych i Administracji zbioru obejmującego serie i numery wszystkich unieważnionych dowodów. GODO stwierdził, że przyjęcie takiego rozwiązania wychodzi naprzeciw potrzebom zgłaszanym przez jednostki samorządu terytorialnego oraz podmioty gospodarcze. Bezspornym jest bowiem, że utworzenie przez organ publiczny zbioru obejmującego serie i numery wszystkich unieważnionych dowodów osobistych w sposób istotny poprawiłoby bezpieczeństwo obrotu prawnego w Polsce oraz mogłoby utrudnić osobom nieuczciwym dokonywanie kradzieży tożsamości. Dlatego też GODO poparł inicjatywę uzupełnienia projektu dokumentu *Projekt założeń projektu ustawy o dowodach osobistych (pl. ID)* o kwestie dotyczące wykazu unieważnionych dowodów osobistych.

GODO zadeklarował pełną współpracę w tej dziedzinie, biorąc jednocześnie pod uwagę, iż ogólna dostępność wykazu unieważnionych dowodów osobistych budzi pewne wątpliwości z punktu widzenia ochrony danych osobowych. W związku z przyjętym stanowiskiem organu do spraw ochrony danych osobowych w kwestii utworzenia przez Ministerstwo Spraw Wewnętrznych i Administracji zbioru wszystkich unieważnionych dowodów osobistych, projektodawcy zaproponowali następujące rozwiązania: wykaz będzie obejmował serie i numery wszystkich unieważnionych dowodów osobistych oraz utraconych niespersonalizowanych blankietów dowodów osobistych, dane te będą się znajdować na stronie internetowej, dostęp do tej strony wymagać będzie uwierzytelnienia podpisem elektronicznym opatrzonym certyfikatem kwalifikowanym lub certyfikatem podpisu osobistego zawartym w nowym dowodzie osobistym, a po uwierzytelnieniu pytający będzie zobligowany podać serię i numer poszukiwanego dowodu osobistego. W odpowiedzi uzyska tylko odpowiedź „Tak” lub „Nie” w kwestii istnienia bądź braku określonego dokumentu w wykazie unieważnionych dowodów osobistych oraz utraconych niespersonalizowanych blankietów dowodów osobistych. Fakt skorzystania przez konkretną osobę z tego wykazu podlegać będzie odnotowaniu.



W ocenie GODO unormowania powyżej opisane w pełni realizują wytyczne organu do spraw ochrony danych osobowych odnośnie zapewnienia kontroli nad dostępem do danych zgromadzonych w przedmiotowym zbiorze, w związku z czym GODO uznał projekt za zgodny z przepisami ustawy o ochronie danych osobowych.

Na uwagę zasługuje także rozpoczęta z końcem 2010 r. praca GODO nad opinią w sprawie *projektu ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej*<sup>79</sup>, do której Generalny Inspektor zgłosił zasadnicze zastrzeżenia. Argumentacja organu do spraw ochrony danych osobowych skupiła się w szczególności na kwestii wdrożenia *decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 roku w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych* (Dz. Urz. UE L 350 z 30.12.2008 r. s. 60). Niestety, Ministerstwo Spraw Wewnętrznych i Administracji dopiero na wysoce zaawansowanym etapie prac dotyczących wdrożenia do polskiego porządku prawnego wspomnianej decyzji, zwróciło się do GODO z prośbą o wyrażenie opinii. Generalny Inspektor podniósł, że gdyby przedmiotowa sprawa została przedstawiona przez MSWiA wcześniej, być może pewne wątpliwe kwestie mogłyby zostać już dawno wyjaśnione, zaś GODO nie musiałby sięgać po tak drastyczny środek, jakim jest negacja projektu w całości. Przeprowadzona bowiem szczegółowa analiza przedstawionych rozwiązań prowadziła do wniosku, że zaproponowana przez Ministerstwo Spraw Wewnętrznych i Administracji formuła polegająca na implementacji w jednej ustawie szeregu aktów prawnych Unii Europejskiej nie była rozwiązaniem dobrym i celowym. Z tego powodu Generalny Inspektor uznał przedstawiony *projekt ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej* za niemożliwy do zaakceptowania. Zaproponował natomiast odrębne wdrożenie *decyzji ramowej* poprzez dokonanie całościowego przeglądu obowiązującej ustawy o ochronie danych osobowych i ustalenie, które przepisy *decyzji ramowej* są już do niej wdrożone, implementacja których wymagałaby zmian ustawy o ochronie danych osobowych, a które przepisy *decyzji ramowej 2008/977/WSiSW* mają na tyle szczególny charakter, iż ich odpowiedniki winny znaleźć się w ustawach szczególnych regulujących funkcjonowanie poszczególnych organów ścigania czy służb.

Generalny Inspektor zadeklarował pełną współpracę i współdziałanie z projektodawcami przy dokonaniu powyższego przeglądu<sup>80</sup>. Szczegółowa analiza innych koniecznych zmian i dostosowań będzie przedmiotem dalszych prac organu do spraw ochrony danych osobowych i zostanie

---

<sup>79</sup> DOLiS-033-452/10

<sup>80</sup> Zapewnienie prawidłowego wdrożenia art. 25 *decyzji ramowej 2008/977/WSiSW*, wymagać będzie usunięcia z ustawy o ochronie danych osobowych zapisów ograniczających uprawnienia Generalnego Inspektora Ochrony Danych Osobowych przewidzianych w art. 15 ust. 2, art. 18 ust. 2 a i art. 43 ust. 2 tejże ustawy oraz wprowadzenia do niej odpowiednika art. 17 ust. 1 pkt b wspomnianej decyzji ramowej. W związku z art. 13 tego dokumentu konieczna będzie także zmiana przepisów ustawy o ochronie danych osobowych dotyczących przekazywania danych osobowych do państwa trzeciego (art. 47 ust. 1).

przedstawiona w przypadku zaakceptowania przez Ministerstwo Spraw Wewnętrznych i Administracji zaproponowanej koncepcji wdrożenia *decyzji ramowej 2008/977/WSiSW*. W działaniach tych ze strony Generalnego Inspektora Ochrony Danych Osobowych mogą uczestniczyć również osoby mające wieloletnie doświadczenie w pracy Wspólnych Organów Nadzorczych dla EUROPOLu, EURODACu oraz organów prowadzących bazy policyjne i sądowe. Niestety MSWiA nie zaakceptowało tej koncepcji. Aktualnie GODO po raz kolejny negatywnie zaopiniował ten projekt<sup>81</sup>.

**Podsumowując działalność Generalnego Inspektora Ochrony Danych Osobowych w zakresie opiniowania projektów znajdujących się na różnych etapach procesu legislacyjnego warto zwrócić uwagę na kilka kwestii generalnych,** które mają wpływ na jakość tworzonego prawa z punktu widzenia zasad ochrony danych osobowych.

- a) Liczba projektów legislacyjnych poddanych opiniowaniu GODO utrzymuje się na stałym – bardzo wysokim – poziomie. Powoduje to, że Generalny Inspektor uczestniczy jednocześnie w co najmniej kilkudziesięciu działaniach legislacyjnych, w których nie może pozostać bierny. Wymaga to stałego zdobywania przez pracowników Biura Generalnego Inspektora wiedzy w sprawach merytorycznych związanych praktycznie z całym spektrum polskiej legislacji.
- b) Wciąż dochodzi do sytuacji, gdy akty prawne nie są zgłaszane do opiniowania Generalnemu Inspektorowi na etapie przygotowania założeń lub projektu aktu, co powoduje, że GODO przyłącza się do dyskusji na zbyt późnym etapie pracy i bywa traktowany jako „przeszkadzający w sprawnym procesie legislacyjnym”, mimo że większość uwag GODO jest uwzględniana jako słuszne.
- c) Zdarza się, że ustawy są przyjmowane przez obie izby Parlamentu bez zapoznania się z opinią Generalnego Inspektora Ochrony Danych Osobowych, mimo że są w oczywisty sposób związane z budową elementów infrastruktury informacyjnej Państwa oraz ze scentralizowanym przetwarzaniem dużej liczby danych osobowych, a nawet wydawaniem decyzji przy użyciu automatycznego przetwarzania danych w systemach teleinformatycznych. Bardzo niepokojącym przykładem takiego działania było przyjęcie ustawy o zmianie ustawy Prawo o ruchu drogowym, której zadaniem było stworzenie podstaw prawnych do budowy Zautomatyzowanego Systemu Informacji o Zdarzeniach Drogowych.
- d) Bardzo pozytywnie ocenić należy współpracę z Komisjami Sejmowymi i Senackimi, które – jeśli GODO włączony został do procesu opiniodawczego – bardzo szczegółowo rozważają

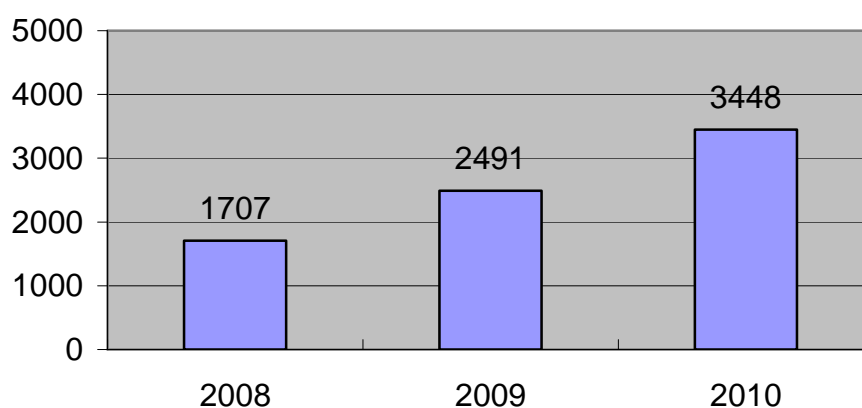
---

<sup>81</sup> Pismo z dnia 24 marca 2011 r. o sygn. 033-452/10/13212/11.

opinie GIODO. Nawet jeśli posłowie lub senatorowie nie podzielają opinii Generalnego Inspektora, biorą ją pod uwagę przy podejmowanych decyzjach.

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

Udzielanie odpowiedzi na pytania dotyczące legalności przetwarzania danych osobowych stanowi istotny element działalności informacyjnej i edukacyjnej Generalnego Inspektora Ochrony Danych Osobowych. Należy przy tym wskazać, że problematyka ta pozostaje przedmiotem zainteresowania szerokiej i zarazem zróżnicowanej grupy interesantów i że zainteresowanie to systematycznie wzrasta. W analizowanym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **3448 pytań prawnych** z prośbą o interpretację obowiązujących w obszarze ochrony danych osobowych przepisów prawa, bądź sygnalizujących różnego rodzaju problemy związane z przestrzeganiem przepisów dotyczących ochrony danych. Porównanie liczby pytań skierowanych do Generalnego Inspektora w latach 2008–2010 przedstawia Wykres 31.



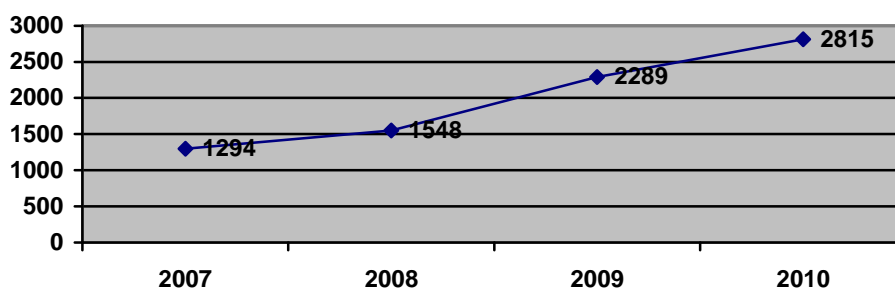
Wykres 31: *Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GIODO w latach 2008–2010.*

W porównaniu z ubiegłym rokiem, w okresie objętym sprawozdaniem o 957 zwiększyła się liczba pytań wpływających do organu do spraw ochrony danych osobowych. Należy to uznać za rezultat aktywności i zaangażowania organu ds. ochrony danych osobowych w popularyzację zasad ochrony danych i prawa do prywatności poprzez udzielanie wywiadów, porad prawnych, publikacje, a także organizację konferencji, spotkań i szkoleń poświęconych tej tematyce. Zagadnienia te będą przedstawione w dalszej części Sprawozdania zatytułowanej „Działalność informacyjna”. Charakterystyczny jest dwukrotny wzrost liczby pytań w ciągu ostatnich dwóch lat. Odpowiedź na coraz bardziej precyzyjne pytania dotyczące trudnych kwestii prawnych – często związanych z

zastosowaniem nowych technologii teleinformatycznych – stanowi bardzo ważną część pracy Biura Generalnego Inspektora. Zadanie to realizowane jest bez możliwości powiększania zespołu merytorycznego.

Warto zwrócić uwagę na zagadnienie, które nie sposób nazwać wprost „problemem”, a które jednak budzi pewien niepokój z punktu widzenia organizacji pracy Biura. Coraz większa liczba pytań kierowana jest do Biura GIODO przez podmioty wykonujące zawodowo działalność prawniczą lub oferujących usługi konsultacyjne. Podmioty te stają się *de facto* pośrednikiem w przekazywaniu informacji dotyczących zasad ochrony danych osobowych. Oferując swym klientom usługi komercyjne, które mają polegać na rozwiązywaniu problemów prawnych, wykonują je poprzez zasięganie opinii w Biurze GIODO, przekazując swym klientom – za opłatą – informacje przekazane przez Biuro GIODO w ramach działalności informacyjnej i edukacyjnej Generalnego Inspektora Ochrony Danych Osobowych. Biuro Generalnego Inspektora nie może odmówić udzielenia informacji podmiotom wykonującym zawodowo działalność prawniczą lub oferującym usługi konsultacyjne. Co więcej kontakt z takimi podmiotami jest bardzo wskazany. Przy organizacji pracy Biura należy wszakże pamiętać, że wzrastająca liczba pytań dotyczących legalności przetwarzania danych osobowych jest w dużej mierze spowodowana zwiększającą się liczbą zapytań ze strony podmiotów pośredniczących pomiędzy Biurem a podmiotami przetwarzającymi dane osobowe lub zaniepokojonych sposobem przetwarzania ich danych osobowych.

W przypadku korespondencji wychodzącej należy wskazać, że w 2010 r. pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych przygotowali łącznie 2815 wystąpień oraz odpowiedzi na pytania prawne kierowane do organu. Oznacza to ponad dwukrotny wzrost (218 %) w porównaniu z 2007 r.



**Wykres 32: Zestawienie liczbowe korespondencji wychodzącej z Biura Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2010 w odniesieniu do wystąpień i pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych.**

## 6.1. Interpretacja przepisów

Przedstawiona poniżej analiza pytań, które w 2010 r. wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych, w głównej mierze dotyczyć będzie problematyki przetwarzania danych osobowych w dziedzinach związanych z szeroko rozumianym rozwojem technologicznym. Z uwagi na kryterium, jakim był sposób przetwarzania danych osobowych, pytania te podzielone zostały na dwie zasadnicze grupy. Pierwszą grupę stanowiły pytania dotyczące przetwarzania danych osobowych za pośrednictwem sieci Internet, drugą zaś – pytania związane z wykorzystaniem systemów informatycznych i monitoringu przy przetwarzaniu danych. Trzecią zaś grupę będą stanowiły pytania prawne, które z uwagi na treść nie mogły zostać zakwalifikowane do dwóch wcześniejszych.

### 6.1.1. Przetwarzanie danych osobowych za pośrednictwem sieci Internet

W dobie szybko rozwijającej się technologii komputerowej, z uwagi na wzrastającą potrzebę sprawnej wymiany informacji, coraz częściej dane osobowe są przetwarzane w sieci Internet. Osoby prywatne, podmioty gospodarcze oraz instytucje państwowe, powszechnie korzystają z udogodnień dostarczanych przez Internet, aby szybciej i sprawniej realizować własne zadania. Dzięki temu sposobowi przetwarzania danych osobowych wykonuje się operacje na coraz większej liczbie danych, często w zakresie nie tylko danych zwykłych, ale także danych szczególnie chronionych.

Oprócz wielu zalet, Internet niesie ze sobą również zagrożenia, zwłaszcza w dziedzinie przetwarzania danych osobowych. W związku z tym wiele pytań kierowanych do Generalnego Inspektora w 2010 r. dotyczyło wydania opinii potwierdzającej prawidłowość przetwarzania danych osobowych za pośrednictwem sieci publicznych.

Jednym z pierwszych wystąpień będących reakcją na sygnały wskazujące na nieprawidłowości w wypełnianiu obowiązków wynikających z ustawy o ochronie danych osobowych, było wystąpienie z dnia 15 stycznia 2010 r. kierowane do **Termedia Sp. z o.o.**<sup>82</sup>. Ustalono bowiem, że w treści strony rejestracyjnej należącej do ww. podmiotu znajdowała się klauzula zgody na przetwarzanie danych osobowych, która nie spełniała warunków wskazanych w art. 7 ustawy o ochronie danych osobowych. Zgodnie z brzmieniem tego przepisu, przez zgodę osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, i że zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. W opisywanym przypadku wyrażenie zgody na przetwarzanie danych osobowych utożsamiane było z czynnością wypełnienia formularza rejestracyjnego. W treści

pisma skierowanego do Prezesa Termedia Sp. z o. o. Generalny Inspektor Ochrony Danych Osobowych powołał się na dwa wyroki Naczelnego Sądu Administracyjnego<sup>83</sup> stanowiące o tym, jakie warunki spełniać powinna klauzula zgody na przetwarzanie danych osobowych. Podkreślił również, że administrator danych może przetwarzać dane w celu marketingu własnych produktów i usług bez konieczności pozyskiwania zgody od osób, których dane przetwarza w tym celu. Ponadto Generalny Inspektor zwrócił uwagę, że w oświadczeniu zamieszczonym na stronie internetowej tej spółki, niesprecyzowany został w sposób wyraźny cel, dla którego podmiot ten pozyskuje zgodę. Określenie „cel informatyczny” brzmi bowiem nazbyt abstrakcyjnie, co narusza zasady wynikające z przepisów o ochronie danych osobowych. Organ ds. ochrony danych osobowych wskazał, iż niedopuszczalnym rozwiązaniem jest pozyskiwanie w jednej klauzuli (oświadczeniu) zgody na przetwarzanie danych „w celach informatycznych” przez „firmy współpracujące” i „inne podmioty”. Ma to bowiem znaczenie w kontekście legalności procesu przetwarzania danych oraz niezbędności (konieczności), bądź zbędności, pozyskiwania zgody na przetwarzanie danych od osób, których te dane dotyczą. Spółka poinformowana została również o obowiązku wynikającym z art. 24 ustawy o ochronie danych osobowych. Przepis ten wyraźnie mówi, że 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. Prezes Termedia Sp. z o. o. przedstawił zmodyfikowaną treść regulaminu odnoszącą się do zakwestionowanych przez Generalnego Inspektora Ochrony Danych Osobowych postanowień, oświadczając tym samym, że dane osobowe pozyskiwane przez Spółkę przetwarzane będą z prawem.

W 2010 r. wpłynęło pismo od **Ministra Infrastruktury** o wydanie opinii prawnej dotyczącej publikacji na stronie internetowej ministerstwa danych osobowych - w tym danych dotyczących skazań - rzeczoznawców majątkowych, pośredników w obrocie nieruchomościami oraz zarządców nieruchomości. Generalny Inspektor w opinii z dnia 23 marca 2010 r.<sup>84</sup> wskazał, iż jakiegokolwiek przetwarzanie danych osobowych jest dopuszczalne tylko po spełnieniu jednej z przesłanek wskazanych w art. 23 ust. 1 pkt 1 – 5 ustawy o ochronie danych osobowych, zaś w odniesieniu do danych tzw. szczególnie chronionych (tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub

---

<sup>82</sup> DOLiS-035-78/10/1760

<sup>83</sup> Wyrok z dnia 4 kwietnia 2003 r. sygn. akt II SA 2135/2002 oraz wyrok z dnia 11 kwietnia 2003 r. sygn. akt: II SA 3942/2004.

związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym) - w art. 27 ust. 2 pkt 1 – 10 tejże ustawy. Przepisy wspomnianego aktu zabraniają również przetwarzania danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Natomiast administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Jawność i dostępność danych osobowych osób, którym nadano uprawnienia i licencje zawodowe w zakresie gospodarowania nieruchomościami, gwarantuje ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (Dz. U. z 2004 r. Nr 261, poz. 2603 z późn. zm.). Obecnie obowiązujące przepisy tej ustawy wyraźnie wskazują, jaki zakres danych osobowych i w jaki sposób może być udostępniany przez ministra właściwego do spraw budownictwa. Generalny Inspektor wyraźnie podkreślił, iż regulacje te nie przewidują możliwości udostępniania za pośrednictwem strony internetowej ministerstwa danych osobowych zarządców, pośredników, czy rzeczoznawców majątkowych w zakresie informacji o orzeczonych wobec nich karach dyscyplinarnych. Zakres podlegających udostępnieniu danych osobowych dotyczących osób, którym nadano uprawnienia i licencje zawodowe w zakresie gospodarowania nieruchomościami, wynika wprost z przepisów ustawy o gospodarce nieruchomościami. Udostępnienie ich w szerszym zakresie będzie możliwe jedynie po zmianie stosownych przepisów prawa.

Kolejnym istotnym wystąpieniem Generalnego Inspektora Ochrony Danych Osobowych dotyczącym publikacji danych osobowych w sektorze administracji państwowej za pomocą Internetu, było wystąpienie z dnia 3 sierpnia 2010 r.<sup>84</sup>. Organ ds. ochrony danych osobowych zwrócił się do **Ministra Finansów** z prośbą o podjęcie prac legislacyjnych mających na celu zawężenie zakresu publikacji danych określonych w art. 76g ust. 1 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2009 r., Nr 152, poz. 1223). Na podstawie tego przepisu prowadzony jest przez ministra właściwego do spraw finansów publicznych wykaz osób, które uzyskały certyfikat księgowy, zawierający imię i nazwisko, numer certyfikatu księgowego, numer PESEL - a w przypadku osób nieposiadających obywatelstwa polskiego - numer i rodzaj dokumentu tożsamości. Wykaz, o którym mowa w ust. 1, i dokonywane w nim zmiany, zamieszczany był w celach informacyjnych na stronie internetowej urzędu obsługującego Ministra właściwego do spraw finansów publicznych. Pozostawał więc do wglądu nieograniczonej liczby odbiorców, umożliwiając tym samym przetwarzanie zawartych w nim danych. Generalny Inspektor uznał, iż komentowany przepis ustawy o rachunkowości dotyczy

---

<sup>84</sup> DOLiS-035-494/10

<sup>85</sup> DOLiS-035-1858/10/30789

udostępniania informacji stanowiących dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych. Mając na uwadze wyżej wskazany zakres informacji o osobach posiadających certyfikat księgowy, a także analizując jedynie informacyjny cel ich publikacji wynikający z powołanego przepisu ustawy o rachunkowości, wskazano, że do spełnienia tak określonego celu wystarczyłaby publikacja danych w zakresie wyłącznie imienia, nazwiska oraz numeru certyfikatu księgowego. Analizując przedmiotową sprawę Generalny Inspektor odniósł się do wynikającej z art. 26 ustawy o ochronie danych osobowych zasady adekwatności oraz zasady związania celem. Stanowią one, że administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane osobowe zbierane były dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2. Zwrócił również uwagę na normy konstytucyjne wynikające z art. 47 Konstytucji Rzeczypospolitej Polskiej, które wyraźnie mówią, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Generalny Inspektor Ochrony Danych Osobowych stwierdził, że choć funkcja pełniona przez osoby wykonujące zawód księgowy bez wątpienia ma doniosłe znaczenie dla prawidłowego obrotu gospodarczego i zrozumiałe jest publikowanie danych osobowych osób wyspecjalizowanych w tej profesji dla celów informacyjnych, to jednak zamieszczanie w Internecie numeru PESEL bądź numeru i rodzaju dokumentu potwierdzającego ich tożsamość nie jest konieczne dla wypełnienia tego celu. Minister Finansów zgodził się z argumentacją przedstawioną przez organ ds. ochrony danych osobowych i zapewnił, iż w przyszłości uwagi zostaną uwzględnione w pracach legislacyjnych nad zmianą przepisów ustawy o rachunkowości.

W dniu 27 grudnia 2010 r. GODO skierował do **proboszcza Parafii św. Mikołaja Biskupa we Wleniu** wystąpienie<sup>86</sup> dotyczące praktyki upubliczniania na stronie internetowej Parafii, imion i nazwisk osób, które sprzątały kościół i tych, które kościoła nie sprzątały. Kościół Katolicki, jak i inne związki wyznaniowe, są w zakresie swojej działalności niezależne i przy wykonywaniu władzy duchownej posługują się swoim wewnętrznym prawem. Nie oznacza to jednak, że są zwolnione z obowiązku respektowania przepisów obowiązujących ustaw, w tym ustawy o ochronie danych osobowych. W piśmie do proboszcza Generalny Inspektor przypomniał, że wszelkie działania ograniczające prawo do prywatności i ochrony danych osobowych, zaliczonych do konstytucyjnych wolności i praw osobistych człowieka i obywatela, powinny znajdować ustawową podstawę. W opisanym przypadku podstawą udostępnienia informacji, które mogą prowadzić do identyfikacji osoby fizycznej na stronie internetowej Parafii, do której dostęp ma nieograniczona liczba

---

<sup>86</sup> DOLiS-035-3381/10/51157



użytkowników, mogłaby być jedynie zgoda osoby, której dane dotyczą (art. 23 ust.1 pkt 1, art. 27 ust. 2 pkt 1 ustawy). Udostępnienie danych osobowych w sieci prowadzić może nie tylko do naruszenia dóbr materialnych, ale i żywotnych interesów osób. W treści wystąpienia przypomniano również, iż Generalny Inspektor oraz Sekretarz Generalny Konferencji Episkopatu Polski podpisali w dniu 23 września 2009 r. instrukcję pt. „Ochrona danych osobowych w działalności Kościoła Katolickiego w Polsce”. Instrukcja ta stanowi swego rodzaju kodeks dobrych praktyk zawierający podstawowe zasady, jakimi należy się kierować przy przetwarzaniu danych osobowych w działalności kościoła. Podobny dokument został przygotowany dla Polskiego Autokefalicznego Kościoła Prawosławnego we współpracy z Prawosławnym Metropolitą Warszawskim i Całej Polski<sup>87</sup>.

Pytanie, czy do danych osobowych można zakwalifikować pliki znane pod angielską nazwą *flash cookies (cookies)*, zadała Generalnemu Inspektorowi **QXL Poland Sp. z o.o.** Pliki te wykorzystywane są na stronach zawierających obiekty *flash* np. bandery reklamowe, gry itp. i służą głównie do automatycznego rozpoznawania przez serwer określonego użytkownika w celu wygenerowania dla niego odpowiednio zindywidualizowanej strony www. Taka funkcjonalność pozwala w praktyce na precyzyjne śledzenie aktywności sieciowej konkretnego użytkownika i budowanie profili behawioralnych wykorzystywanych następnie dla potrzeb dostarczenia spersonalizowanych reklam internetowych. Zakres informacji, które mogą być zapisane w pliku *flash cookies* jest znacznie szerszy niż w tradycyjnym pliku *cookie*, co zwiększa prawdopodobieństwo, że zarejestrowane w ten sposób informacje będą wystarczające do ustalenia tożsamości określonego użytkownika. Ciasteczka *flashowe* nie mogą być przeglądane oraz kasowane przez użytkownika. Brak możliwości zablokowania *flash cookies*, ani też ustawienia daty ich wygaśnięcia za pomocą opcji ochrony prywatności wbudowanych standardowo w przeglądarki internetowe, stanowi poważne niebezpieczeństwo dla tego prawa. Nierzadko użytkownik sieci nie jest w ogóle świadomy ich istnienia. Kolejnym ryzykiem związanym ze stosowaniem ciasteczek *flash* jest funkcjonalność, która pozwala za ich pomocą odtwarzać zwykłe pliki *cookies* usunięte wcześniej przez użytkownika. *Flash cookies* są zapisywane nie tylko przez strony, które użytkownik odwiedza świadomie, ale również przez tzw. strony trzecie (t.j. kod podlinkowany z innej strony www.). Odpowiadając na pytanie QXL Poland Sp. z o.o., Generalny Inspektor Ochrony Danych Osobowych przywołał Opinię 1/2008 Grupy Roboczej Art. 29 dotyczącą zagadnień ochrony danych związanych z wyszukiwarkami, zgodnie z którą plik typu *cookies* może należeć do kategorii danych, na podstawie których możliwe będzie zidentyfikowanie osoby, której on dotyczy. Wykorzystanie trwałych plików *cookies* lub podobnych instrumentów zawierających niepowtarzalny identyfikator użytkownika, pozwala na śledzenie użytkowników określonego

---

<sup>87</sup> W dniu 22 marca 2011 r. dr Wojciech R. Wiewiórowski, GODO, i Metropolita Sawa, Prawosławny Metropolita Warszawski i całej Polski, podpisali dokument pt. „Zalecenia opracowane przez Generalnego Inspektora Ochrony Danych Osobowych i Sobór Biskupów Polskiego Autokefalicznego Kościoła Prawosławnego”. Zalecenia określają zasady ochrony danych osobowych w działalności Polskiego Autokefalicznego Kościoła Prawosławnego, wskazując na prawa i obowiązki

komputera nawet w przypadku, gdy korzysta on z dynamicznych adresów IP. Dane na temat zachowań użytkownika sieci, generowane przy wykorzystaniu takich instrumentów, pozwalają na szczegółowe poznanie zainteresowań, a nawet pewnych cech osobowościowych internauty. Trwałe pliki *cookies* zawierające niepowtarzalny identyfikator użytkownika komputera – zgodnie z ww. opinią 1/2008 – mogą należeć do kategorii danych, na podstawie których można ustalić tożsamość osób, których one dotyczą. W takim rozumieniu mogą stanowić dane osobowe. Zgodnie zatem z przytoczoną definicją danych osobowych, będą to dane, które umożliwiają identyfikację osób, których dotyczą, natomiast same ich nie identyfikują. Kwestia uznania tych informacji za daną osobową jest zależna od charakteru, okoliczności, sposobu i celu, w jakim te dane są zbierane i wykorzystywane.

W 2010 roku szczególnym zainteresowaniem wśród pytających cieszył się również temat dotyczący **legalności przetwarzania danych osobowych przez portal WHOIS**<sup>88</sup>. Jedno z pierwszych wystąpień GIODO w tej sprawie miało miejsce 16 lutego 2010 r.<sup>89</sup>. Baza WHOIS jest powszechnie dostępną bazą danych o abonentach domen internetowych i podmiotach rejestrujących domeny internetowe. Głównym celem prowadzenia takiej bazy jest zapewnienie poszanowania praw użytkowników Internetu, właścicieli znaków towarowych, praw autorskich i innych dóbr chronionych prawem. Zakres danych abonenta powszechnie dostępnych w bazie WHOIS obejmuje imię i nazwisko, adres pocztowy, miasto, adres poczty elektronicznej oraz numer telefonu. Właściciel portalu WHOIS jest akredytowanym rejestratorem nazw domen internetowych, działającym w oparciu o porozumienie zawarte pomiędzy rejestratorem i ICANN (Internet Corporation for Assigned Names and Numbers). ICANN to podmiot odpowiedzialny za przyznawanie nazw domen internetowych, ustalanie ich struktury oraz sprawujący ogólny nadzór nad działaniem serwerów Domain Name Servers na całym świecie. Występuje w procesie rejestracji nazwy domenowej w charakterze partnera, tj. podmiotu upoważnionego przez abonenta do reprezentowania go przed rejestratorem (w tym przypadku – przed ICANN) w oparciu o stosowne porozumienie. Rejestrator ma prawo do przetwarzania danych osobowych abonenta w zakresie wskazanym w art. 4 przedmiotowej umowy. Na mocy tego przepisu, w celu dokonania rejestracji abonent zobowiązuje się podać za pośrednictwem partnera swoje imię i nazwisko (albo pełną nazwę w przypadku podmiotów nie będących osobami fizycznymi), adres zamieszkania lub siedziby, numer PESEL albo inny numer ewidencyjny w sposób jednoznaczny identyfikujący abonenta, adres poczty elektronicznej, numer telefonu oraz numer faksu o ile występuje. Przekazanie ww. danych jest niezbędne w celu rejestracji domeny oraz przekazania ich do ICANN przez partnera w związku z koniecznością wykonania obowiązków rejestratora wynikających z umowy akredytacyjnej zawartej z ICANN, o czym partner powinien poinformować abonenta. Niezależnie od obowiązku przekazywania przez rejestratorów nazw domen internetowych abonentów do bazy danych

---

kościelnych osób prawnych, o których mowa w Ustawie z dnia 4 lipca 1991 r. o stosunku Państwa do Polskiego Autokefalicznego Kościoła Prawosławnego, w sprawach dotyczących bezpieczeństwa przetwarzanych danych osobowych.

<sup>88</sup> DOLiS-035-660/10, DOLiS-035-2173/10, DOLiS-035-2360/10.

WHOIS, podmioty takie oferują często usługę polegającą na ograniczeniu zakresu lub ukryciu danych abonenta, dostępnych w wynikach bazy WHOIS – tzw. usługa ID PROTECT. W przypadku skorzystania z takiej usługi w bazie WHOIS wyświetlane są wyłącznie dane rejestratora określonej nazwy domenowej oraz wskazanie, że jej abonentem jest osoba fizyczna (status nazwy domenowej: „INDIVIDUAL”).

Bardzo wiele pytań kierowanych do Generalnego Inspektora Ochrony Danych Osobowych dotyczyło przetwarzania danych osobowych na **forach internetowych**. Omawiając ten problem warto wskazać wystąpienie dotyczące bezprawnego opublikowania przez pracownika **Liberty Direct** na internetowym forum dyskusyjnym, danych osobowych klientów Spółki oraz powiązanych z nimi osób biorących udział w zdarzeniach komunikacyjnych<sup>89</sup>. W wystąpieniu do tego podmiotu wskazano na obowiązki administratora danych wynikające z art. 26 ust. 1 ustawy o ochronie danych osobowych. Przepis tego artykułu stanowi, że administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (z zastrzeżeniem ust. 2), merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane oraz by były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, jednak nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. GIODO odwołał się również do zasad dotyczących zabezpieczenia danych osobowych wyrażonych w art. 36 ustawy, który zobowiązuje administratora danych do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Na skutek interwencji Generalnego Inspektora władze Spółki usunęły dane bezprawnie upublicznione w Internecie przez pracownika Liberty Direct. Nie zmienia to jednak faktu, że przez pewien okres dane te były dostępne dla nieograniczonej liczby osób, które mogły je przetwarzać z naruszeniem zasad określonych w ustawie o ochronie danych osobowych, za co grozi odpowiedzialność karna. W związku z przedstawionym wystąpieniem władze Liberty Direct przekazały Generalnemu Inspektorowi Ochrony Danych Osobowych dokumentację wskazującą na dostosowanie się do zasad przetwarzania danych osobowych i zapewniły, że upublicznienie danych osobowych klientów Spółki miało charakter wyłącznie incydentalny.

---

<sup>89</sup> DOLiS-035-87/10/6606

<sup>90</sup> DOLiS-035-1565/10/ 27280

### **6.1.2. Przetwarzanie danych osobowych z zastosowaniem systemów informatycznych oraz monitoringu**

Przetwarzanie danych osobowych jest nieodzowną częścią działalności każdego pracodawcy bez względu na to, czy jest to jednostka o charakterze publicznym, czy prywatnym. Z oczywistych względów w interesie każdego pracodawcy leży usprawnienie procesu przetwarzania danych osobowych pracowników. W związku z tym wiele takich podmiotów decyduje się na zastosowanie systemów i nośników informatycznych służących do zwiększenia efektywności przetwarzania danych.

Wyżej wskazane zagadnienie było przedmiotem wystąpienia Generalnego Inspektora Ochrony Danych Osobowych z 15 lutego 2010 r. wydanego w związku z pytaniem Ministra Pracy i Polityki Społecznej dotyczącym **legalności archiwizowania danych osobowych pracowników** (byłych i obecnych) przez pracodawców na nośnikach informatycznych. W odpowiedzi Generalny Inspektor Ochrony Danych Osobowych wskazał, że w kontekście przetwarzania danych osobowych pracowników przez pracodawców oraz formy przeprowadzania tego procesu, należy odnieść się do przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) oraz do rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286 z późn. zm.). Z treści przywołanego rozporządzenia wynika zasada prowadzenia dokumentacji dotyczącej zatrudnienia w formie pisemnej. Wskazują na to choćby takie sformułowania jak: „karta”, „lista”, „dokument”, czy „pisemne potwierdzenie”. Powyższe nie wskazuje jednak, iż prowadzenie dokumentacji pracowniczej w formie elektronicznej jest zabronione. Wysnuć można wniosek, że w obecnym stanie prawnym pracodawca mógłby prowadzić taką dokumentację, aczkolwiek dodatkowo, pomocniczo, czy też równoległe do prowadzenia jej w formie papierowej. Niemniej jednak czynnikiem decydującym o obowiązkowym prowadzeniu dokumentacji w formie pisemnej, na podstawie aktualnie obowiązujących przepisów prawa pracy, jest moc dowodowa przedmiotowej dokumentacji w kontekście np. ewentualnych sporów sądowych ze stosunku pracy. Na koniec swych rozważań Generalny Inspektor Ochrony Danych Osobowych wskazał, że w kontekście prowadzenia przez pracodawców dokumentacji pracowniczej, rozważyć należy podjęcie prac legislacyjnych mających na celu dostosowanie obowiązujących przepisów, bądź stworzenie nowych regulacji prawnych, odnoszących się wprost do elektronicznej formy prowadzenia tejże dokumentacji, przewidujących m.in. stosowne, szczególne zasady jej zabezpieczenia.

Z wielu sygnałów napływających do Generalnego Inspektora Ochrony Danych Osobowych wynika, iż zwiększa się dostępność systemów, których istotą jest przetwarzanie danych osobowych biometrycznych. Przykładem wskazanej powyżej problematyki było **przetwarzanie danych biometrycznych uczniów i nauczycieli** w jednym z zespołów szkół, w celu ograniczenia dostępu na

teren szkoły osobom nieuprawnionym. W wystąpieniu z dnia 21 stycznia 2010 r.<sup>91</sup> Generalny Inspektor wskazał, że dane biometryczne określonej osoby, takie jak np. jej linie papilarne czy obraz tęczówki oka, niewątpliwie można uznać za dane osobowe. Pozwalają one bowiem na ustalenie tożsamości osoby w sposób pewny. Z racji ich wyłącznej przynależności do konkretnej osoby, dane te stanowią swego rodzaju „identyfikator”. Analizując przedmiotowy przypadek, GODO odwołał się do opinii Grupy Roboczej Art. 29, przyjętej w dniu 1 sierpnia 2003 r. pod nazwą „Dokument Roboczy w sprawie biometrii” (12168/02/FR GT 80). Jak wskazano w przedmiotowej opinii *„(...) szybki rozwój technologii biometrycznych, jak i coraz powszechniejsze ich stosowanie w ostatnich latach, wymagają uważnej analizy z punktu widzenia ochrony danych. Powszechne i niekontrolowane posługiwanie się biometrią wzbudza niepokój z punktu widzenia ochrony wolności i fundamentalnych praw człowieka. (...) Szczególne zaniepokojenie związane z danymi biometrycznymi wzbudza ryzyko zmniejszenia wrażliwości ludzi - spowodowane coraz większą powszechnością używania tych danych - na konsekwencje, jakie przetwarzanie ich danych może mieć w życiu codziennym. Na przykład, posługiwanie się biometrią w bibliotekach może zmniejszyć świadomość dzieci, co do zagrożeń związanych z ochroną dotyczących ich danych, a to może mieć dla nich poważne konsekwencje w przyszłości. Dane biometryczne zawsze powinny być uważane za „dane dotyczące osoby fizycznej”, ponieważ odnoszą się do danych ze swej natury dotyczących określonej osoby”*. GODO przypomniał, że zakres danych osobowych, jakie pracodawca może gromadzić w związku z zatrudnieniem, został szczegółowo określony w przepisach art. 22<sup>1</sup> ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 1998 r. Nr 21, poz. 94 z późn. zm.)<sup>92</sup>. Mając na uwadze powyższe, organ ds. ochrony danych osobowych uznał, że pozyskiwanie odcisków palców, jak również porównywanie odwzorowania punktów charakterystycznych palca przez czytniki linii papilarnych z zapisanymi na nich danymi, w celu ich identyfikacji w związku z wprowadzeniem systemu dokonującego na ich podstawie kontroli dostępu do budynku (np. szkoły), narusza zasadę adekwatności przetwarzania danych, o której mowa w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Argumentując powyższą kwestię zwrócił uwagę na wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2009 r. (sygn. akt I OSK 249/09), w którym NSA orzekł, iż *„w przyjętym przez Grupę Roboczą Art. 29 w dniu 1 sierpnia 2003 r. dokumencie roboczym w sprawie biometrii przyjęto jako niezbędną zasadę proporcjonalności*

---

<sup>91</sup> DOLiS- 035-115/10/2681

<sup>92</sup> Art. 22<sup>1</sup> § 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).

*i legalności. Oznacza to, że ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności wyrażona w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników (...) jest nieproporcjonalne do zamierzonego celu ich przetwarzania*". Na podstawie powyższego stanowiska oraz w toku prowadzonej korespondencji dyrektor zespołu szkół zobowiązała się do usunięcia systemu przetwarzającego dane biometryczne uczniów i nauczycieli.

Odpowiadając na inne pytania dotyczące przetwarzania danych biometrycznych, Generalny Inspektor wskazywał na nieadekwatność takich rozwiązań dla weryfikacji czasu pracy, powołując ww. opinię Grupy Roboczej Art. 29 ds. ochrony danych osobowych oraz sądu. Organ ds. ochrony danych osobowych wielokrotnie prezentował stanowisko, iż dopuszczalne jest przetwarzanie danych biometrycznych pracowników wyłącznie w przypadku konieczności zapewnienia szczególnego bezpieczeństwa informacji bądź zasobów gromadzonych w związku z działalnością administratora danych.

Oprócz stosowania systemów bezpieczeństwa przetwarzających dane biometryczne, wiele instytucji i przedsiębiorców decyduje się na zastosowanie **monitoringu**. Mając na uwadze, że tego typu rozwiązania stanowią niebezpieczną ingerencję w prawo do prywatności, sprawy związane z monitoringiem stały się przedmiotem szczególnego zainteresowania Generalnego Inspektora Ochrony Danych Osobowych<sup>93</sup>. W jednym ze swoich wystąpień zwrócił się do władz Miejskiego Ośrodka Sportu i Rekreacji w Ostrowcu<sup>94</sup> o zaprzestanie praktyki monitorowania tego obiektu przy użyciu kamer zainstalowanych w bezpośrednim sąsiedztwie kabin służących do przebierania się. GODO przywołał art. 47 Konstytucji Rzeczypospolitej Polskiej, który stanowi, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym i że prawo to nie może doznawać ograniczeń także w stanach nadzwyczajnych. Zwrócił również uwagę na przyjętą w dniu 11 lutego 2004 r. opinię (nr 4/2004) Grupy roboczej do spraw ochrony osób fizycznych, w której zwrócono uwagę m. in. na konieczność respektowania zasady proporcjonalności (dane muszą być adekwatne i istotne dla celów przetwarzania) przy posługiwaniu się wideonadzorem. Zasada ta oznacza przede wszystkim, że urządzenia wideonadзору mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje prawnie określony cel uzasadniający ich użycie, a dotychczas stosowane środki niewymagające pozyskiwania obrazu okażą się ewidentnie niewystarczające dla jego realizacji. Ta sama zasada dotyczy również wyboru odpowiedniej

---

<sup>93</sup> Np: DOLiS-035-2261/10, DOLiS-035-2775/10, DOLiS-035-2873/10, DOLiS-035-2882/10, DOLiS-035-2933/10, DOLiS-035-3134/10, DOLiS-035-3173/10.

<sup>94</sup> DOLiS-035-137/2010/ 3163

technologii, kryteriów wykorzystywania urządzeń w konkretnych sytuacjach oraz ustaleń dotyczących przetwarzania danych, zasad dostępu i okresu przechowywania. Generalny Inspektor wskazał ponadto, że osoby korzystające z usług monitorowanego obiektu muszą mieć świadomość faktu prowadzenia na jego terenie czynności wideonadzoru. Tablice informacyjne o wideonadzorze powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Muszą także wskazywać cele działań nadzoru jak również administratora przetwarzania, natomiast wymiary tablic muszą być proporcjonalne do miejsca, gdzie są umieszczone. W toku przedstawionych wyjaśnień władze Miejskiego Ośrodka Sportu i Rekreacji zobowiązały się do przestrzegania podstawowych praw i wolności osób korzystających z usług obiektu.

W podobnych sprawach dotyczących stosowania wideomonitoringu, Generalny Inspektor niejednokrotnie wskazywał, że stosowanie tej techniki nadzoru prowadzi do przetwarzania danych osobowych. A jeśli dochodzi do ich gromadzenia w zbiorze to zastosowanie w tym wypadku mają przepisy dotyczące ochrony danych osobowych.

### 6.1.3. Inne

Na wstępie tej części podsumowującej pracę GODO w zakresie udzielania odpowiedzi na pytania prawne, należy wskazać na nasuwający się po analizie poszczególnych spraw wniosek, iż wzrasta społeczna potrzeba ochrony prywatności, zwłaszcza wobec środków masowego przekazu. Za przykład może posłużyć sprawa dotycząca realizacji programu „Uwaga Pirat” emitowanego przez stację TVN TURBO<sup>95</sup>. Organ ds. ochrony danych skierował wystąpienie do **Komendanta Głównego Policji**, w którym przedstawił informacje o zaniepokojeniu widzów w związku z przetwarzaniem danych osobowych osób biorących udział w nagraniu ww. programu. Nie ulega wątpliwości, że program ten miał charakter prewencyjny, a jego celem było zminimalizowanie liczby przestępstw oraz wykroczeń drogowych. GODO podkreślił jednak rangę konstytucyjnego prawa osoby do ochrony życia prywatnego, wskazując przy tym odpowiednie przepisy Konstytucji Rzeczypospolitej Polskiej oraz innych ustaw. Na przykład art. 12 ust. 1 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. z 1984 r. Nr 5, poz. 24 z późn. zm.), zgodnie z którym dziennikarz jest obowiązany zachować szczególną staranność i rzetelność przy zbieraniu i wykorzystaniu materiałów prasowych, zwłaszcza sprawdzić zgodność z prawdą uzyskanych wiadomości lub podać ich źródło oraz chronić dobra osobiste, a ponadto interesy działających w dobrej wierze informatorów i innych osób, które okazują mu zaufanie. Natomiast regulacje zawarte w art. 23 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 1964 r. Nr 16 poz. 93 z późn. zm.) wyraźnie stanowią, że dobra osobiste człowieka, w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek,

---

<sup>95</sup> DOLiS-035-1428/24024/10

tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Dlatego sposób realizacji programu „Uwaga Pirat” przez podległych Komendantowi Głównemu Policji funkcjonariuszy powinien być tak zorganizowany, aby osobom biorącym udział w przedmiotowym programie zagwarantowane zostało poszanowanie ich prywatności, a dotyczące ich dane osobowe były przetwarzane zgodnie z prawem. W odpowiedzi na wystąpienie Generalnego Inspektora, Komendant Główny Policji obiecał zwrócić uwagę na sposób realizacji przedmiotowego programu, uczulając funkcjonariuszy biorących udział w nagraniach oraz dziennikarzy, na prawa uczestniczących w nich osób.

W wystąpieniu z dnia 25 maja 2010 r. do dyrektora **Miejskiej Izby Wytrzeźwień** w Szczecinie, GİODO wyraził swoje zaniepokojenie praktyką tego podmiotu, polegającą na ustanawianiu zastawu na komórkowym aparacie telefonicznym (razem z kartą pamięci), w sytuacji, gdy osoba zatrzymana w izbie wytrzeźwień nie posiada środków finansowych na opłacenie swojego pobytu. Podobnie jak w poprzednim wypadku i tutaj powołano się na regulacje zamieszczone w polskiej ustawie zasadniczej podkreślając gwarantowane jej przepisami prawo do prywatności. Dodatkowo wskazano, że stosownie do 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. Oceniono, że stosowana przez Miejską Izbę Wytrzeźwień w Szczecinie praktyka może prowadzić do pozyskiwania danych osobowych, a także naruszenia tajemnicy komunikowania się, co stanowi pogwałcenie art. 49 Konstytucji. Ograniczenie w tej sferze może nastąpić jedynie w przypadkach określonych w ustawie. Zaznaczono, że uprawnienie to należy rozumieć szeroko, a więc nie tylko jako prawo do tajemnicy treści korespondencji, ale również prawo do zachowania w tajemnicy przed innymi podmiotami faktu, że do komunikacji pomiędzy określonymi osobami w ogóle doszło. Wskazano również, że podmiot ten poprzez zatrzymywanie telefonu w zastaw może dochodzić do pozyskiwania danych osobowych, do których przetwarzania nie jest mocą przepisów szczególnych uprawniony. Jednocześnie, w ten sposób ogranicza się dysponentowi danych osobowych dostęp do nich, co uniemożliwia mu zapewnienie ich prawidłowej ochrony i odpowiedniego zabezpieczenia. W ramach składanych wyjaśnień dyrektor placówki wskazał, że podlegająca mu Izba Wytrzeźwień działa w oparciu o przepisy w ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2002 r. Nr 128, poz. 1401 z późn. zm.) oraz wydanych na jej podstawie aktów wykonawczych, w szczególności w oparciu o przepisy rozporządzenia Ministra Zdrowia z dnia 4 lutego 2004 r. w sprawie trybu doprowadzania, przyjmowania i zwalniania osób w stanie nietrzeźwości oraz organizacji izb wytrzeźwień i placówek utworzonych lub wskazanych przez jednostkę samorządu terytorialnego (Dz. U. Nr 20, poz. 192). Wskazał jednocześnie, że podlegli



mu pracownicy przestrzegają regulacji zawartych w powyższych aktach prawnych, zapewniając tym samym bezpieczeństwo w procesie pozyskiwania i gromadzenia danych osobowych znajdujących się w telefonach komórkowych i kartach pamięci.

W związku wykonywanym zadaniem w przedmiocie doskonalenia regulacji prawnych związanych z przetwarzaniem danych osobowych, GODO skierował do **Ministra Infrastruktury** wystąpienie dotyczące zmiany w toku prac legislacyjnych, załącznika do rozporządzenia Ministra Transportu z dnia 25 września 2007 r. w sprawie warunków i trybu rejestracji odbiorników radiofonicznych i telewizyjnych (Dz. U. 2007 r. Nr 187, poz. 1342), poprzez usunięcie klauzuli zgody na przetwarzanie danych osobowych<sup>96</sup>. Podczas analizy przedmiotowego załącznika zauważył bowiem, że w celu rejestracji odbiorników radiowych należy wypełnić odpowiedniej treści formularz o nazwie „Wniosek o rejestrację odbiorników radiofonicznych/telewizyjnych”, który oprócz jednoznacznie określonego przez ustawodawcę zakresu danych osobowych, zawierał klauzulę zgody na przetwarzanie danych osobowych. Generalny Inspektor stwierdził, że jeśli podstawę przetwarzania danych osobowych stanowią przepisy prawa – a tak jest w przypadku rejestracji odbiorników radiofonicznych i telewizyjnych przy pomocy formularza obowiązującego mocą przepisów przedmiotowego rozporządzenia – to pozyskiwanie od osób, których dane dotyczą, zgody na przetwarzanie tych danych, jako dodatkowej przesłanki legalizującej przetwarzanie danych osobowych, jest zbędne i wprowadzające w błąd co do możliwości i ewentualnie skutków jej niewyrażenia. W konsekwencji uznano, iż zasadne jest usunięcie ww. klauzuli zgody z treści przedmiotowego formularza o nazwie „Formularz zgłoszenia zmiany danych”, będącego załącznikiem do rozporządzenia Ministra Transportu w sprawie warunków i trybu rejestracji odbiorników radiofonicznych i telewizyjnych. W odpowiedzi Minister Infrastruktury zgodził się z przedstawioną wyżej argumentacją, obiecując jednocześnie, że przy najbliższej nowelizacji rozporządzenie zostanie zmienione zgodnie ze stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych.

W niniejszym sprawozdaniu należy również przedstawić problematykę przetwarzania danych osobowych w zakładach opieki zdrowotnej bądź w instytucjach związanych z działalnością na rzecz zdrowia. Działalność takich jednostek zasługuje na szczególną uwagę ze strony Generalnego Inspektora, ponieważ dotyczy przetwarzania danych osobowych szczególnie chronionych (wrażliwych).

Mając na uwadze powyższe warto przytoczyć treść wystąpienia Generalnego Inspektora z dnia 21 kwietnia 2010 r. kierowanego do niepublicznego zakładu opieki zdrowotnej **Medicus**<sup>97</sup>. Organ ds. ochrony danych osobowych pozyskał informacje, że aby móc zarejestrować się w przychodni, pacjenci placówki obowiązani byli w obecności innych osób oczekujących w kolejce, podawać dane osobowe,

---

<sup>96</sup> DOLiS-035-287/10/5918

<sup>97</sup> DOLiS-035-948/10/16743

jak imię i nazwisko, adres zamieszkania, numer PESEL i numer telefonu. W ocenie Generalnego Inspektora tego typu działania skutkowały ryzykiem pozyskania przez osoby nieupoważnione danych osobowych rejestrujących się pacjentów. Przetwarzanie danych osobowych odbywać się powinno w zgodzie z art. 26 i 36 ustawy o ochronie danych osobowych. W szczególności ich pozyskiwanie musi odbywać się w sposób zapewniający im ochronę przed udostępnieniem osobom nieuprawnionym. Gromadzenie danych od osób rejestrujących się w wyżej wskazany sposób, stwarza wysokie ryzyko naruszenia prawa do prywatności tych osób. Istniało bowiem duże prawdopodobieństwo, iż osoby znajdujące się w pobliżu (nieupoważnione) mogły pozyskać dane osobowe rejestrującego się pacjenta. W wystąpieniu zwrócono uwagę na potrzebę zabezpieczenia przetwarzanych danych osobowych, które powinny uniemożliwić m.in. pozyskanie danych przez osoby nieupoważnione. Obowiązek zabezpieczenia przetwarzanych danych powinien być realizowany przy zastosowaniu odpowiednich do zagrożeń, a zatem skutecznych środków technicznych i organizacyjnych. W wyniku podjętej interwencji, Generalny Inspektor otrzymał od władz niepaństwowego zakładu opieki zdrowotnej zapewnienia, iż sposób rejestrowania pacjentów został zmieniony, a proces przetwarzania danych osobowych przebiega obecnie w zgodzie z wymogami wskazanymi we właściwych aktach prawnych.

Kolejne stanowisko dotyczące przetwarzania danych osobowych w związku z działalnością jednostek świadczących usługi zdrowotne, przedstawiono w wystąpieniu odnoszącym się do przetwarzania danych osobowych osób poszkodowanych w wypadkach drogowych przez **Interdyscyplinarne Centrum Genetyki Zachowań przy Uniwersytecie Warszawskim**, w ramach programu „Psychologiczne przyczyny i następstwa wypadków drogowych” TRAKT<sup>98</sup>. Do Generalnego Inspektora Ochrony Danych Osobowych dotarły informacje wskazujące na przesyłanie przez ww. Centrum, pism informacyjnych zawierających ofertę udzielenia pomocy psychologicznej dla osób poszkodowanych w wypadkach drogowych. W wystąpieniu GODO podkreślił, że wszelkie przetwarzanie danych osobowych powinno odbywać się z poszanowaniem zasad przetwarzania danych osobowych wyznaczonych w art. 26 ust. 1 i 2 ustawy, w szczególności z zasadą celowości. Wykorzystywanie danych adresowych uzyskanych przez administratora danych w celu innym niż ten, dla którego dane zostały pierwotnie zebrane, jest prawnie dopuszczalne, jeżeli nie narusza to praw i wolności osoby, której dane dotyczą, oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, z zachowaniem przepisów art. 23 i art. 25 ustawy o ochronie danych osobowych<sup>99</sup>. Zastrzeżenia Generalnego Inspektora budziły nieścisłości oraz nieprawidłowości w treści

---

<sup>98</sup> DOLiS-035-285/10/5903

<sup>99</sup> Zgodnie z art. 25 ust. 1 ustawy w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu i zakresie danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, 3) źródle danych, 4) prawie dostępu do treści swoich danych oraz ich poprawiania, 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

pisma informacyjnego wysyłanego przez Centrum do osób poszkodowanych w wypadkach, które skutkowały ograniczoną kontrolą procesu przetwarzania danych osobowych przez osoby, których dane dotyczyły. Dla przykładu, w piśmie nieprawidłowo określono źródło pozyskanych przez Centrum danych osobowych, wskazując, że zostały one otrzymane z „Centralnego Rejestru Kolizji i Wypadków Drogowych za rok 2008 Komendy Głównej Policji za zgodą MSWiA i GIODO”. Tymczasem zgodę na przetwarzanie danych osobowych może wyrazić jedynie osoba, której dane dotyczą, nie zaś wymieniony organ administracji publicznej. Zwrócono więc uwagę, iż w przedmiotowym piśmie informacyjnym należałoby wskazać, że dane adresowe zostały ustalone przez Departament Ewidencji Państwowych MSWiA, na podstawie uzyskanych przez Centrum informacji o numerach PESEL ofiar wypadków i kolizji drogowych z terenu województwa mazowieckiego za okres 2008 – 2009. Informacje te pochodziły z Systemu Ewidencji Wypadków i Kolizji – SIWEK, prowadzonego przez Komendę Główną Policji, a następnie przekazane administratorowi danych przez ww. departament MSWiA. Stwierdzono również, iż pismo przewodnie nie zawierało wskazania administratora ww. danych, na którym spoczywają określone w ustawie o ochronie danych osobowych obowiązki związane z procesem przetwarzania danych. Brak informacji o pełnej nazwie oraz adresie siedziby administratora, praktycznie uniemożliwia osobie, której dane dotyczą, realizację uprawnień, o których mowa w art. 32 i 33 ustawy, tj. do kontroli przetwarzania dotyczących jej danych osobowych. Dodatkowo Generalny Inspektor powołał się na art. 26 ust. 1 pkt 4 ustawy, zgodnie z którym administrator danych ma obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (zasada ograniczenia czasowego przetwarzania danych). Zaznaczono, że dane pozyskanie w wyraźnie wskazanym celu, nie bezpośrednio od osoby, której dotyczą, nie mogą być następnie przetwarzane w jakimkolwiek innym celu, np. dla ochrony interesów finansowych administratora danych przez ograniczanie kosztów wysyłanej przez niego korespondencji. Podsumowując, organ ds. ochrony danych osobowych przyjął, że przetwarzanie danych osobowych osób poszkodowanych w wypadkach drogowych, które zechcą wziąć udział w programie TRAKT w związku z jego realizacją, może nastąpić tylko po tym, jak osoby te zwrócą się do administratora danych o pomoc objętą programem oraz wyrażą zgodę na przetwarzanie ich danych osobowych przez Centrum we wskazanym powyżej celu.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych zajmował się zagadnieniem zakresu danych osobowych żądanych przez władze gminy i dyrektorów **przedszkoli** od rodziców w procesie rekrutacji dzieci do przedszkoli. Zainteresowanie organu do spraw ochrony danych osobowych tą problematyką spowodowane zostało napływającą do Biura Generalnego Inspektora Ochrony Danych Osobowych korespondencją głównie ze strony rodziców dzieci uczestniczących w procesie rekrutacji do przedszkoli prowadzonych w wielu gminach na terenie całego

kraju, którzy wyrazili wątpliwość co do zasadności przedstawiania w związku z rekrutacją ich dzieci do przedszkoli różnego rodzaju dokumentów, a zwłaszcza zaświadczeń ZUS RMUA (na potwierdzenie zatrudnienia), zaświadczeń o niepełnosprawności, orzeczeń sądowych oraz rocznych rozliczeń podatkowych PIT (potwierdzających miejsce zamieszkania i opłacania podatku dochodowego). Zaniepokojenie tym zjawiskiem wyraził również Rzecznik Praw Dziecka, który zwrócił się do Generalnego Inspektora z zapytaniem, czy praktyka żądania przez władze gminy i dyrektorów przedszkoli przedłożenia przez rodziców ww. dokumentów na potrzeby przyjęcia dziecka do przedszkola jest zgodna z obowiązującym prawem. Sprawą zainteresował się także Rzecznik Praw Obywatelskich. Dokonana przez Generalnego Inspektora Ochrony Danych Osobowych analiza powszechnie obowiązujących przepisów prawa, tj. ustawy z dnia 7 września 1991 r. o systemie oświaty (tekst jednolity: Dz. U. 2004 r. Nr 256, poz. 2572 z późn. zm.) oraz wydanych na jej podstawie aktów wykonawczych, doprowadziła do stwierdzenia, iż przepisy te nie dają ww. organom uprawnienia do pozyskiwania tego rodzaju dokumentów. Jakkolwiek bowiem ustawa o systemie oświaty odnosi się do zasad rekrutacji dzieci do przedszkoli upoważniając w jej art. 22 ministra właściwego do spraw oświaty i wychowania do określenia w drodze rozporządzenia warunków i trybu przyjmowania uczniów do szkół i przedszkoli, to nie reguluje zakresu danych osobowych (w tym dokumentów dane te zawierających) rodziców niezbędnego dla przeprowadzania rekrutacji. Tym bardziej podstawą nie mogą być w tym przypadku akty prawa miejscowego (np. uchwały rady gminy), których zakres regulacji nie może zostać rozszerzony poza materię stanowiącą regulację ustawową, co w badanym przypadku ma miejsce. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych taka praktyka jest niedopuszczalna w świetle powszechnie obowiązujących przepisów prawa, stanowi nadmierną ingerencję w prywatność rodziców, a nader wszystko prowadzi do nałożenia na nich dodatkowych obowiązków bez podstaw prawnych. Powyższe ustalenia dały przyczynek do wystąpienia przez Generalnego Inspektora Ochrony Danych Osobowych z pismem do **Ministra Edukacji Narodowej** w sprawie konieczności uregulowania ustawowego zasad przetwarzania danych osobowych przy naborze do przedszkoli. Stanowisko w tym zakresie Generalny Inspektor Ochrony Danych Osobowych potwierdził w toku opiniowania w ramach uzgodnień międzyresortowych zmiany ustawy o systemie oświaty wskazując konieczność zmiany przepisów w kierunku precyzyjnego uregulowania sposobu pozyskiwania i zakresu danych osobowych przetwarzanych przy rekrutacji do publicznych szkół i przedszkoli, dla wykluczenia rozszerzania przez rady gmin, prezydentów, burmistrzów i wójtów przy procesie rekrutacji do publicznych szkół, przedszkoli, zakresu pozyskiwanych danych osobowych rodziców. Niezależnie od tego Generalny Inspektor zasugerował **Ministrowi Spraw Wewnętrznych i Administracji**, by w przypadku kontynuowania praktyki ustalania kryteriów przyjęć oraz zasad przetwarzania danych osobowych w uchwałach rad gminy

województwie korzystali ze swych uprawnień nadzorczych i zapobiegali wejściu w życie odpowiednich przepisów prawa miejscowego.

Podczas analizy pytań prawnych, które w 2010 r. wpłynęły do GIODO, należy mieć również na względzie to, że w roku tym odbyły się wybory samorządowe i w związku z prowadzonymi kampaniami wyborczymi napłynęło wiele sygnałów świadczących o nielegalnym pozyskiwaniu danych osobowych wyborców celem promowania programów wyborczych osób kandydujących na stanowiska samorządowe<sup>100</sup>. Przykładem nieprawidłowości w przetwarzaniu danych osobowych potencjalnych wyborców było pytanie z dnia 25 listopada 2010 r., związane z przesyłaniem na prywatne adresy e-mail, treści promujących kandydata na prezydenta miasta Szczecin. W odpowiedzi Generalny Inspektor wskazał na uprawnienia kontrolne wynikające z rozdziału 4 ustawy o ochronie danych osobowych, przysługujących każdej osobie, której dane osobowe przetwarzane są w zbiorach danych i zaznaczył, że bezprawne przetwarzanie danych osobowych może skutkować poniesieniem odpowiedzialności karnej przewidzianej.

## **6.2. Działalność informacyjna**

W celu upowszechniania wiedzy z zakresu ochrony danych osobowych, Generalny Inspektor, wzorem lat ubiegłych, korzystał z pośrednictwa mediów (prasa, radio, telewizja, agencje informacyjne i portale 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](http://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 z pracownikami Biura GIODO. Duży krąg odbiorców informacji z zakresu ochrony danych osobowych zapewniły również inicjowane przez GIODO publikacje książkowe, szkolenia oraz konferencje naukowe.

Przygotowywane i upowszechniane przez GIODO materiały edukacyjne i informacyjne obejmowały m.in. interpretacje przepisów o ochronie danych osobowych, wystąpienia Generalnego Inspektora do podmiotów z zasygnalizowanymi nieprawidłowościami dotyczącymi 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.

---

<sup>100</sup> DOLiS-035-2872/10

## 6.2.1 Współpraca ze środkami masowego przekazu

### 1. Stałe kontakty z mediami

W celu upowszechniania wiedzy o ochronie danych osobowych, GODO – wzorem lat ubiegłych – w roku 2010 kontynuował stałą współpracę z mediami polegającą na przekazywaniu do publikacji opracowanych przez GODO materiałów informacyjno-edukacyjnych. Współpraca prowadzona była zarówno z prasą codzienną o zasięgu ogólnopolskim, przede wszystkim zaś z „Rzeczpospolitą” i „Dziennikiem Gazeta Prawna”, jak i ogólnopolskimi pismami branżowymi, m.in. „Serwisem Prawno-Pracowniczym”, „Przeglądem Komunalnym”, „Computerworldem”, „Kadrami w Urzędzie” oraz portalami, takimi jak np. Dziennik Internautów. Dodatkową formą upowszechniania wiedzy z zakresu ochrony danych osobowych była publikacja wyjaśnień GODO w czasopismach kobiecych, takich jak „Twoje Imperium”, „Tina” czy „Przyjaciółka”. W 2010 r. GODO zainicjował ponadto stałe kontakty m.in. z tygodnikiem „Współnota” (pismem kierowanym do jednostek samorządu terytorialnego) oraz Radiem TOK FM, co zaowocowało regularnym upowszechnianiem w tych mediach problematyki z zakresu ochrony danych osobowych (w tym godzinne audycje w cyklu „W Sieci Sieci” poświęcone w całości problematyce ochrony prywatności). Dodatkowo w 2010 r. GODO zrealizował **dwa cykle audycji radiowych**. Pierwszy był przygotowany dla rozgłośni Polskiego Radia w Kielcach i obejmował 8 audycji. Drugi zrealizowało Radio Pomorza i Kujaw – liczył łącznie 15 audycji. Dzięki stałej współpracy z wymienionymi wyżej mediami, w 2010 r. zostało opublikowanych lub wyemitowanych około **140** materiałów poświęconych tematyce ochrony danych osobowych. Większość z nich jest dostępna na stronie 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 2010 r. GODO udzielił – pisemnie lub telefonicznie – około **300** takich odpowiedzi. Wśród problemów, z którymi najczęściej zgłaszali się przedstawiciele mediów, były m.in.:

- funkcjonowanie portali społecznościowych,
- zasady przetwarzania danych osobowych dłużników,
- wykorzystywanie danych osobowych na potrzeby marketingu,
- ochrona danych osobowych w procesie rekrutacji i zatrudnienia,
- wycieki danych osobowych zarówno z instytucji publicznych, jak i prywatnych,
- zasady przetwarzania danych osobowych przez placówki medyczne,
- zabezpieczanie danych osobowych,
- zasady przetwarzania danych osobowych przez kościoły i związki wyznaniowe,
- pozyskiwanie danych osobowych zawartych w internetowym systemie ksiąg wieczystych,

- dostarczanie korespondencji przez pracowników spółdzielni i wspólnot mieszkaniowych,
- udostępnianie danych osobowych będących w dyspozycji jednostek samorządu terytorialnego,
- upublicznianie przez jednostki samorządu terytorialnego danych osobowych zarówno w BIP, jak i w uchwałach czy decyzjach,
- dopuszczalność świadczenia usługi *Google Street View*,
- możliwość stosowania monitoringu wizyjnego przez podmioty inne niż ustawowo upoważnione.

### 3. Wywiady i wystąpienia

Jedną z form działalności edukacyjno-informacyjnej były wywiady radiowe i telewizyjne z GODO, których w 2010 r. udzielił blisko **130**. Ich tematyka dotyczyła zarówno ogólnych zasad ochrony danych osobowych określonych w ustawie o ochronie danych osobowych, jak i rozwiązań ustanowionych przepisami branżowymi. Oprócz opisanych wcześniej tematów zainteresowanie mediów budziło także przetwarzanie danych osobowych na potrzeby zatrudnienia, w sektorze ubezpieczeniowym, bankowym, marketingowym, mieszkalnictwa, oświaty i służby zdrowia. Wiele wywiadów i wypowiedzi odnosiło się do kwestii ochrony danych osobowych w kontekście rozwoju nowoczesnych technologii. Dziennikarze bardzo często pytali, jak bezpiecznie korzystać z portali internetowych, zwłaszcza społecznościowych, m.in. takich jak Facebook czy Nasza Klasa. Wśród innych tematów rozmów związanych z wykorzystaniem nowoczesnych technologii wymienić można: wyłudzenie bądź wykradanie danych osobowych, monitorowanie pracowników, czy dopuszczalność świadczenia usługi polegającej na umieszczaniu w Internecie zdjęć ulic. GODO niejednokrotnie udzielał wywiadów poświęconych zatrzymywaniu i przetwarzaniu przez operatorów usług telekomunikacyjnych danych pozyskanych w związku ze świadczeniem usług łączności telefonicznej lub internetowej, a także przetwarzaniu danych osobowych przez wyszukiwarki, w tym nowo uruchomioną 123people.pl.

Przetwarzanie danych osobowych na potrzeby przeprowadzenia powszechnego spisu rolnego w 2010 r., zwłaszcza w kontekście właściwej ich ochrony, to kolejny temat częstych wystąpień medialnych GODO w 2010 r. Pod koniec 2010 r. duże zainteresowanie mediów budziły zmiany prawa o ochronie danych osobowych, takie jak nowelizacja ustawy o ochronie danych osobowych czy zmiana Dyrektywy 95/46/WE *o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym przepływie tych danych*. Częstym tematem rozmów była też kwestia przetwarzania danych osobowych przez służby specjalne, co było spowodowane m.in. omawianymi przez parlament propozycjami zwiększenia uprawnień kontrolnych GODO w stosunku do tych służb.

#### e) **Konferencje i spotkania prasowe**

W związku z potrzebą nagłośnienia niektórych wydarzeń lub upublicznienia stanowiska GIODO w istotnych sprawach, GIODO w 2010 r. zorganizował 1 spotkanie oraz 3 konferencje prasowe. Poświęcone one były:

- obchodom IV Dnia Ochrony Danych Osobowych i podpisaniu pomiędzy GIODO a Związkiem Pracodawców Branży Internetowej IAB Polska porozumienia na rzecz upowszechniania prawa do ochrony danych osobowych i prawa do prywatności oraz tworzenia kodeksu dobrych praktyk (28 stycznia 2010 r.),
- realizacji przez Biuro GIODO programu pilotażowego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”, a także dwóch projektów finansowanych ze środków unijnych (11 marca 2010 r.),
- pozyskiwaniu w czasie rekrutacji do przedszkoli zbyt szerokiego zakresu danych osobowych dzieci i ich rodzin (25 sierpnia 2010 r.),
- wykorzystywaniu danych osobowych na potrzeby samorządowej kampanii wyborczej (13 grudnia 2010 r.).

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

#### f) **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 2010 r. dwa zagadnienia zostały rozpropagowane w ten właśnie sposób.

- W związku z przypadającym 28 stycznia Dniem Ochrony Danych Osobowych GIODO podjął działania mające na celu nagłośnienie europejskich i polskich obchodów tego Dnia, zwłaszcza ich tematu przewodniego – tj. prawa do prywatności w Internecie. 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 Pracodawców Branży Internetowej IAB Polska mające na celu upowszechnianie prawa do ochrony danych osobowych i prawa do prywatności oraz tworzenie kodeksu dobrych praktyk. Obchody Dnia Ochrony Danych Osobowych były też okazją do organizacji przez GIODO oraz redakcję „Dziennika Gazety Prawnej” debaty „Masz prawo do prywatności w Internecie”. Odbędzie się ona 12 stycznia 2010 r. w siedzibie redakcji. Akcja informacyjna dotycząca Dnia Ochrony Danych Osobowych zaowocowała publikacją licznych artykułów prasowych i internetowych związanych z jego tematem



przewodnim. Dzięki współpracy GIODO z Wydawnictwem Wiedza i Praktyka z okazji Dnia Ochrony Danych Osobowych wydany został specjalny plakat edukacyjny zawierający wskazówki GIODO dotyczące bezpiecznego korzystania z Internetu, który był kolportowany w styczniowym numerze miesięcznika „Bezpieczniej w Przedszkolu”, a także podczas Dnia Otwartego w Biurze GIODO.

- W celu edukowania dzieci i młodzieży w 2010 r. GIODO nawiązało współpracę z redakcją programu „Zagadkowa niedziela” emitowanego w Programie 3 Polskiego Radia, dzięki czemu wziął udział w trzech wydaniach tej audycji (25 kwietnia oraz 9 i 23 maja 2010 r.), podczas których wyjaśniał, co to są dane osobowe i jak są chronione, co oznaczają takie pojęcia, jak tożsamość czy prywatność. Tłumaczył, jak bezpiecznie korzystać z Internetu oraz jak dzieci i młodzież powinny dbać o dane osobowe, zarówno swoje, jak i swoich najbliższych. Dodatkowym elementem tego cyklu audycji był konkurs wiedzy o ochronie danych osobowych, w którym nagrodą był wyjazd do Brukseli dla trzech młodych słuchaczy połączony ze zwiedzaniem Parlamentu Europejskiego.

### **6.2.2 Publikacje**

W 2008 roku Generalny Inspektor Ochrony Danych Osobowych rozpoczął publikację serii broszur informacyjnych na temat ochrony danych osobowych. Dotychczas wydanych zostało 6 publikacji o następujących tytułach:

- „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.”

W 2010 r. GIODO kontynuowało opracowywanie broszur z serii „ABC ochrony danych osobowych”. W efekcie zakończone zostały prace redakcyjne nad broszurą „ABC przetwarzania danych osobowych w działalności marketingowej”.

### 6.2.3 Szkolenia

#### a) Szkolenia podmiotów zewnętrznych

W ramach szeroko prowadzonej 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.: dyrektorów warszawskich placówek szkolnych, pracowników Kuratorium Oświaty w Warszawie, Biura Edukacji m. st. Warszawy i Narodowego Centrum Kultury. W szkoleniu zorganizowanym przez GIODO w Kielcach udział wzięli liderzy reprezentujący Samorządowy Ośrodek Doradztwa Metodycznego i Doskonalenia Nauczycieli w Kielcach zaś w szkoleniu w Gliwicach – liderzy Gliwickiego Ośrodka Metodycznego, które to ośrodki uczestniczyły w programie pilotażowym *„Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”*. Ponadto wśród podmiotów szkolonych w 2010 r. znalazł się Narodowy Bank Polski, Urząd Komunikacji Elektronicznej, Urząd ds. Cudzoziemców, Sąd Okręgowy w Przemyśle, Prokuratura Okręgowa w Warszawie i Okręgowa Izba Radców Prawnych w Lublinie, a także Urząd Miasta Zgierz, Wojewódzki Urząd Pracy w Warszawie, Izba Skarbowa w Gdańsku oraz Izba Celna w Gdyni i Izba Celna w Łodzi. Na liście przeszkolonych przez Generalnego Inspektora Ochrony Danych Osobowych pracowników ministerstw znalazły się Ministerstwa: Spraw Zagranicznych, Infrastruktury, Finansów (Departament Izby Celnej i Departament Kontroli Skarbowej) oraz Spraw Wewnętrznych i Administracji (w tym Centrum Personalizacji Dokumentów MSWiA). W szkoleniach z zakresu ochrony danych osobowych brali też udział pracownicy Mazowieckiej Jednostki Wdrażania Programów Unijnych i funkcjonariusze Służby Więziennej oraz – podobnie jak w latach poprzednich - kadra kierownicza i urzędnicza Kancelarii Sejmu RP i Kancelarii Prezesa Rady Ministrów.

Szkolenia odbywały się na zasadzie cyklicznie zorganizowanych spotkań, albo w ramach seminariów czy konferencji. Przykładem może być XIV Ogólnopolska Konferencja Uniwersyteckich Poradni Prawnych, której uczestnicy wzięli udział w szkoleniu na temat prawa do prywatności i ochrony danych osobowych w związku z działalnością poradni studenckich.

W sumie w 2010 r. przeprowadzonych zostało 55 szkoleń z zakresu ochrony danych osobowych dla podmiotów zewnętrznych. Ich wykaz znajduje się w załączniku nr 6.

#### b) Szkolenia wewnętrzne pracowników Biura GIODO

W zależności od dynamiki przyjmowania nowych pracowników do pracy w Biurze Generalnego Inspektora Ochrony Danych Osobowych, organizowane były szkolenia dla wszystkich nowo zatrudnionych. Tematyka szkoleń obejmowała zagadnienia takie 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.

#### **c) Udział pracowników Biura GIODO w szkoleniach organizowanych przez jednostki zewnętrzne**

Pracownicy Biura GIODO korzystali ze szkoleń informatycznych, które mają na celu 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 2010 pracownicy Biura GIODO uczestniczyli w 4 takich szkoleniach.

Ponadto w związku z przygotowaniem polskiej administracji do Prezydencji w Radzie Unii Europejskiej, przedstawiciele Biura Generalnego Inspektora Ochrony Danych Osobowych brali udział w szkoleniach z zakresu wiedzy ogólnej na temat systemu prawnego, porządku instytucjonalnego oraz procesu decyzyjnego UE.

#### **6.2.4 Konkursy**

Generalny Inspektor Ochrony Danych Osobowych ogłosił **III edycję Konkursu rysunkowego pt. „Ochrona danych osobowych we współczesnym świecie”**, który tym razem adresowany był do wychowanków placówek opiekuńczo - wychowawczych w wieku 12 - 16 lat. Prace uczestników konkursu zostały zaprezentowane na wystawie zorganizowanej w dniu 28 stycznia 2010 roku z okazji IV Europejskiego Dnia Ochrony Danych Osobowych. W konkursie udział 25 osób, które nadesłały 27 prac.

#### **6.2.5 Projekty i programy**

W roku sprawozdawczym 2010, Biuro GIODO kontynuowało swój udział w dwóch rodzajach projektów. Pierwszy z nich stanowiły projekty finansowane ze środków Unii Europejskiej w ramach Programu Leonardo da Vinci (LdV) będącego częścią Programu „Uczenia się przez całe życie” (*Lifelong Learning Programme*), a mianowicie projekt wymiany i projekt partnerski. Drugim rodzajem był krajowy projekt edukacyjny, który po okresie pilotażu przekształcił się w ogólnopolski program edukacyjny, realizowany pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka.

## I. Projekty unijne

### a) Projekt wymiany

W latach 2009-2010 przedstawiciele Biura GIODO wzięli udział w międzynarodowej wymianie pracowników europejskich organów ochrony danych osobowych w ramach projektu „*Wzmocnienie umiejętności pracowników Biura GIODO*”. Zostali oni oddelegowani na 1-2 tygodniowe pobyty w urzędach organów ochrony danych osobowych z krajów biorących udział w projekcie, takich jak Słowenia, Cypr, Węgry oraz Niemcy. Dzięki wymianie pracowników zorganizowanej w ramach Programu, uczestnicy wyjazdów mieli możliwość pogłębienia wiedzy, pozyskania nowych informacji związanych ze stosowaniem prawa z zakresu ochrony danych osobowych przez inne organy zajmujące się tą problematyką, wymiany doświadczeń dotyczących funkcjonowania organów ochrony danych osobowych w kraju partnera, zapoznania się z systemem wdrażania prawodawstwa unijnego w wybranych obszarach objętych projektem wymiany, a także podniesienia umiejętności językowych. Realizacja tego projektu trwała od 1 sierpnia 2009 r. do 30 czerwca 2010 r. W podobnym projekcie Biuro GIODO uczestniczyło w latach 2007-2008.

### b) Projekt partnerski

W 2010 r. w ramach Programu Leonardo da Vinci kontynuowany był projekt partnerski pt.: **„Zwiększanie świadomości w zakresie ochrony danych wśród przedsiębiorców funkcjonujących na rynkach Unii Europejskiej”** („Raising awareness of the data protection issues among the entrepreneurs operating in the UE”). Celem projektu jest dostarczenie materiałów edukacyjnych i szkoleniowych dla podmiotów podejmujących działalność w jednym z krajów uczestniczących w konsorcjum projektowym. 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 adresowany jest projekt 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 oraz zintensyfikowanie współpracy między organami ochrony danych w różnych krajach członkowskich UE. W ramach projektu powstanie publikacja, w której omówione zostaną zagadnienia ochrony danych w kontekście prowadzenia działalności gospodarczej oraz przeprowadzony zostanie przegląd praktyk stosowanych w poszczególnych krajach partnerskich, w zakresie stosowania przepisów prawa ochrony danych osobowych, mogących mieć bezpośredni wpływ na legalność i zgodność z przepisami wykonywanej działalności gospodarczej. Poruszone też 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 z zakresu ochrony danych osobowych, w sposób umożliwiający efektywną i samodzielną naukę przez adresatów przepisów prawa w tym obszarze w krajach partnerskich.

Pierwsze spotkanie konsorcjum partnerskiego realizującego ten projekt tj. Generalnego Inspektora Ochrony Danych Osobowych z przedstawicielami Urzędu Ochrony Danych z Czech i Węgier, odbyło się w Warszawie, w Biurze GIODO w dniach 5-6 listopada 2009 r. W 2010 r. w siedzibie Czeskiego Urzędu Ochrony Danych Osobowych w Pradze odbyły cztery spotkania tego konsorcjum, podczas których dyskutowano nad kształtem przygotowywanej publikacji „Selected data protection issues. Vademecum for entrepreneurs operating in the EU”.

Projekt kontynuowany będzie w 2011 roku.

W 2010 r. Biuro GIODO rozpoczęło realizację kolejnego projektu partnerskiego w ramach Programu Leonardo da Vinci **„Postrzeganie zagadnień związanych z ochroną danych i prywatnością przez dzieci i młodzież”**. Projekt realizowany będzie w latach 2010-2011 we współpracy z Węgierskim Organem Ochrony Danych oraz Chorwacką Agencją Ochrony Danych Osobowych. Założeniem projektu jest przeprowadzenie badań w Polsce, Chorwacji i na Węgrzech wśród dzieci i młodzieży, na temat oceny ich podejścia do zagadnień związanych z ochroną danych osobowych i prywatności. W rezultacie powstanie raport podsumowujący badania wraz z oceną tego zjawiska w trzech krajach członkowskich Unii Europejskiej.

## **II. Krajowy program edukacyjny**

W celu poszerzenia oferty edukacyjnej szkół o treści związane z ochroną danych osobowych i prawem każdego człowieka do prywatności, powstała inicjatywa edukacyjna zakładająca współdziałanie na zasadzie partnerstwa dwóch samorządowych ośrodków doskonalenia zawodowego nauczycieli (z Kielc i Gliwic) i Generalnego Inspektora Ochrony Danych Osobowych, nad zwiększeniem wiedzy nauczycieli, pedagogów szkolnych i uczniów szkół gimnazjalnych o zagadnienia związane z tą tematyką. Powstał więc projekt programu **„Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli”**, który został objęty honorowym patronatem Rzecznika Praw Dziecka. Pilotaż programu realizowany był w województwach śląskim i świętokrzyskim przy wykorzystaniu „dobrych praktyk” europejskich organów ochrony danych osobowych. W ramach I etapu, w okresie od września 2009 r. do czerwca 2010 r. odbyły się w Kielcach i Gliwicach szkolenia kadry nauczycielskiej. Podstawowym celem szkoleń było podniesienie kompetencji nauczycieli w obszarze kształtowania wśród uczniów wiedzy i umiejętności związanych z ochroną prywatności i danych osobowych, a także poszerzenie warsztatu

metodycznego. Idea programu prezentowana była także na forum międzynarodowym, podczas spotkania Generalnego Inspektora Ochrony Danych Osobowych z dziennikarzami w dniu 11 marca 2010 r. Prezentacja taka była możliwa m.in. dzięki temu, że w marcu 2010 r. GODO był współorganizatorem dwóch międzynarodowych wizyt.

Pierwszą z nich była wizyta przedstawicieli węgierskiego organu ds. ochrony danych osobowych przyjeżdżających do Polski w ramach wymiany między urzędami. Drugą zaś - wizyta studyjna finansowana ze środków UE w ramach Programu Wizyt Studyjnych, będącego częścią wspomnianego Programu „Uczenie się przez całe życie” (Warszawa, 9-12 marca 2010 r.). Było to spotkanie osób uczestniczących w projekcie „Zagadnienia ochrony danych osobowych i prywatności w edukacji” realizowanym przez GODO z funduszy UE. Już sam tytuł projektu wskazywał, 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 oceniana była możliwość wprowadzenia programów edukacyjnych do szkół podstawowych, gimnazjów i liceów oraz przedyskutowano najbardziej efektywne formy prowadzenia edukacji w tym obszarze. Uczestnikami wizyty byli reprezentanci europejskich organów ochrony danych osobowych oraz instytucji zajmujących się edukacją z takich unijnych państw, jak Cypr, Chorwacja, Grecja, Włochy i Hiszpania. Ze strony polskiej w spotkaniu udział wzięli przedstawiciele instytucji i środowisk związanych z edukacją i doradztwem, nauczyciele szkół podstawowych, gimnazjów i liceów, decydenci w zakresie programów edukacyjnych Ministerstwa Edukacji Narodowej, przedstawiciele lokalnych i regionalnych władz związanych z edukacją, a także przedstawiciele środowisk, które monitorują zagrożenia płynące z korzystania Internetu.

Natomiast w II etapie pilotażu programu „Twoje dane – twoja sprawa...” nastąpiło bezpośrednie włączenie do tematyki zajęć szkolnych zagadnień związanych z ochroną danych osobowych. Powstały konspekty zajęć dla nauczycieli i uczniów, raport ewaluacyjny podjętych działań oraz opracowany został w oparciu o wyniki pilotażu **edukacyjny program o zasięgu ogólnopolskim**, pod honorowym patronatem Minister Edukacji Narodowej oraz Rzecznika Praw Dziecka. Jego adresatami są nauczyciele, pedagodzy szkolni i uczniowie szkół gimnazjalnych. W jego ramach nauczyciele będą mogli korzystać z bezpłatnych szkoleń, konsultacji materiałów dydaktycznych oraz wymiany doświadczeń. W ramach programu przygotowane zostały pakiety edukacyjne dla jego uczestników, zawierające m.in. skrypty informacyjne dotyczące zasad ochrony danych osobowych, scenariusze i konspekty lekcji, prezentacje multimedialne, ankiety do ewaluacji zajęć i inne pomoce dydaktyczne. Ostatnim etapem programu był konkurs na konspekt zajęć „Lekcja z wykorzystaniem treści dotyczących ochrony danych osobowych i bezpieczeństwa w sieci”, skierowany do nauczycieli wszystkich typów szkół oraz konkurs „Twoje dane – twoja sprawa” adresowany do uczniów

gimnazjum. Realizacja programu rozpoczęła się w październiku 2010 r. i trwać będzie do sierpnia 2011 r.

#### **6.2.6 Konferencje, seminaria, spotkania**

W roku sprawozdawczym 2010, Generalny Inspektor Ochrony Danych Osobowych organizował konferencje i seminaria, jak również brał aktywny udział w konferencjach zorganizowanych przez inne podmioty. Poniżej przedstawiony został wykaz najważniejszych konferencji, seminariów i spotkań z udziałem Generalnego Inspektora bądź przedstawicieli jego Biura.

##### **1. IV Dzień Ochrony Danych Osobowych – 28 stycznia 2010 r.**

W dniu 28 stycznia 2008 r. Generalny Inspektor Ochrony Danych Osobowych już po raz czwarty organizował Europejski Dzień Ochrony Danych Osobowych ustanowiony przez Komitet Ministrów Rady Europy. W tym dniu świętowana jest rocznica otwarcia do podpisu Konwencji 108 Rady Europy z dnia 28 stycznia 1981 r. w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych - najstarszego aktu prawnego o zasięgu międzynarodowym, kompleksowo regulującego zagadnienia związane z ochroną danych osobowych. Z tej okazji zorganizowany został w Biurze GODO Dzień Otwarty, w ramach którego uczestnicy mieli okazję uzyskać informacje na temat ochrony danych osobowych oraz porady prawne i konsultacje. W ramach obchodów Dnia Ochrony Danych Osobowych zorganizowany został cykl wykładów poświęconych ochronie prywatności i danych osobowych. Tegoroczne hasło Dnia Otwartego brzmiało: „Masz prawo do prywatności w Internecie”. W związku z tym wykłady koncentrowały się przede wszystkim wokół tematów związanych z ochroną prywatności w świecie elektronicznym, a w szczególności ochroną praw dziecka w Internecie. Zorganizowany również został czat GODO z uczniami 7 gliwickich gimnazjów objętych programem pilotażowym „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli”, jako że w tym roku do obchodów tego święta włączył się Urząd Miasta Gliwice, Gliwicki Ośrodek Metodyczny oraz nauczyciele i uczniowie gliwickich szkół gimnazjalnych uczestniczących w programie. W czasie obchodów Dnia odbyło się wręczenie nagród laureatom konkursu rysunkowego pod hasłem „Ochrona danych osobowych we współczesnym świecie”, którego adresatami byli wychowankowie warszawskich placówek opiekuńczo-wychowawczych.

Podczas Dnia Otwartego miało też miejsce uroczyste podpisanie porozumienia pomiędzy **GIODO i Związkiem Pracodawców Branży Internetowej IAB Polska** na rzecz upowszechniania prawa do ochrony danych osobowych i prawa do prywatności poprzez podejmowanie wspólnych działań, w tym stworzenie kodeksu dobrych praktyk.

Wydarzenia, jakie towarzyszą obchodom Dnia Ochrony Danych Osobowych, tradycyjnie od czterech lat odbywają się nie tylko w Polsce, ale i w Brukseli. W 2010 r. Generalny Inspektor Ochrony Danych Osobowych na spotkaniu z przedstawicielami Koła Poselskiego zainicjował debatę na temat przetwarzania danych osobowych w pracach Parlamentu Europejskiego. Natomiast spotkanie w siedzibie Stałego Przedstawicielstwa RP przy Unii Europejskiej było okazją do wymiany doświadczeń na poziomie europejskim w zakresie prawa do prywatności i ochrony danych osobowych w Internecie.

**2. Seminarium „Prawnokarna ochrona danych osobowych”** (Warszawa, 25 lutego 2010 r.)

25 lutego 2010 r. odbyło się seminarium naukowe „Prawnokarna ochrona danych osobowych” zorganizowane przez Generalnego Inspektora Ochrony Danych Osobowych na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Współorganizatorem spotkania był Dziekan Wydziału Prawa prof. Jarosław Majewski.

**3. Konferencja „Ochrona danych osobowych w ubezpieczeniach – problemy w praktyce obrotu”** (Warszawa, 21 maja 2010 r.)

Konferencję poświęconą praktycznym aspektom zapewnienia ochrony danych osobowych w działalności ubezpieczeniowej, w której uczestniczył przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych, zorganizowali: Rzecznik Ubezpieczonych oraz Fundacja Edukacji Ubezpieczeń.

**4. II Konferencja naukowa „Bezpieczeństwo w Internecie”** (Warszawa, 8 czerwca 2010 r.)

Organizatorami konferencji, której honorowy patronat sprawował Generalny Inspektor Ochrony Danych Osobowych oraz Minister Sprawiedliwości, był Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie i Polski Instytut Demokracji Lokalnej. Konferencja poświęcona była aspektom prawnym, organizacyjnym i technicznym bezpiecznego korzystania z Internetu. Na spotkaniu tym GODO wygłosił referat na temat identyfikacji osób w Internecie w świetle orzecznictwa i przepisów o ochronie danych osobowych. W trakcie konferencji odbyło się również uroczyste wręczenie dyplomów absolwentom podyplomowych studiów prawno-informatycznych w zakresie ochrony danych osobowych, zorganizowanych na UKSW.

**5. Spotkanie GODO i RPO w sprawie retencji danych** (Warszawa, 10 sierpnia 2010 r.)

Generalny Inspektor Ochrony Danych Osobowych oraz jego zastępca spotkali się z prof. Ireną Lipowicz, Rzecznik Praw Obywatelskich, w celu omówienia zasad stałej współpracy obu instytucji. Głównym tematem spotkania była współpraca dotycząca m.in. działań na rzecz osób niepełnosprawnych. Wskazano również na potrzebę poprawy standardów ochrony danych osobowych, w szczególności w kwestii retencji danych telekomunikacyjnych.



#### 6. **Letnie Konwersatorium Ochrony Danych Osobowych** (Wisła, 20 sierpnia 2010 r.)

Krajowe Stowarzyszenie Ochrony Informacji Niejawnych było organizatorem odbywającego się co roku Letniego Konwersatorium Ochrony Danych Osobowych, podczas którego przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych przedstawił prezentację zatytułowaną „Zagrożenia związane z przetwarzaniem danych osobowych w systemach informatycznych. Wymagania dotyczące dokumentacji przetwarzania danych osobowych”. 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.

#### 7. **Międzynarodowa konferencja naukowa „Zarządzanie informacją i energią w systemie bezpieczeństwa Unii Europejskiej”** (Józefów k/Otwocka, 20 września 2010 r.)

Dyskusja na temat tego, jak informacja i energia w życiu codziennym i jej umiejętne wykorzystanie może wpłynąć na system bezpieczeństwa państw Unii Europejskiej, identyfikacja nowych zagrożeń, jakie generuje środowisko międzynarodowe XXI wieku w kontekście efektywnego wykorzystania i zarządzania informacją o nich dla celów związanych z usprawnieniem systemów informacyjnych państwa, to jedno z wielu tematów poruszonych na międzynarodowej konferencji naukowej z udziałem dr Wojciecha R. Wiewiórowskiego, Generalnego Inspektora Ochrony Danych Osobowych, który wygłosił na niej referat pt. Bezpieczeństwo informacji a dezinformacja”. Organizatorem tego wydarzenia była Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi i Euro-Centrum Park Naukowo-Technologiczny. Generalny Inspektor Ochrony Danych Osobowych zasiadał w Komitecie Honorowym konferencji.

#### 8. **Konferencja naukowa „Aktualne problemy rozgraniczenia właściwości sądów administracyjnych i powszechnych – zagadnienia szczegółowe”** (Warszawa, 29 września 2009 r.)

Reguły kolizyjne, rozstrzyganie sporów o właściwość pomiędzy sądami administracyjnymi i sądami powszechnymi (w szczególności w sprawach z zakresu prawa pracy i ubezpieczeń społecznych) to najważniejsze tematy poruszane na konferencji naukowej z udziałem dr Wojciecha R. Wiewiórowskiego, Generalnego Inspektora Ochrony Danych Osobowych. Organizatorami spotkania był Zakład Prawa Administracyjnego Instytutu Nauk Prawnych PAN oraz Naczelny Sąd Administracyjny.

**9. Cykl wykładów poświęconych problematyce ochrony danych osobowych na Wszechnicy Polskiej Szkoły Wyższej 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”. 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.

**8. VIII edycja seminarium „Jakość danych w systemach informatycznych zakładów ubezpieczeń społecznych”** (Warszawa, 11 października 2010 r.)

Tematyka seminarium dotyczyła zagadnień związanych z konsekwencjami nowelizacji ustawy o ochronie danych osobowych dla sektora ubezpieczeniowego, w szczególności w zakresie jej wpływu na standardy i procedury ochrony danych w zakładach ubezpieczeń. Na spotkaniu tym zastępca GIODO wygłosił referat pt. „Kodeksy Dobrych Praktyk jako gwarant postępowań zgodnych z prawem ochrony danych osobowych”. Organizatorem seminarium była Polska Izba Ubezpieczeń.

**9. Konferencja „Czy istnieje uniwersalny standard praw człowieka? Kulturowe i cywilizacyjne uwarunkowania statusu jednostki”** (Chlewiska k/Szydłowca, 22-23 października 2010 r.)

Luksemburska Fundacja Praw Człowieka oraz Katedra Prawa Konstytucyjnego Uniwersytetu Wrocławskiego zorganizowały Konferencję „Czy istnieje uniwersalny standard praw człowieka? Kulturowe i cywilizacyjne uwarunkowania statusu jednostki”, na której GIODO wygłosił referat zatytułowany *„Ochrona danych osobowych w Europie na tle światowych standardów ochrony prywatności”*.

**10. VIII edycja studiów podyplomowych** (Sosnowiec, 23 października 2010 r.)

Na Wydziale Informatyki i Nauki o Materiałach Uniwersytetu Śląskiego w Sosnowcu, podczas inauguracji VIII edycji Studiów podyplomowych „Ochrona informacji niejawnych i administracja bezpieczeństwa informacji”, Generalny Inspektor Ochrony Danych Osobowych wygłosił przemówienie

*„Przetwarzanie danych w chmurze (cloud computing), jako nowe wyzwanie dla prawa ochrony informacji”.*

**11. I Krajowe Forum Kierowników Jednostek Organizacyjnych oraz V Forum Pełnomocników ds. Ochrony Informacji Niejawnych** (Rynia k/Warszawy, 3 listopada 2010 r.)

*„Nowe technologie i rozwiązania prawne a potrzeby i wyzwania społeczeństwa informacyjnego”* to tytuł wystąpienia dr Wojciecha R. Wiewiórowskiego, GODO, wygłoszonego podczas I Krajowego Forum Kierowników Jednostek Organizacyjnych oraz V Forum Pełnomocników ds. Ochrony Informacji Niejawnych. Organizatorem tych wydarzeń było Krajowe Stowarzyszenie Ochrony Informacji Niejawnych.

**12. Seminarium „Identyfikacja kluczowych zagadnień lokalnej administracji cyfrowej”** (Warszawa, 8 listopada 2010 r.)

Stowarzyszenie Miasta w Internecie było organizatorem seminarium poświęconemu kwestii identyfikacji kluczowych zagadnień związanych z funkcjonowaniem e-administracji. Na spotkaniu tym dr Wojciech R. Wiewiórowski, GODO, wygłosił referat *„Korzystanie z informacji osobowych przez pracowników administracji samorządowej”*.

**13. IX Forum ADO/ABI „Nowelizacja 2010 ustawy o ochronie danych osobowych”** (Warszawa, 16 listopada 2010 r.)

Program spotkania zdominowany został przez zagadnienia związane z nowelizacją ustawy o ochronie danych osobowych, a także z przyszłością prawa do prywatności i ochrony danych osobowych w świetle ostatnich stanowisk zajmowanych przez właściwe organy w Polsce i w innych krajach Unii Europejskiej. Podczas obrad, Generalny Inspektor Ochrony Danych Osobowych wygłosił referat, pt. *„Konsekwencje nowelizacji ustawy o ochronie danych osobowych oraz kierunki dalszych prac nad zmianami w publicznoprawnej ochronie danych osobowych”*. Spotkanie zorganizowało Centrum Promocji Informatyki.

**14. TransparencyCamp 2010** (Warszawa, 18 listopada 2010 r.)

*„Granice prywatności przy dostępie do informacji publicznej. Spojrzenie w przyszłość”* – referat pod takim tytułem wygłosił Generalny Inspektor Ochrony Danych Osobowych podczas TransparencyCamp 2010, zorganizowanego przez Stowarzyszenie Liderów Lokalnych Grup Obywatelskich.

**15. Konferencja „Od papierowej do cyfrowej: e-administracja w Polsce”** (Warszawa, 19 listopada 2010 r.)

*„Współdzielenie informacji przetwarzanych w rejestrach publicznych. Jawność formalna w świecie cyfrowym”* to tytuł wystąpienia dr Wojciecha R. Wiewiórowskiego, GODO, podczas Konferencji „Od papierowej do cyfrowej: e-administracja w Polsce”, zorganizowanej przez Władzę Wdrażającą Programy Europejskie.

**16. XIV Ogólnopolska Konferencja Uniwersyteckich Poradni Prawnych** (Kraków, 22-23 listopada 2010 r.)

Temat Konferencji odnosił się do praktycznych aspektów realizacji prawa do prywatności i ochrony danych osobowych w związku z działalnością poradni studenckich. Organizatorem wydarzenia była Fundacja Uniwersyteckich Poradni Prawnych i Krakowska Akademia im. Frycza Modrzewskiego. Uczestnikami zorganizowanego w ramach Konferencji szkolenia na temat zasad ochrony danych, byli przedstawiciele 25 studenckich poradni z całego kraju, a także z Ukrainy i Czech.

**17. XIV Kongres Administratorów Bezpieczeństwa Informacji** (Wisła, 1-3 grudnia 2010 r.)

Podczas XIV Kongresu Administratorów Bezpieczeństwa Informacji, zorganizowanego przez European Network Security Institute, Generalny Inspektor Ochrony Danych Osobowych wygłosił referat zatytułowany *„Nowelizacja ustawy o ochronie danych osobowych A.D. 2010 a kierunki zmian w zasadach ochrony prywatności w Europie”*.

**18. Debata „Bilingi, inwigilacja, interes publiczny”** (Warszawa, 2 grudnia 2010 r.)

„Bilingi, inwigilacja, interes publiczny” to temat debaty zorganizowanej 2 grudnia 2010 r. przez prof. Irenę Lipowicz, Rzecznik Praw Obywatelskich. Jej uczestnicy wskazywali, że należy wzmocnić kontrolę nad stosowaniem rozmaitych metod inwigilacji obywateli, takich jak wykorzystywanie danych z bilingów czy informacji o miejscu logowania się czyjegoś telefonu komórkowego. Generalny Inspektor Ochrony Danych Osobowych odniósł się do problemu zbyt szerokiej implementacji do polskiego porządku prawnego dyrektywy retencyjnej (dyrektywa 2006/24/WE), zobowiązującej państwa członkowskie Unii Europejskiej do zapewnienia, aby dostawcy usług telekomunikacyjnych oraz publicznie dostępnych usług internetowych, zatrzymywali i przechowywali szczegółowe informacje o wszystkich realizowanych połączeniach. Ponadto przedstawił uwagi wobec niektórych przepisów projektu ustawy o zmianie ustawy - Kodeks postępowania karnego oraz niektórych innych ustaw, a także omówił projektowany zakres zmian w ustawie z dnia 28 września 1991 r. o kontroli skarbowej. Zdaniem dr Wojciecha R. Wiewiórowskiego, GIODO, projekt ten przewiduje zbyt szerokie uprawnienia kontroli skarbowej w zakresie wykorzystywania dowodów uzyskanych podczas stosowania przez tę służbę kontroli operacyjnej.

**19. Konferencja z okazji obchodów Międzynarodowego Dnia Przeciwdziałania Korupcji** (Warszawa, 9 grudnia 2010 r.)

W ramach VIII obchodów Międzynarodowego Dnia Przeciwdziałania Korupcji odbyła się w Warszawie Konferencja z udziałem przedstawiciela Biura GIODO, poświęcona prawnym i społecznym aspektom działań antykorupcyjnych w sektorze publicznym i prywatnym oraz wypracowaniu i wdrożeniu dobrej praktyki walki z tym zjawiskiem. Organizatorem Dnia było Centralne Biuro Antykorupcyjne.

## **20. Seminarium „Reforma ochrony prywatności” (Warszawa, 16 grudnia 2010 r.)**

Konferencją „Reforma ochrony prywatności” Generalny Inspektor Ochrony Danych Osobowych otworzył publiczną debatę o tym, jak skutecznie chronić naszą prywatność w dobie dynamicznego rozwoju nowoczesnych technologii. Stała się ona przyczynkiem do wypracowania stanowiska w kwestii koniecznych zmian w polskich i unijnych przepisach dotyczących tego tematu. Podczas spotkania dr Wojciech R. Wiewiórowski, GIODO, wygłosił referat zatytułowany „Privacy by Design jako paradygmat ochrony prywatności. Legislacja z ‘wbudowaną’ ochroną prywatności”. Organizatorami konferencji byli Generalny Inspektor Ochrony Danych Osobowych, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie oraz Naukowe Centrum Prawno-Informatyczne.

### **6.2.7 Internet**

W roku 2010 przeprowadzona została modyfikacja systemu e-GIODO (platforma e-GIODO) w części dotyczącej obsługi funkcjonalności dostępnej pod nazwą „Twoja sprawa”. Jej celem było rozszerzenie udostępnianych przez tą funkcję informacji o wnioskach dotyczących rejestracji zbiorów danych osobowych lub ich zmianach, których obsługę zakończono wydaniem decyzji innej niż rejestracja lub aktualizacja zbioru. Modyfikacja ta wymagała dość istotnych zmian w strukturze bazy danych systemu e-GIODO oraz procedurach przenoszenia danych pomiędzy systemami e-GIODO i Rejestr Zbioru Danych Osobowych. Pod koniec 2010 r. opracowany został projekt kolejnej modyfikacji, której celem jest ułatwienie dla administratorów danych procesu wypełniania wniosku o rejestrację poprzez dodanie podpowiedzi w formie listy specyfikującej najczęściej występujące podstawy prawne. Zgodnie z zaplanowanym harmonogramem prac wdrożenie tej ostatniej modyfikacji planowane jest na koniec stycznia 2011 r.

### **6.2.8 Inne informacje**

#### **a) Porozumienie pomiędzy GIODO a Związkiem Pracodawców Branży Internetowej IAB Polska**

Ochronie prywatności i bezpieczeństwu danych osobowych użytkowników sieci służyć miała inicjatywa GIODO nawiązania współpracy z dostawcami usług internetowych. Zaowocowała ona podpisaniem 28 stycznia 2010 r. porozumienia ze Związkiem Pracodawców Branży Internetowej IAB Polska. Dostawcy usług zobowiązali się w nim do zapewnienia właściwego stosowania przepisów o ochronie danych osobowych oraz podjęcia wspólnych działań nad opracowaniem kodeksu dobrych praktyk. Poprzez podpisanie ww. porozumienia, firmy zrzeszone w IAB Polska, w tym wszystkie największe media internetowe chciały pokazać, że przywiązują szczególną wagę do zapewnienia bezpieczeństwa danych osobowych swoich użytkowników i zainteresowane są wypracowaniem wspólnie z GIODO kodeksu dobrych praktyk, który pozwoli jeszcze lepiej je chronić.

#### **b) Porozumienie pomiędzy GIODO a Uniwersytetem Śląskim w Katowicach**

W dniu 23 października 2010 r. Generalny Inspektor Ochrony Danych Osobowych podpisał z Prorektorem ds. Nauki i Współpracy z Gospodarką Uniwersytetu Śląskiego Porozumienie zakresie współpracy w zakresie ochrony danych osobowych. Porozumienie było rezultatem wieloletniej współpracy dr Wojciecha R. Wiewiórowskiego, GIODO, z Instytutem Informatyki Wydziału Informatyki i Nauki o Materiałach Uniwersytetu Śląskiego, gdzie prowadzone są Studia podyplomowe z zakresu ochrony danych osobowych. Współpraca obejmować będzie m. in. realizację wspólnych projektów badawczych, opracowywanie publikacji oraz wymianę materiałów naukowych i dydaktycznych, organizację konferencji, seminariów, sympozjów, szkoleń i warsztatów, a także inne formy podejmowanych wspólnie działań i wzajemnego świadczenia pomocy. Z okazji oficjalnego rozpoczęcia kolejnej edycji Studiów podyplomowych *Ochrona informacji niejawnych i administracja bezpieczeństwa informacji*, Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład inauguracyjny „Przetwarzanie danych w chmurze (cloud computing) jako nowe wyzwanie dla prawa ochrony informacji”.

#### **c) Udział w pracach Komitetu Technicznego nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych przy Polskim Komitecie Normalizacyjnym**

Podobnie, jak w latach poprzednich, również w 2010 r. Generalny Inspektor Ochrony Danych Osobowych aktywnie 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 2010 w ramach ww. Komitetu Technologicznego KT-182 przygotowanych zostało 35 projektów norm.

#### **d) Współpraca GIODO z Naszą Klasą**

W analizowanym roku 2010 kontynuowana była - zainicjowana w 2009 r. - współpraca Generalnego Inspektora Ochrony Danych Osobowych z portalem nk.pl, na którym w specjalnej zakładce pomaga jego użytkownikom bezpiecznie korzystać z Internetu i wyjaśnia kwestie związane z ochroną danych. W zakładce *Bezpieczeństwo* znajdują się materiały poświęcone między innymi konsekwencjom nieprzemyślanych działań w Internecie oraz prezentacja instytucji oferujących pomoc dla ofiar cyberprzemocy.

**e) Spotkanie dotyczące budowy europejskiego odpowiednika systemu ESTA w Unii Europejskiej**

W dniu 24 marca 2010 r. w siedzibie Generalnego Inspektora Ochrony Danych Osobowych, odbyło się spotkanie z ekspertami PricewaterhouseCoopers (PwC) dotyczące ewentualnej budowy europejskiego odpowiednika amerykańskiego/australijskiego systemu ESTA (Electronic System for Travel Authorization) w Unii Europejskiej. PricewaterhouseCoopers jest globalną organizacją świadczącą profesjonalne usługi doradcze we wszystkich sektorach gospodarki. Podczas spotkania eksperci PwC przedstawili ogólny zarys ich zadań oraz harmonogram prac. Przebadane zostały cztery państwa UE – Holandia, Francja, Grecja oraz Polska (ze względu na najdłuższą granicę zewnętrzną w Unii) - pod kątem spełnienia warunków budowy wspomnianego systemu. W opinii Generalnego Inspektora Ochrony Danych Osobowych na obecnym etapie wprowadzenie tego projektu w życie nie znajduje uzasadnienia. Niezbędne jest wprawdzie uzasadnienie istnienia EU ESTA oraz szczegółowa analiza obecnych rozwiązań i systemów w ramach np. VIS, SIS i innych.

**f) Newsletter „Prywatność w świecie. Przegląd wydarzeń.”**

W celu zagwarantowania systematycznego otrzymywania informacji dotyczących ochrony prywatności i danych osobowych za granicą, od września 2008 r. Departament Edukacji Społecznej i Współpracy Międzynarodowej cyklicznie rozsyła pracownikom Biura GIODO tłumaczenia artykułów z prasy zagranicznej w postaci Newslettera „Prywatność w świecie. Przegląd wydarzeń.” W 2010 r. dokonał tłumaczeń i przekazał 5 numerów Newslettera o łącznej liczbie 27 artykułów.

**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 na forum Unii Europejskiej. Do najważniejszych zadań GIODO w ramach współpracy międzynarodowej należy udział w pracach Grupy Roboczej Art. 29 ds. ochrony danych osobowych, w tym w pracach podgrup tematycznych, współpraca z rzecznikami ochrony danych innych krajów - w szczególności w ramach Grupy Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej – i związany z tym udział w organizowanych cyklicznie Międzynarodowych Konferencjach Rzeczników Ochrony Danych Osobowych i Prywatności, Wiosennych Konferencjach Europejskich Organów

Ochrony Danych oraz w Warsztatach Rozpatrywania Spraw. Uczestniczy także w pracach Komitetu Konsultacyjnego ds. Konwencji Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (T-PD). Inne ważne zadania stojące przed polskim organem ds. ochrony danych w ramach współpracy międzynarodowej, związane są z jego udziałem w pracach Wspólnego Organu Nadzorczego zajmującego się zagadnieniami ochrony danych osobowych w związku z utworzeniem Strefy Schengen (WON Schengen), Wspólnego Organu Nadzorczego nad Europolem (WON Europolu), a także Wspólnego Organu Nadzorczego właściwego w sprawach ochrony danych osobowych w Systemie Informacji Celnej (WON Cła). Ponadto bierze aktywny udział w pracach grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac oraz Systemem Informacji Celnej, a także Grupy roboczej ds. policji i wymiaru sprawiedliwości oraz Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji.

W omawianym roku sprawozdawczym 2010, podobnie jak w latach poprzednich, na szczególne podkreślenie zasługuje zwłaszcza współpraca Generalnego Inspektora z w ramach **Grupy Roboczej Art. 29 ds. ochrony danych osobowych** (GR Art. 29), która została ustanowiona na podstawie art. 29 dyrektywy 95/46/WE. W skład Grupy Roboczej wchodzi po jednym przedstawicielu z każdego państwa członkowskiego UE, Europejski Inspektor Ochrony Danych Osobowych oraz przedstawiciel Komisji Europejskiej. Spotkania GR Art. 29 odbywają się cztery razy w roku, w Brukseli. Podczas pierwszego posiedzenia Grupy Roboczej Art. 29, które miało miejsce 15-16 lutego 2010 r., odbyły się wybory nowych władz Grupy. Na stanowisko Przewodniczącego wybrany został Pan Jacob Kohnstamm, Dyrektor Holenderskiego Organu Ochrony Danych. Natomiast na funkcje wiceprzewodniczących Grupy Roboczej Art. 29 wybrani zostali Pan Michał Serzycki, Generalny Inspektor Ochrony Danych Osobowych III kadencji oraz Pan Artemi Rallo Lombarte, Dyrektor Hiszpańskiej Agencji Ochrony Danych. W trakcie posiedzenia Grupa Robocza Art. 29 przyjęła także Program prac na lata 2010-2011 (WP 170)<sup>101</sup>, w którym podkreślono, że celem Grupy będzie przede wszystkim zapewnienie spójnego i prawidłowego stosowania istniejących ram prawnych w zakresie ochrony danych osobowych. Grupa w swoich pracach skoncentruje się również na wyzwaniach związanych z rozwojem nowych technologii, globalizacją i zmianami instytucjonalnymi wynikającymi z wejścia w życie Traktatu Lizbońskiego. W ramach prac dotyczących zapewnienia prawidłowego stosowania istniejących ram prawnych i przygotowania przyszłych działań, Grupa Robocza Art. 29 postanowiła skoncentrować się na interpretacji najważniejszych przepisów dyrektywy 95/46/WE (administrator danych/przetwarzający, prawo właściwe, realizacja zasady związania celem, analiza podstaw prawnych przetwarzania danych osobowych), a także na kwestiach związanych z wdrożeniem dyrektywy o prywatności i łączności elektronicznej i oceną skutków wejścia w życie Traktatu

---

<sup>101</sup> Dokumenty przyjęte przez Grupę Roboczą Art. 29 w wersji elektronicznej dostępne są na stronie internetowej: [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm)



Lizbońskiego. W odniesieniu do wyzwań związanych z procesem globalizacji, Grupa zaplanowała dalsze działania mające na celu rozwój wiążących reguł korporacyjnych (BCR), udział w pracach normalizacyjnych (np. w ramach ISO), rozwijanie międzynarodowych standardów w zakresie ochrony danych i udział w przeglądzie wytycznych OECD w sprawie ochrony danych osobowych. Natomiast w odniesieniu do wyzwań technologicznych, Grupa ma się skoncentrować na analizie technologii „cloud computing”, profilowaniu, a także na ocenie skutków w odniesieniu do ochrony prywatności i danych w zakresie identyfikacji radiowej (RFID). Ponadto przedmiotem działań mają być kwestie związane z wyszukiwarkami, prawem do zapomnienia i portalami społecznościowymi. Odrębnymi grupami spraw będących przedmiotem prac Grupy Roboczej art. 29 są: zwiększenie skuteczności działań organów ochrony danych i samej Grupy Roboczej art. 29 oraz inne kwestie sektorowe (np. dane osobowe podróżnych, przekazywanie danych w kontekście transferów finansowych).

W roku sprawozdawczym 2010 Generalny Inspektor Ochrony Danych Osobowych uczestniczył w Brukseli w czterech posiedzeniach wspomnianej Grupy. W trakcie kolejnych spotkań przyjęto opinię 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”; opinię 2/2010 w sprawie internetowej reklamy behawioralnej, jak również opinię 3/2010 w sprawie zasady odpowiedzialności. Grupa Robocza wypowiedziała się również na temat europejskiego kodeksu postępowania Europejskiej Federacji Marketingu Bezpośredniego (FEDMA) w sprawie ochrony danych osobowych wykorzystywanych w marketingu bezpośrednim (opinia 4/2010) oraz na temat propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (opinia 5/2010). Odrębne opinie zostały poświęcone sprawie odpowiedzialności (nr 6/2010), Komunikatowi Komisji Europejskiej w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażerów (PNR) państwom trzecim (nr 7/2010), a także w sprawie prawa właściwego (nr 8/2010). Grupa Robocza Art. 29 przyjęła także Raport 1/2010 dotyczący sposobu wdrożenia dyrektywy 2006/24/WE w sprawie zatrzymywania danych transmisyjnych oraz dokument pt. „Najczęściej zadawane pytania związane z wejściem w życie decyzji Komisji Europejskiej 2010/87/UE” z dnia 5 lutego 2010 r. dotyczący standardowych klauzul umownych wykorzystywanych do przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich, zgodnie z dyrektywą 95/46/WE Parlamentu Europejskiego i Rady (WP 176).

W 2010 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. GODO kontynuował również współpracę na forum Wspólnego Organu Nadzorczego Schengen oraz Wspólnego Organu Nadzorczego ds. systemu informacji celnej.

W 2010 r. Generalny Inspektor Ochrony Danych Osobowych uczestniczył w pracach grupy koordynującej nadzór nad **systemem Eurodac**, w ramach których przyjęto rekomendacje dotyczące wykorzystywania systemu DubliNet, a także rozpoczęto prace nad skoordynowaną kontrolą dotyczącą zasad usuwania danych.

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. Jednocześnie zajmowano się różnymi aspektami wdrożenia Konwencji z Prüm, w tym przekazywaniem danych DNA do państw trzecich, czy dialogiem prowadzonym ze Stanami Zjednoczonymi Ameryki w sprawie standardów ochrony danych osobowych. Innym ważnym obszarem prac było przygotowanie katalogu dotyczącego nadzoru i współpracy.

Jedną z form współpracy GODO z innymi organami ochrony danych osobowych był udział w różnego rodzaju międzynarodowych projektach badawczych. W 2010 r. polski organ ds. ochrony danych osobowych uczestniczył w dwóch takich projektach finansowanych przez Komisję Europejską. Jeden z nich o nazwie „European Privacy and Human Rights (EPHR) prowadzony był przez Electronic Privacy Information Center<sup>102</sup> i Privacy International and Central European University. Rezultatem projektu było sporządzenie raportu na temat europejskiego ustawodawstwa oraz najnowszych zagadnień dotyczących ochrony prywatności, opublikowanego w przeglądzie EPIC’u pt. „Prywatność i Prawa Człowieka”. Drugi z kolei projekt dotyczył „Badania w ramach oceny wpływu przyszłych ram prawnych UE na ochronę danych osobowych”. Badanie prowadzone było przez GHK Consulting w imieniu Dyrekcji Generalnej ds. Wolności, Bezpieczeństwa i Sprawiedliwości Komisji Europejskiej i miało na celu dostarczenie Komisji informacji m.in. o charakterze i skali obecnych problemów w obszarze ochrony danych i ułatwić ocenę istniejącego w tym zakresie ustawodawstwa. W szczególności zaś o uzyskanie konkretnych informacji o przypadkach nielegalnego przetwarzania/naruszeniach ochrony danych i o ich skutkach, a także o zadośćuczynieniu, karach i odszkodowaniach dla osób, których dane dotyczą.

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.

---

<sup>102</sup> Więcej informacji na temat projektu można znaleźć na stronie: <http://phr.privacyinternational.org/>

## 7.1 Międzynarodowe spotkania i konferencje

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

### 1. **Wiosenna Konferencja Europejskich Rzeczników Ochrony Danych i Prywatności** (Praga, 29-30 kwietnia 2010 r.)

Organizatorem Wiosennej Konferencji był Przewodniczący Urzędu Ochrony Danych Osobowych Republiki Czeskiej. Motto tegorocznego spotkania organów ochrony danych i prywatności brzmiało: „Ocena przeszłości z myślą o przyszłości”. Jego głównym celem było przedyskutowanie kwestii dotyczących mocnych i słabych stron europejskich przepisów dotyczących ochrony danych w kontekście postępującej globalizacji, a także określenie ich skutków dla obywateli, prawodawców i administratorów danych. Na Konferencji tej przyjęte zostały następujące rezolucje: o przyszłości rozwoju ochrony danych; w sprawie rozpoczęcia wspólnych działań informacyjnych oraz edukacji dzieci i młodzieży na szczeblu europejskim i międzynarodowym; w sprawie planowanej umowy pomiędzy Unią Europejską a Stanami Zjednoczonymi w sprawie standardów ochrony danych w obszarze współpracy policyjnej i sądowej w sprawach karnych, a także rezolucja dotycząca zasad używania skanerów ciała (urządzeń prześwietlających sylwetkę) dla zapewnienia bezpieczeństwa na lotniskach.

### 2. **XII. Spotkanie Rzeczników Ochrony Danych Osobowych Europy Środkowej i Wschodniej** (Sopot, 17-20 maja 2010 r.)

Temat XII Spotkania Rzeczników Ochrony Danych Osobowych Europy Środkowej i Wschodniej (Central and Eastern European Data Protection Authorities – CEEDPA) koncentrował się wokół zagadnień związanych z rozwojem nowoczesnych technologii wykorzystywanych w stosunkach pracy oraz ochroną prywatności i danych osobowych w mediach elektronicznych. Omawiano kwestie odnoszące się do nowoczesnych metod identyfikacji i sprawowania nadzoru nad pracownikami oraz zagadnienia ochrony danych w kontekście interesu publicznego w mediach elektronicznych. W Spotkaniu tym udział wzięło 20 przedstawicieli organów ochrony danych osobowych z 11 krajów, w tym po raz pierwszy z Mołdawii i Albanii. Należy podkreślić, że rzecznicy biorący udział w Spotkaniu zaprosili również do współpracy te kraje, w których prace nad przepisami prawa z dziedziny ochrony danych osobowych dopiero się rozpoczynają. W trakcie obrad przyjęto dwie deklaracje. Pierwsza z nich dotyczyła rozwoju współpracy i wspierania nowych członków CEEDPA – Albanii i Mołdawii. Druga zaś odnosiła się do trwających prac nad zmianą dyrektywy 96/46/WE Rady i Parlamentu Europejskiego o ochronie osób w związku z przetwarzaniem danych osobowych oraz ich swobodnym przepływem.

3. **26. plenarne posiedzenie Komitetu Konsultacyjnego Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych T-PD** (Strasburg, 1-4 czerwca 2010)

Najważniejsze decyzje podjęte na posiedzeniu to przyjęcie rekomendacji w sprawie profilowania oraz wybory nowego Komisarza Ochrony Danych przy Radzie Europy. Ponownie wybrano na to stanowisko dotychczasowego komisarza Pana Karla Neuwirta.

4. **48. Spotkanie Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji** (Berlin, 6 - 7 września 2010 r.)

Tematem debaty były kwestie związane z ochroną danych osobowych w związku z dynamicznym rozwojem nowych technologii w dziedzinie telekomunikacji i próba znalezienia równowagi między prawnie uzasadnionymi potrzebami przedsiębiorstw i państwa wykorzystujących różne informacje do wypełniania swoich zadań a prawem obywateli do prywatności i ochrony danych osobowych. Podczas spotkania omawiane były zagadnienia przetwarzania danych osobowych w „samochodowych czarnych skrzynkach”, mobilność a bezpieczeństwo, ochrona danych osobowych w portalach społecznościowych, dane geoprzestrzenne, ochrona prywatności i międzynarodowa standaryzacja oraz prezentacja usługi „deleteme.on” i jednej z aplikacji płatności dla telefonów komórkowych. Ponadto Grupa obradowała nad wspólnym stanowiskiem w sprawie ochrony prywatności i informacji o lokalizacji w usługach komunikacji bezprzewodowej.

5. **Spotkanie ekspertów w zakresie dotyczącym kradzieży dokumentów identyfikacyjnych oraz zarządzania identyfikacją** (Bruksela, 4-5 października 2010 r.)

Głównym punktem spotkania ekspertów w zakresie dotyczącym kradzieży dokumentów identyfikacyjnych oraz zarządzania identyfikacją, które odbyło się w Brukseli w dniach 4-5 października 2010 r. było przedstawienie raportu z badań Komisji Europejskiej, który informował o zakresie przestępczości w zakresie kradzieży i fałszowania dokumentów oraz prawno-administracyjnych uwarunkowaniach walki z tą przestępczością w poszczególnych krajach „Comparative study on identity theft (national legislation and reporting mechanisms)”. W podsumowaniu spotkania wskazano na różnorodność środków prawnych w różnych krajach do walki z tą formą przestępczości i podkreślono konieczność opracowania specjalnych przepisów dotyczących raportowania. Zaznaczono, że równie najważniejszym elementem jest istnienie specjalnych linii zgłoszeń oraz powinny być prowadzone publiczne kampanie edukacyjne w tym zakresie.

6. **32. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności** (Jerozolima, 27 – 29 października 2010 r.)

W dniach 25 – 30 października 2010 r. Generalny Inspektor Ochrony Danych Osobowych przebywał z wizytą w Jerozolimie, w związku z uczestnictwem w 32. Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności oraz w seminarium organizowanym przez

Organizację Współpracy Gospodarczej i Rozwoju z okazji 30-lecia OECD. W tym czasie spotkał się z Ambasadorem RP w Izraelu, Panią Agnieszką Magdziak-Miszewską. Odbywające się corocznie międzynarodowe konferencje rzeczników ochrony danych uważane są za najważniejsze spotkania przedstawicieli organów ochrony danych osobowych z przedstawicielami Rady Europy, Komisji Europejskiej oraz korporacji międzynarodowych i świata nauki. Organizacja tegorocznej Konferencji zbiegła się z trwającymi na forum Unii Europejskiej pracami, mającymi na celu uznanie przez Komisję Europejską obowiązującego w Izraelu ustawodawstwa za zapewniające odpowiedni poziom ochrony danych osobowych. Podczas ogólnodostępnych sesji otwartych prowadzone były rozmowy m. in. na temat zagrożeń związanych z rozwojem nowych technologii, zapewnieniem bezpieczeństwa użytkownikom Internetu oraz podjęcia odpowiednich działań chroniących prawa obywateli. Zebrani zastanawiali się również nad przyszłością ochrony danych oraz kierunkami prowadzenia polityki ochrony prywatności w zmieniającym się świecie. Podczas sesji zamkniętej przyjęte zostały następujące dokumenty: *Rezolucja w sprawie grupy roboczej ds. organizacji konferencji*, *Rezolucja wzywająca do organizacji konferencji międzynarodowej mającej na celu opracowanie wiążącego instrumentu międzynarodowego w zakresie prywatności i ochrony danych osobowych* oraz *Rezolucja w sprawie prywatności w fazie projektowania*.

Natomiast na seminarium z okazji 30-lecia wydania przez OECD wytycznych dotyczących międzynarodowych przepływów danych osobowych, dyskutowano o możliwych sposobach stosowania prawa o ochronie danych osobowych oraz o możliwych rozwiązaniach, które mogą zostać przyjęte w przyszłości<sup>103</sup>.

#### 7. **Obrady Światowej Sieci Egzekwowania Przepisów o Ochronie Prywatności** (Jerozolima, 28 października 2010 r.)

W dniu 28 października 2010 r. podczas pobytu w Jerozolimie w związku z odbywającą się 32. Międzynarodową Konferencją Rzeczników Ochrony Danych Osobowych i Prywatności (ICDPPC), Generalny Inspektor Ochrony Danych Osobowych brał udział w posiedzeniu forum o nazwie **Światowa Sieć Egzekwowania Przepisów o Ochronie Prywatności (Global Privacy Enforcement Network - GPEN)**. Misją tej organizacji jest m. in. wymiana informacji i doświadczeń na arenie międzynarodowej, na temat problemów dotyczących ochrony prywatności oraz wspieranie dialogu z podmiotami sektora prywatnego w tym zakresie. GPEN skupia obecnie 19 organów ochrony danych osobowych, w tym Międzynarodową Komisję Handlu USA. Od listopada 2010 r. wśród członków tej międzynarodowej sieci znajduje się Generalny Inspektor Ochrony Danych Osobowych.

---

<sup>103</sup> Więcej informacji na stronie <http://www.privacyconference2010.org/>

## 8. Europejski Kongres Ochrony Danych IAPP (Paryż, 29-30 listopada 2010 r.)

Inauguracyjny Europejski Kongres Ochrony Danych z udziałem przedstawiciela Biura GODO, który wziął udział w panelu poświęconym ochronie prywatności w stosunkach pracy, miał miejsce 29-30 listopada 2010 r. w Paryżu, zorganizowany był przez Międzynarodowe Stowarzyszenie Ekspertów ds. Prywatności (International Association of Privacy Professionals - IAPP). Jest to forum skupiające ekspertów z dziedziny ochrony danych zaangażowanych w działania propagujące ideę ochrony danych osobowych, poprzez organizację spotkań, debat, konferencji oraz działania edukacyjne.

### 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 **16-18 czerwca 2010 r. przedstawiciele Generalnego Inspektora Ochrony Danych Osobowych** **złożyli wizytę w węgierskim organie ochrony danych osobowych.** Spotkanie z Andrássem Jóri, Rzecznikiem Ochrony Danych i Wolności Informacji Węgier, miało związek ze współpracą obu organów w ramach projektu partnerskiego *„Zwiększanie świadomości w zakresie ochrony danych wśród przedsiębiorców funkcjonujących na rynkach Unii Europejskiej”* finansowanego ze środków Unii Europejskiej w ramach Programu Leonardo da Vinci „Uczenie się przez całe życie”. Jednym z efektów tej współpracy miałoby być powstanie poradnika dla przedsiębiorców, w którym przedstawione zostaną problemy ochrony danych w kontekście prowadzenia działalności gospodarczej, przeprowadzony zostanie przegląd praktyk stosowanych w poszczególnych krajach partnerskich w zakresie stosowania przepisów prawa o ochronie danych osobowych, a także 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.

### 7.3 Warsztaty Rozpatrywania Spraw

Przedstawiciele Biura Generalnego Inspektora Ochrony Danych Osobowych systematycznie uczestniczą w organizowanych dwa razy w roku warsztatach rozpatrywania spraw, tzw. warsztatach skargowych (case handling workshop). W dniach 18-19 marca 2010 r. odbyły się w Brukseli **XXI warsztaty rozpatrywania spraw**, zorganizowane przez Rzecznika Ochrony Danych Osobowych

Belgii. Podczas warsztatów omawiane były kwestie związane z odpowiedzialnością dostawców usług internetowych, określeniem ram prawnych dla reklam behawioralnych w Internecie, znalezieniem równowagi pomiędzy wolnością badań naukowych a ochroną danych osobowych, projekt Google Street View, sprawa opłat drogowych oraz systemu pay-as-you-drive.

Natomiast **XXII warsztaty rozpatrywania spraw** odbyły się w dniach 20-21 września 2010 r. w Manchesterze. Ich organizatorem był Rzecznik Informacji (ICO) w Wielkiej Brytanii. Organizatorzy spotkania przedstawili uczestnikom strukturę organizacyjną i działalność Biur organów ochrony danych z kilku wybranych krajów: Wielkiej Brytanii, Holandii, Czech, Hiszpanii, Szwecji, Finlandii i Danii.

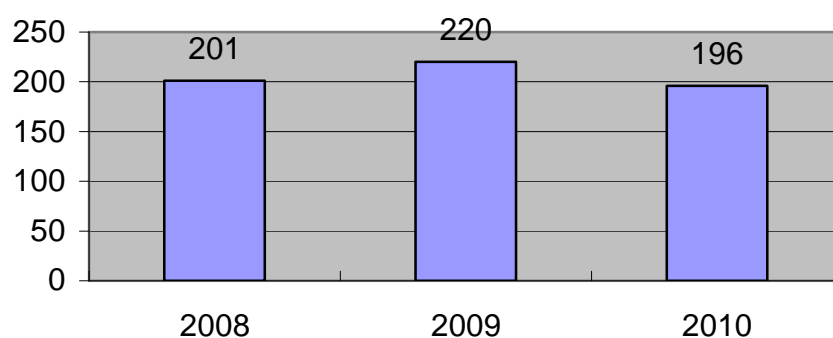
#### **7.4 Warsztaty TAIEX**

W dniu 16 grudnia 2010 r. przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych uczestniczył w Warsztatach TAIEX zorganizowanych w Kijowie przez Dyрекcję ds. Rozszerzenia Komisji Europejskiej w związku z przyjęciem w ukraińskim porządku prawnym ustawodawstwa o ochronie danych osobowych. Celem warsztatów poświęconych kwestiom prawnym i instytucjonalnym ram ochrony danych osobowych było przekazanie przedstawicielom ukraińskiej administracji publicznej, informacji i doświadczeń związanych ze stosowaniem europejskiego i krajowego prawa ochrony danych osobowych.

### **Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2010 roku**

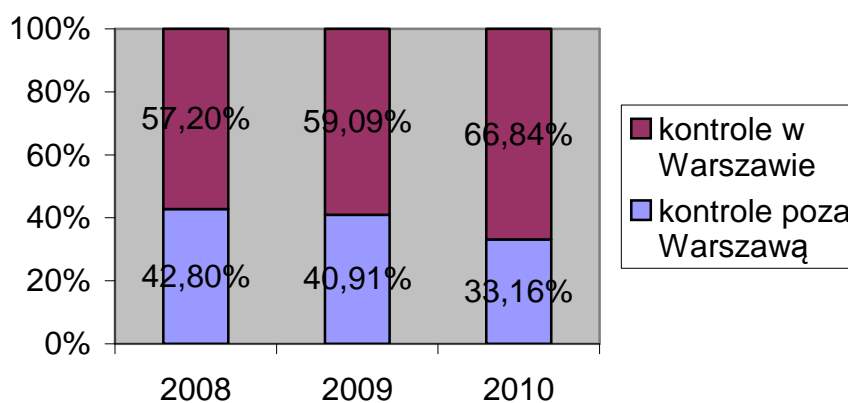
W odniesieniu do przeprowadzonych **kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych należy stwierdzić, że – podobnie jak w latach ubiegłych – znaczna część kontrolowanych podmiotów nadal miała problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych przed ich udostępnieniem bądź zabránieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także z prawidłowym opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych, w tym polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

W 2010 r. przeprowadzonych zostało 196 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W porównaniu z poprzednim rokiem sprawozdawczym, w którym było 220 kontroli, liczba ta nieznacznie spadła (zob. Wykres 33), ale wciąż utrzymuje się na wyrównanym poziomie.



Wykres 33: *Porównanie liczby kontroli przeprowadzonych w latach 2008–2010.*

Z kolei Wykres 34 przedstawia procentowe zastawienie kontroli przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych na terenie Warszawy oraz poza nią.



Wykres 34: *Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2008–2010.*



Najwięcej kontroli przeprowadzonych zostało z urzędu (120). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący:

Inicjatywa kontroli	Liczba kontroli
Z urzędu	120
Departament Orzecznictwa, Legislacji i Skarg	51
Departament Rejestracji Zbiorów Danych Osobowych	14
Prokuratura	2
W związku z inną kontrolą	9
<b>RAZEM</b>	<b>196</b>

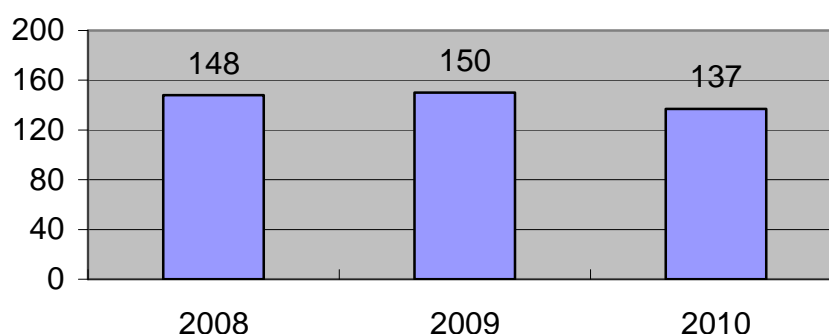
Czynnościom kontrolnym poddane zostały m.in. firmy inwestycyjne prowadzące działalność maklerską, szkoły wyższe, urzędy kontroli skarbowej oraz dostawcy usług telekomunikacyjnych. Dużą grupę jednostek kontrolowanych stanowiły również podmioty zaliczone do sektora „Inne”, obejmującego te podmioty, które 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 objęto w 2010 r. szkoły wyższe (26 kontroli), firmy inwestycyjne prowadzące działalność maklerską (16 kontroli), urzędy kontroli skarbowej (10 kontroli), dostawców usług telekomunikacyjnych (14 kontroli), komunalne jednostki organizacyjne (16 kontroli) oraz towarzystwa ubezpieczeniowe (12 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.

W okresie sprawozdawczym, w związku z obecnością Polski w strefie Schengen, przeprowadzono kontrole mające na celu sprawdzenie, czy wykorzystywanie przez Szefa Urzędu do Spraw Cudzoziemców danych osobowych przetwarzanych w Krajowym Systemie Informatycznym, nie narusza praw osób, których dane dotyczą, a w szczególności, na jakiej podstawie dokonano wpisu tych danych do Systemu Informacyjnego Schengen.

Sprawdzano ponadto, czy podmioty, wobec których Generalny Inspektor wydał decyzje nakazujące usunięcie uchybień w procesie przetwarzania danych osobowych, przywróciły stan zgodny z prawem. W tym celu upoważnieni inspektorzy przeprowadzili **11 kontroli sprawdzających** wykonanie decyzji administracyjnych, w toku których stwierdzono, że 9 podmiotów poddanych w tym zakresie kontroli wykonało wydane wobec nich decyzje.

W 2010 r. Generalny Inspektor w związku z przeprowadzonymi kontrolami wydał łącznie **137 decyzji administracyjnych**.



Wykres 35: *Porównanie liczby decyzji wydanych w związku z kontrolami przeprowadzonymi w latach 2008–2010.*

Oceniając wyniki przeprowadzonych kontroli należy stwierdzić, że spora grupa administratorów danych miała problemy z prawidłowym sformułowaniem treści oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych, tak aby wyrażona w taki sposób zgoda nie była domniemana lub dorozumiana z oświadczenia woli o innej treści. Analiza treści oświadczeń zebranych w toku kontroli niejednokrotnie wskazywała, że osobom składającym oświadczenie nie została zapewniona swoboda wyboru przy składaniu tych oświadczeń. Do częstych uchybień w tym zakresie należało również łączenie w jednym oświadczeniu zgód na różne cele przetwarzania danych i na rzecz kilku podmiotów. Jednostki kontrolowane miały również problemy 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.

Przeprowadzone kontrole wykazały również, że kontrolowane jednostki nadal mają problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniami przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także z prawidłowym opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń i kategorii danych objętych ochroną, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Nieprawidłowości w tym zakresie

stwierdzono w szczególności w toku kontroli szkół wyższych. 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.

Szczegółowa analiza ustaleń dokonanych w toku kontroli wskazuje, że ponad 12 % kontrolowanych jednostek nie opracowało dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zdarzały się również sytuacje, że opracowane dokumenty nie spełniały wymogów określonych 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. Dotyczyło to zarówno polityki bezpieczeństwa (30 % opracowanych dokumentów nie zawierało wszystkich elementów), jak i instrukcji zarządzania systemem informatycznym, gdzie 19 % opracowanych dokumentów nie zawierało niezbędnych informacji. W porównaniu z rokiem 2009 odnotowano również tendencję spadkową w realizacji obowiązków odnoszących się do wyznaczenia administratora bezpieczeństwa informacji oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych. Ponad 5 % kontrolowanych jednostek nie wyznaczyło administratora bezpieczeństwa informacji. Około 8 % podmiotów nie prowadziło ewidencji lub ewidencja nie spełniała wymagań określonych w art. 39 ust. 1 ustawy o ochronie danych osobowych. Uzyskane wyniki dotyczące prowadzonej dokumentacji, jak i powołania administratora bezpieczeństwa informacji, wskazują na tendencję spadkową w porównaniu z rokiem 2009. Jedną z przyczyn tego stanu były liczne nieprawidłowości w tym zakresie stwierdzone w procesie przetwarzania danych w jednostkach należących do sektora komunalnych jednostek organizacyjnych oraz szkół wyższych.

W kontrolowanych w 2010 r. podmiotach stwierdzano uchybienia polegające na braku wymaganych funkcjonalności systemów informatycznych służących do przetwarzania danych osobowych. Uchybienia te dotyczyły najczęściej braku odnotowania daty pierwszego wprowadzenia danych do systemu (ponad 10 %), braku odnotowywania identyfikatora użytkownika wprowadzającego dane do systemu (ponad 10 %). Brak powyższych odnotowań był również jednym z powodów tego, że systemy informatyczne nie umożliwiały wygenerowania i wydrukowania raportu, o którym mowa w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (ponad 15 % systemów).

W 2010 r. nadal napotymano również na nieprawidłowości polegające na niestosowaniu środków kryptograficznej ochrony danych w przypadkach ich teletransmisji z wykorzystaniem sieci publicznej, w tym sieci Internet. Uchybienia te dotyczyły braku bądź niewłaściwej implementacji protokołu kryptograficznego.

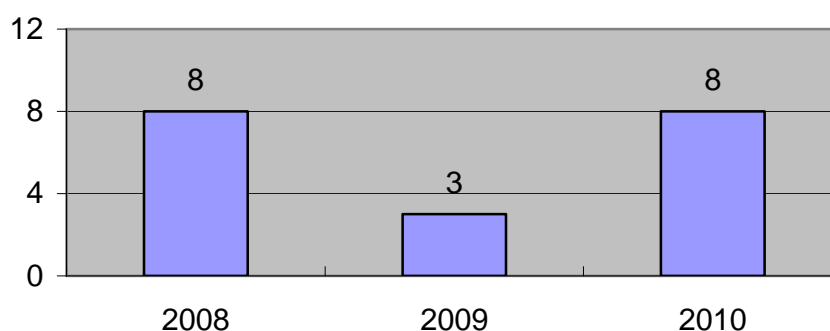
W porównaniu z poprzednimi latami w 2010 r. poprawił się stopień wypełnienia obowiązków w zakresie odnotowywania informacji o odbiorcach danych w systemach informatycznych służących do przetwarzania danych osobowych. Ponad 98 % użytkowanych systemów informatycznych skontrolowanych w 2010 r. umożliwiało odnotowanie ww. informacji w sytuacji, gdy udostępnienie takie miało miejsce.

W 2010 r. poprawiło się również w porównaniu z rokiem 2009, wdrożenie mechanizmów autoryzacji dostępu do danych. W 99 % skontrolowanych w 2010 r. systemów informatycznych istniały odpowiednie mechanizmy uwierzytelnienia użytkowników. Najczęściej stosowaną metodą uwierzytelnienia było nadal logowanie do systemu z wykorzystaniem kont użytkowników (identyfikator oraz hasło). W nielicznych przypadkach do autoryzacji używano kart chipowych powiązanych z numerem PIN. Nadal jednak pomimo tego, że skontrolowane systemy informatyczne dysponowały mechanizmem uwierzytelnienia, zdarzały się przypadki niewłaściwego stosowania ww. mechanizmów. Jednym z uchybień napotkanych w procesie logowania było wykorzystywanie jednego identyfikatora logowania przez więcej niż jedną osobę. Stwierdzono również wykorzystywanie wspólnego hasła logowania przez kilka osób lub też stosowanie nieodpowiednich parametrów haseł do wymaganego poziomu bezpieczeństwa, czy też zmiana haseł rzadziej niż raz na 30 dni.

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 2010 r. kontroli były podmioty, dla których ochrona przetwarzanych danych osobowych jest ważnym zagadnieniem. Do podmiotów tych należą głównie firmy inwestycyjne prowadzące działalność maklerską, 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 roku 2010 do Wojewódzkiego Sądu Administracyjnego oraz Naczelnego Sądu Administracyjnego skierowanych zostało **8 skarg** w związku z przeprowadzonymi kontrolami.



Wykres 36: *Zestawienie porównawcze liczby skarg wniesionych do Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Naczelnego Sądu Administracyjnego w związku z przeprowadzonymi kontrolami w latach 2008-2010.*

W 2010 r. przed sądami administracyjnymi zapadło **5 orzeczeń** dotyczących decyzji wydanych na skutek przeprowadzonych kontroli oraz jedno postanowienie Wojewódzkiego Sądu Administracyjnego w Warszawie dotyczące odmowy udostępnienia informacji publicznej.

Do ważnych orzeczeń Naczelnego Sądu Administracyjnego należał wyrok z dnia 5 stycznia 2010 r.<sup>104</sup>, w którym sąd przychylając się do stanowiska Generalnego Inspektora uznał, że dealer samochodowy ma obowiązek uzyskania zgody na przetwarzanie danych osobowych w celach marketingowych od potencjalnych klientów, tj. osób, które są zainteresowane kupnem samochodu, ale 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 art. 23 ust. 1 pkt 5 ustawy, tzn. jako usprawiedliwiony cel administratora danych.

Ważnym orzeczeniem było postanowienie z dnia 12 maja 2010 r.<sup>105</sup> Wojewódzkiego Sądu Administracyjnego w Warszawie, który uznał skargę na decyzję Generalnego Inspektora Ochrony Danych Osobowych w przedmiocie odmowy udostępnienia informacji publicznej w postaci protokołu

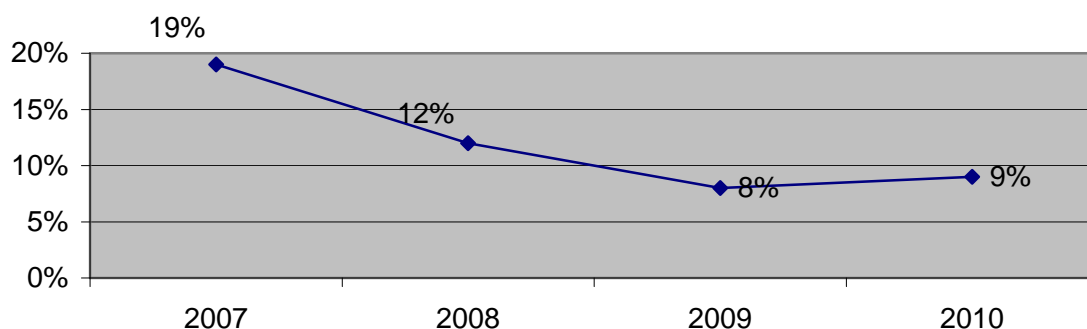
<sup>104</sup> I OSK 399/09

<sup>105</sup> II SA/Wa 652/10

kontroli przeprowadzonej w państwowym przedsiębiorstwie użyteczności publicznej, za niedopuszczalną i podlegającą odrzuceniu. Generalny Inspektor odmawiając skarżącemu udostępnienia informacji publicznej powołał się na tajemnicę przedsiębiorcy, którego żądana informacja dotyczyła.

Na podstawie ustaleń z kontroli przeprowadzonych w 2010 r. należy stwierdzić, że w porównaniu z latami ubiegłymi osoby odpowiedzialne za przetwarzanie danych osobowych wykazały większą świadomość zagrożeń związanych z przetwarzaniem danych osobowych, a tym samym świadomość konieczności zapewnienia odpowiednich środków organizacyjnych i technicznych zapewniających 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. Innym negatywnym zjawiskiem zaobserwowanym w 2010 r. był brak współpracy podmiotu kontrolowanego z inspektorami dokonującymi czynności kontrolnych. Ten brak współpracy przejawiał się w szczególności trudnościami w umówieniu spotkania z osobami reprezentującymi jednostkę kontrolowaną celem okazania imiennych upoważnień i legitymacji służbowych uprawniających do przeprowadzenia kontroli oraz w długim czasie oczekiwania na osoby dysponujące wiedzą o procesie przetwarzania danych osobowych w celu przyjęcia od nich do protokołu ustnych wyjaśnień i na dokumenty mające bezpośredni związek z przedmiotem kontroli. Powyższy stan rzeczy powinien jednak ulec zmianie z chwilą wejścia w życie znowelizowanych przepisów ustawy o ochronie danych osobowych, które przewidują sankcje karne za udaremnianie lub utrudnianie inspektorowi wykonania czynności kontrolnych.

W porównaniu z poprzednimi latami, w 2010 r. daje się już zauważyć niewielki wzrost liczby **skarg**, które wpłynęły do Biura GODO. W roku 2008 wpłynęło 986 skarg, w 2009 – 1049, zaś w 2010 – 1114. Należy podkreślić, że przyczyn wzrostu liczby skarg, które wpłynęły do GODO w analizowanym okresie 2010 r. należy upatrywać przede wszystkim we wzroście świadomości społeczeństwa co do zasad ochrony danych osobowych i jego aktywności w dochodzeniu przysługujących mu praw. Zauważyć jednakże należy, że żądania zawarte w skargach były coraz precyzyjniej formułowane, zaś same podania zawierały mniej braków formalnych, których następstwem byłoby pozostawienie ich bez rozpoznania albo zwrot. Do takiego wniosku prowadzi m.in. analiza zastawienia porównawczego liczby postanowień Generalnego Inspektora Ochrony Danych Osobowych o zwrocie skarg z powodu nieuiszczenia opłaty skarbowej w stosunku do całkowitej liczby skarg.



Wykres 37: *Zestawienie porównawcze liczby postanowień GODO o zwrocie skarg z powodu nieuiszczenia opłaty skarbowej w stosunku do całkowitej liczby skarg w latach 2007–2010.*

Decyzje Generalnego Inspektora Ochrony Danych Osobowych zawierające nakaz, były najczęściej wydawane w związku z niedopełnieniem przez administratorów danych obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych albo nieudostępnieniem danych osobowych żądanych na podstawie art. 29 ust. 2 ustawy o ochronie danych osobowych przez osobę zainteresowaną. Podobnie jak wystąpienia organu dotyczące obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych, decyzje nakazujące jego dopełnienie kierowane były przede wszystkim do banków i innych instytucji finansowych oraz operatorów telekomunikacyjnych. Głównym zaś powodem występowania do administratorów danych z wnioskami z art. 29 ust. 2 ustawy o ochronie danych osobowych, była potrzeba posiadania przez osoby zainteresowane danych osobowych koniecznych do wytoczenia powództwa o ochronę dóbr osobistych.

W sprawach zainicjowanych skargami warte odnotowania były rozstrzygnięcia sądów administracyjnych dotyczące przetwarzania danych osobowych w celach marketingowych. Naczelny Sąd Administracyjny podzielił stanowisko organu stwierdzając, że podmioty prowadzące sprzedaż cudzych produktów i usług w przypadku reklamowania tych produktów i usług nie przetwarzają danych osobowych w celach marketingowych na podstawie art. 23 ust. 1 pkt 5 w związku z art. 23 ust. 4 pkt 1 ustawy o ochronie danych osobowych<sup>106</sup>. W innej zaś sprawie, Wojewódzki Sąd Administracyjny w Warszawie przychylił się do stanowiska organu, że od momentu zalogowania się osoby fizycznej do jej konta na stronie internetowej, na skutek jej spersonifikowania, administrator danych powinien uwzględnić wniesiony przez nią sprzeciw wobec przetwarzania danych osobowych w celach marketingowych, tj. zaprzestać wyświetlania reklam<sup>107</sup>.

Analizując z kolei działalność **opiniotwórczą** Generalnego Inspektora Ochrony Danych Osobowych, można było dostrzec szczególne zaniepokojenie organu tendencją do tworzenia przez

<sup>106</sup> Wyrok NSA z dnia 5 stycznia 2010 r. sygn. akt I OSK 399/09.

<sup>107</sup> Wyrok WSA w Warszawie z dnia 15 czerwca 2010 r. sygn. akt II SA/WA 556/10.

różne podmioty tzw. megabaz danych osobowych, zawierających informacje o milionach osób fizycznych. W 2010 roku GODO opiniował akty prawne, mocą których planowane jest wprowadzenie Systemu Informacji w Ochronie Zdrowia<sup>108</sup> zwanego obecnie Systemem Informacji Medycznej (SIM), Systemu Informacji Oświatowej (SIO)<sup>109</sup>, który ze zbioru o charakterze statystycznym stać się ma zbiorem obejmującym dane osobowe, w tym dane szczególnie chronione dotyczące przedszkolaków, uczniów, studentów, nauczycieli czy Centralnego Rejestru Podmiotów – Krajowej Ewidencji Podatników polegającego na częściowym „zduplikowaniu” i szerszemu udostępnieniu bazy PESEL, celem wykorzystania jej jako numeru referencyjnego także w kontaktach z organami podatkowymi<sup>110</sup>.

Projektowanie megazbiorów zawierających dane osobowe, także szczególnie chronione, jest przedsięwzięciem budzącym wiele wątpliwości organu ds. ochrony danych. Dostęp do takiego zbioru z założenia przysługuje olbrzymiej grupie podmiotów, co naraża zawarte w nich dane osobowe na ryzyko bezprawnej ingerencji, w tym w szczególności ryzyko ich ujawnienia. Istnieje również problem prawidłowego i odpowiedniego do zagrożeń zabezpieczenia zawartych w nich danych osobowych, zwłaszcza, gdy ich przekazywanie odbywa się poprzez sieć publiczną, a także zapewnienia dostępu do danych osobowych wyłącznie tym podmiotom, które – w związku z wykonywaniem swoich ustawowych obowiązków – dysponować nimi muszą.

GODO poinformował projektodawców, że w świetle utrwalonego stanowiska organu do spraw ochrony danych osobowych tworzenie megabazy zawierającej olbrzymią ilość informacji będących danymi osobowymi nie może być swoistą receptą na istniejące niedoskonałości wykorzystywanych w danej dziedzinie systemów informatycznych. Przetwarzanie danych osobowych zgromadzonych w megabazach stanowi bowiem formę ingerencji w prawa i wolności jednostki. Dlatego ingerencja ta musi spełniać kryterium konieczności w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Oznacza to, że ustawodawca nie ma całkowitej swobody w doborze środków służących mu do osiągnięcia zamierzonych celów. Musi uwzględnić, iż „konieczność w demokratycznym państwie prawnym to zastosowanie środków niezbędnych 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<sup>111</sup>. Dlatego Generalny Inspektor Ochrony Danych Osobowych dbał, aby projektodawcy w taki sposób konstruowali proponowane przepisy, aby pozwoliły na respektowanie praw przysługujących osobom, których dane dotyczą.

---

<sup>108</sup> DOLiS-033-338/10

<sup>109</sup> DOLiS-035-414/09 i DOLiS-033-103/10.

<sup>110</sup> DOLiS-033-447/10 – Założenia do projektu ustawy o zmianie ustawy o zasadach ewidencji i identyfikacji podatników i płatników oraz o zmianie niektórych innych ustaw.

<sup>111</sup> Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. w sprawie o sygn. K. 32/2004.



W projektach aktów normatywnych przesyłanych Generalnemu Inspektorowi do zaopiniowania w 2010 r. można też było zaobserwować brak precyzyjnego, wyczerpującego określenia zakresu przetwarzanych danych osobowych w odniesieniu do konkretnej sytuacji. Projektodawcy wychodzili bowiem z założenia, że sformułowania, takie jak np. „w szczególności” czy „między innymi” są wystarczające dla uznania prawidłowości brzmienia przepisu z punktu widzenia zasad ochrony danych osobowych. Tymczasem takie sformułowania nie określają w sposób jednoznaczny zakresu danych osobowych ani podmiotów, które są uprawnione do przetwarzania danych. W konsekwencji pojawił się poważny problem interpretacyjny dla podmiotów stosujących tak ustanowione normy prawa. W takich sytuacjach Generalny Inspektor podkreślał, iż każdorazowo przepis prawa odnoszący się do przetwarzania danych osobowych powinien wprost wskazywać zakres informacji, jakie na jego podstawie mają być przetwarzane oraz podmiot, bądź krąg podmiotów uprawnionych do ich przetwarzania. W przeciwnym razie – przy tak błędnie sformułowanych przepisach prawa – zachodzi ryzyko np. przedkładania przez osoby, których dane dotyczą, czy żądania przez administratorów danych, informacji nieadekwatnych do rzeczywistego celu przetwarzania danych. Analizując tak skonstruowane przepisy, Generalny Inspektor Ochrony Danych Osobowych wielokrotnie wskazywał, że w ten sposób dochodzić będzie do naruszenia jednej z naczelnych zasad wynikających z przepisów o ochronie danych osobowych, a mianowicie zasady adekwatności danych w stosunku do celów ich przetwarzania<sup>112</sup>.

Innym problemem, na jaki Generalny Inspektor wielokrotnie wskazywał analizując projekty aktów prawnych, było rozszerzanie zakresu danych osobowych wskazanego w przepisach aktu prawa o randze ustawy, przepisami aktów wykonawczych, a także brak określenia przez projektodawców terminu przetwarzania danych osobowych lub wskazywania przez nich okresu nieproporcjonalnie długiego. Stosowanie tego rodzaju praktyk uznał za rozwiązanie niedopuszczalne.

Dokonując analizy aktywności opiniodawczej GIODO nasuwa się też wniosek, iż wciąż istnieje wiele regulacji prawnych wymagających zmiany, celem zapewnienia prawidłowego przetwarzania danych osobowych w sektorze publicznym jak i prywatnym. Pilnym zadaniem jest zwiększenie świadomości podmiotów przetwarzających dane osobowe w sieci Internet oraz osób prywatnych korzystających z tego rodzaju udogodnienia. Należy również zauważyć, że administratorzy danych wielokrotnie przetwarzają dane osobowe w zakresie szerszym niż mają do tego prawo, a postępujący rozwój technologiczny prowadzi do niebezpiecznego pogłębiania tego zjawiska. Nagminnym zaniedbaniem ze strony administratorów danych jest przede wszystkim brak wypełniania obowiązku informacyjnego wynikającego z art. 24 i 25 ustawy o ochronie danych osobowych, a także błędne formułowanie treści klauzul zgody na przetwarzanie danych osobowych. Są one bowiem często

---

<sup>112</sup> Art. 26 ustawy o ochronie danych osobowych.

łączone z wypełnianiem obowiązku informacyjnego i/lub z klauzulą zgody na przetwarzanie danych osobowych dla celów przesyłania informacji handlowej (która, zgodnie z przepisami ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną<sup>113</sup> powinna być pozyskiwana mocą odrębnego oświadczenia woli). Niezadowolająca jest również wiedza osób, których dane osobowe są przetwarzane w zbiorach danych, w zakresie praw kontrolnych określonych w rozdziale czwartym ustawy o ochronie danych osobowych, na tym polu często konieczne jest informowanie podmiotów danych o przysługujących im prawach.

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.

Po prawie trzech latach intensywnych prac parlamentarnych znowelizowane zostały przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Na mocy *ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw* wprowadzone zostały nowe regulacje, które obowiązują od dnia 7 marca 2011 r. Umożliwią one skuteczniejsze oddziaływanie organu ds. ochrony danych osobowych na poziom przestrzegania prawa do prywatności i ochrony danych osobowych w Polsce. Doświadczenia wynikające z okresu obowiązywania ustawy o ochronie danych osobowych z jej dotychczasowymi unormowaniami wskazują, iż – ze względu na rzadkie przypadki stosowania i niską skuteczność sankcji zawartych w przepisach karnych tejże ustawy – w pełni zasadnym było wyposażenie Generalnego Inspektora Ochrony Danych Osobowych w możliwość nakładania kar finansowych na podmioty niestosujące się do jego decyzji. Wpłynie to korzystnie zarówno na aktualny poziom przestrzegania regulacji dotyczących ochrony danych osobowych (a co za tym idzie – ogólny stopień ochrony konstytucyjnych praw obywateli), jak i może mieć istotne oddziaływanie prewencyjne w przyszłości.

Jednocześnie zaś – obok upoważnienia do stosowania środków o charakterze dyscyplinująco-penalnym – przedmiotowy projekt ustawy w sposób jednoznaczny sankcjonuje – wykorzystywane już przez organ do spraw ochrony danych osobowych w sposób niesformalizowany – środki służące doskonaleniu ochrony danych osobowych w postaci wystąpienia do podmiotów publicznych i prywatnych oraz żądania zmiany aktualnie obowiązujących przepisów w sprawach dotyczących ochrony danych osobowych. Uregulowanie przez ustawodawcę sposobu podejmowania przez Generalnego Inspektora Ochrony Danych Osobowych powyższych działań i zobligowanie adresatów

---

<sup>113</sup> Dz. U. z 2002 r. Nr 144, poz.1204 z późn. zm.

wystąpien do ustosunkowania się do ich treści w określonym trzydziesto dniowym terminie, pozwoli na szybkie i skuteczne usuwanie istniejących niejasności dotyczących zasad ochrony danych osobowych w poszczególnych dziedzinach życia, a tym samym – intensyfikację tej ochrony.

Natomiast w kwestii charakterystyki **pytań prawnych** kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w 2010 r., w większości dotyczyły one wykładni przepisów regulujących przetwarzanie danych osobowych. Należy bowiem pamiętać, że problematyka ochrony danych osobowych obejmuje niemalże wszelkie sfery życia, a zatem jest uregulowana w przepisach wielu dziedzin prawa. W związku z tym udzielanie odpowiedzi na zadawane pytania w znacznej większości wiązało się z analizą przepisów szczególnych wobec przepisów ustawy o ochronie danych osobowych.

Pytania osób fizycznych zazwyczaj dotyczyły podstaw prawnych do przetwarzania dotyczących ich danych osobowych, adekwatności przetwarzanych danych w stosunku do celu przetwarzania oraz możliwości skontrolowania procesu przetwarzania danych osobowych zarówno administratora danych zarówno na wniosek osoby zainteresowanej, jak i za pośrednictwem organu ds. ochrony danych osobowych. Pytania pochodzące od instytucji bądź podmiotów gospodarczych (od administratorów danych lub administratora bezpieczeństwa informacji), wiązały się z szeroko rozumianą legalnością procesu przetwarzania danych osobowych, w tym podstaw prawnych do przekazywania danych osobowych innym podmiotom w ramach realizacji określonego zadania oraz zabezpieczania danych osobowych. Wiele z nich dotyczyło przetwarzania danych osobowych w związku z prowadzeniem serwisów społecznościowych. Analiza pytań, które w 2010 r. napływały do Biura Generalnego Inspektora Ochrony Danych Osobowych prowadziła do wniosku, że wciąż istnieje wiele regulacji prawnych niejasnych z punktu widzenia ochrony danych osobowych, których interpretacja sprawia trudności osobom, których dane są przetwarzane, jak też i podmiotom, które te dane przetwarzają. Sprawcami nieprawidłowości w stosowaniu zasad przetwarzania danych osobowych były w równym stopniu podmioty prywatne, jak instytucje państwowe i samorządowe.

Z brzmienia art. 19 ustawy o ochronie danych osobowych wynika uprawnienie Generalnego Inspektora Ochrony Danych Osobowych do kierowania do organu powołanego do ścigania przestępstw (w przypadku uzasadnionego podejrzenia popełnienia przestępstwa) **zawiadomienia o podejrzeniu popełnienia przestępstwa**. W 2010 roku Generalny Inspektor 23 razy skorzystał z tego uprawnienia. Najwięcej zawiadomień dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego 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 zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Przeważająca część zawiadomień dotyczyła

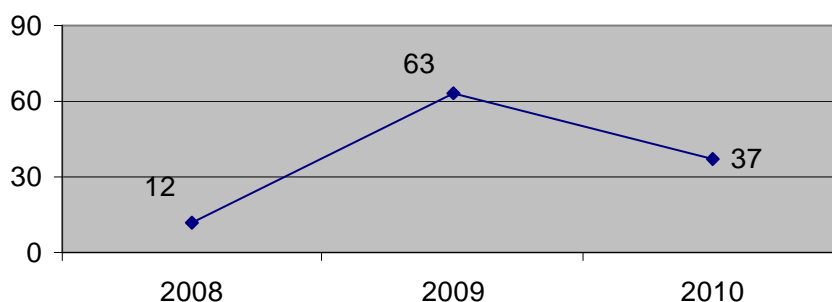
spraw o naruszenie ochrony danych osobowych na stronach internetowych oraz – podobnie jak w latach ubiegłych – w związku z prowadzoną przez dane podmioty działalnością marketingową. Dane pozyskane i przetwarzane za pośrednictwem systemów komputerowych, w sieciach publicznych, czy też z udziałem zaawansowanej technologii - z uwagi na wysoką sprawność przeprowadzanych na nich operacji – coraz częściej stają się przedmiotem nielegalnego procesu przetwarzania danych osobowych. Zdaniem organu ds. ochrony danych osobowych prywatność w Internecie powinna być traktowana w sposób szczególny, gdyż to właśnie w wirtualnej rzeczywistości najłatwiej ją naruszyć, a walka ze skutkami takiego naruszenia bywa niezwykle trudna.

W porównaniu do poprzednich okresów sprawozdawczych niezmiennie maleje liczba spraw, w których organ skierował zawiadomienia o podejrzeniu popełnienia przestępstwa. W roku 2008 było 31 zawiadomień, w 2009 – 27, zaś w 2010 – 23. Wynika to niewątpliwie z podjętych przez Generalnego Inspektora intensywnych działań w zakresie propagowania idei ochrony danych osobowych oraz bardziej stanowcze i skrupulatne egzekwowanie od różnych podmiotów przestrzegania przepisów ustawy o ochronie danych osobowych. Analiza przypadków zawiadomień o podejrzeniu popełnienia przestępstwa prowadzi do wniosku, że 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 argumentując, że czyn, o którym zawiadamiał GODO, nie zawierał znamion czynu zabronionego albo jego społeczna szkodliwość była znikoma. Z analizy treści uzasadnień takich postanowień niezmiennie od wielu lat nasuwa się identyczny wniosek, że organy ścigania wciąż wykazują się bezzasadną oceną przypadków złamania tej ustawy, jako czynów o znikomej społecznej szkodliwości, co zawsze budziło zaniepokojenie organu ds. ochrony danych osobowych. Dlatego znowelizowana ustawa o ochronie danych osobowych, która wejdzie w życie z dniem 7 marca 2011 r. wyposaży organ ds. ochrony danych osobowych w bardziej skuteczne instrumenty egzekwowania prawa.

W 2010 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **37 wniosków o wydanie zgody na przekazanie danych do państw trzecich**, czyli o 17 wniosków mniej niż w 2009 r. W stosunku do poprzedniego okresu sprawozdawczego<sup>114</sup> nastąpił również spadek wydanych przez Generalnego Inspektora decyzji administracyjnych gdyż wydano ich **37**. Spadek liczby rozpatrywanych wniosków był najprawdopodobniej spowodowany tym, że w roku 2009 w większym zakresie rozpatrywano w zasadzie jednolite wnioski składane przez różnych administratorów danych należących do tych samych grup kapitałowych, które ze względów formalnych były rozpatrywane oddzielnie.

---

<sup>114</sup> W 2009 r. Generalny Inspektor wydał 63 decyzje w sprawie wyrażenia zgody na przekazanie danych do państwa trzeciego.



**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 2008-2010.**

W 36 sprawach Generalny Inspektor zezwolił na przekazanie danych, w tym w 11 sprawach częściowo umorzył postępowanie ze względu na przekazanie danych: w ramach Europejskiego Obszaru Gospodarczego, do państw trzecich na podstawie zgody osób, których dane dotyczą w rozumieniu art. 47 ust. 3 pkt 1 ustawy, do krajów lub terytoriów zamorskich państw członkowskich UE, które należy uznać za zapewniające odpowiednią ochronę danych osobowych w rozumieniu art. 25 ust. 1 dyrektywy 95/45/WE (np. Gibraltary, Nowa Kaledonia czy Polinezja Francuska), oraz do odbiorcy, względem którego Generalny Inspektor wydał wcześniej decyzję.

Podobnie jak w roku poprzednim, również w 2010 r. znaczna część wniosków dotyczyła przekazywania danych osobowych pracowników, kandydatów do pracy, klientów lub dostawców w ramach międzynarodowych grup kapitałowych, w celu ujednolicenia procesów zarządzania zasobami ludzkimi, prowadzenia rachunkowości lub zwiększania bezpieczeństwa danych poprzez zastosowanie jednolitych praktyk oraz procedur. Popularne są także transfery w ramach tzw. outsourcingu. Znacząco zmieniła się też liczba państw, do których administratorzy danych zamierzali przekazywać dane.

W omawianym okresie sprawozdawczym wnioskodawcy, w celu zagwarantowania praw i wolności osób, których dane dotyczą, w większości deklarowali zastosowanie standardowych klauzul umownych, aczkolwiek po raz pierwszy pojawiły się też wnioski o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego, w których powołano się na zastosowanie wiążących reguł korporacyjnych.

Podkreślenia wymaga, że nadal do najczęściej pojawiających się błędów w składanych wnioskach o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego należą różnego rodzaju braki formalne, w tym związane z niedopełnieniem obowiązków wynikających z przepisów ustawy z dnia 7 października 1999 r. o języku polskim (Dz. U. 1999 r. Nr 90, poz. 999 z późn. zm.), a także braki w zakresie informacji dotyczących planowanych transferów danych oraz zastosowania odpowiednich środków organizacyjno-technicznych przez importerów danych.

W 2010 roku wśród **zgłoszeń zbiorów danych osobowych do rejestracji** pochodzących od podmiotów publicznych stosunkowo dużą liczbę, w porównaniu z ubiegłymi latami, stanowiły zbiory danych osobowych prowadzone na podstawie ustawy z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz. U. z 2005 r. Nr 14, poz. 114 z późn. zm.). W myśl art. 72 ustawy z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz. U. z 2005 r. Nr 14, poz. 114 z późn. zm.), postępowania w sprawach o naruszenie dyscypliny finansowej prowadzone są przez rzeczników dyscypliny finansów publicznych (postępowanie wyjaśniające), komisje orzekające oraz Główną Komisję Orzekającą (postępowanie odwoławcze). W związku z prowadzeniem wyżej wymienionych postępowań w podmiotach, przy których działają komisje orzekające i rzecznicy dyscypliny finansów publicznych, np. u ministrów i w regionalnych izbach obrachunkowych, tworzone są zbiory danych osobowych. Jednocześnie należy uznać, że zbiory te podlegają obowiązkowi zgłoszenia do rejestracji, gdyż nie zachodzi żadna z przesłanek określonych w art. 43 ustawy o ochronie danych osobowych, zwalniająca administratorów danych z ww. obowiązku. Reasumując, do rejestracji zgłaszane były między innymi: rejestry zawiadomień o naruszeniu dyscypliny finansów publicznych, zbiory danych osób w stosunku do których rzecznik dyscypliny finansów publicznych wystąpił do komisji orzekającej z wnioskiem o ukaranie oraz zbiory danych osób występujących w postępowaniu przed komisją orzekającą.

Ponadto w przypadku podmiotów publicznych w 2010 roku wystąpił znaczny wzrost, w porównaniu do lat poprzednich, liczby zgłoszeń dokonywanych w związku z realizacją przez te podmioty zadań wynikających z ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.). Zgłoszenia te podzielić można na trzy grupy. Pierwsza grupa to zbiory danych prowadzone przez szkoły podstawowe oraz gimnazja w celu realizacji obowiązku wynikającego z rozporządzenia wykonawczego do powyższej ustawy, wydanego przez Ministra Edukacji Narodowej i Sportu w dniu 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. Nr 23, poz. 225 z późn. zm.). Zadaniem tych placówek jest prowadzenie ksiąg ewidencji dzieci i młodzieży podlegających obowiązkowi rocznego przygotowania przedszkolnego i obowiązkowi szkolnemu, zamieszkałych w obwodzie szkoły i gimnazjum. Drugą grupę stanowią zgłaszane przez przedszkola i szkoły podstawowe zbiory danych osób upoważnionych przez rodziców i opiekunów prawnych do odbioru dzieci odpowiednio ze szkoły lub przedszkola. Zaś trzecia grupa to zbiory danych prowadzone w celu ewidencji korespondencji przychodzącej i wychodzącej.

W 2010 roku, podobnie jak w latach poprzednich, odnotowano wzrost w zakresie liczby zgłoszeń zbiorów danych, które utworzone zostały w związku ze stosowaniem przez administratorów danych nowoczesnych technologii. Chodzi tu głównie o wykorzystywanie możliwości Internetu. Zgłoszenia takie dokonywane były głównie przez podmioty prywatne. Jednakże należy zwrócić uwagę na wzrost liczby tego rodzaju zgłoszeń dokonanych przez podmioty publiczne w związku z rozwojem informatyzacji w administracji publicznej. Przykładem mogą być zgłaszane przez te podmioty zbiory danych osób korzystających z możliwości przesłania dokumentów elektronicznych pomiędzy systemami teleinformatycznymi podmiotów publicznych a systemami podmiotów niebędącymi podmiotami publicznymi, tzw. elektroniczne skrzynki podawcze.

Innym przykładem wykorzystania sieci Internet przez podmiot publiczny może być zbiór danych osób korzystających z portalu informacyjnego uruchomionego przez jeden z sądów okręgowych dla stron postępowania. Założenie konta na tym portalu umożliwia stronom (powodowi, pozwanemu, wnioskodawcy, wierzycielowi, dłużnikowi) oraz ich pełnomocnikom, zdalny dostęp do informacji o stanie sprawy, o wyznaczonych rozprawach i wgląd do dokumentów wytworzonych przez sąd.

Kolejnym przykładem zbiorów danych utworzonych na skutek wykorzystywania nowych technologii do realizacji zadań publicznych mogą być zbiory danych tworzone w związku z wprowadzeniem spersonalizowanych elektronicznych kart miejskich. Uprawniają one nie tylko do korzystania z komunikacji miejskiej, ale także umożliwiają korzystanie z innych usług, np. dokonywania opłat za korzystanie z miejsc postojowych w strefach płatnego parkowania. W przypadku takich zbiorów Generalny Inspektor Ochrony Danych Osobowych zwracał uwagę na zbyt szeroki zakres danych osobowych pasażerów przetwarzanych w celu wydania i obsługi spersonalizowanych kart miejskich, w szczególności kwestionował kodowanie na kartach numeru ewidencyjnego PESEL oraz przetwarzanie danych o ruchu pasażerów komunikacji miejskiej (tzw. danych geolokalizacyjnych), jako nieadekwatnych do celu ich przetwarzania.

#### **Część IV. Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych**

Generalny Inspektor Ochrony Danych Osobowych, jako konstytucyjny organ demokratycznego państwa prawa, stoi na straży przestrzegania prawa o ochronie danych osobowych w Polsce. Do jego ustawowych obowiązków należy coroczne składanie Sejmowi sprawozdania ze swej działalności, w którym dokonywana jest analiza spraw dotyczących naruszeń ochrony danych, wyników przeprowadzonych kontroli, wydanych opinii, przedsięwzięć legislacyjnych, orzecznictwa sądów administracyjnych i innych działań ujętych w art. 12 ustawy o ochronie danych osobowych. Na

ich podstawie formułowane są wnioski i wytyczne co do kierunków działań organu na przyszłość. Generalny Inspektor współpracuje ściśle ze wszystkimi organami, które mają wpływ na tworzenie prawa i jego egzekwowanie, a także z podmiotami takimi, jak stowarzyszenia, ośrodki naukowe czy organizacje branżowe zajmujące się ochroną danych osobowych i prawami obywateli oraz ze środkami masowego przekazu. Wszystkie te elementy aktywności GIODO składają się na sumę jego doświadczeń w kwestii usprawnienia pracy organu i zapewnienia skutecznej ochrony prywatności i danych osobowych.

Dane osobowe stanowią podstawę zarządzania przedsiębiorstwami i administracją publiczną. Rolą organu ds. ochrony danych jest znalezienie odpowiedniej **równowagi** między prawnie uzasadnionymi potrzebami przedsiębiorstw i Państwa, wykorzystujących informacje osobowe do wypełniania swojej roli w społeczeństwie oraz między prawem obywateli do tego, aby dotyczące ich dane osobowe wykorzystywane były wyłącznie w ich interesie. Polityka dotycząca ochrony danych osobowych powinna opierać się zarówno na dobrej legislacji i właściwie pojmowanych zadaniach administratorów baz danych, jak i wzroście świadomości obywateli, co do przysługujących im praw. Realizacja tych zamierzeń wymaga wielokierunkowego i wielopłaszczyznowego podejścia w celu wypracowania optymalnej strategii ukierunkowanej na poprawę skuteczności organu, jak i zapewnieniu spójności przepisów krajowych i unijnych dotyczących ochrony danych osobowych. Dyskusja dotycząca zakresu koniecznych zmian już się rozpoczęła, a jednym z pierwszych jej efektów było ogłoszenie 4 listopada 2010 r. komunikatu Komisji Europejskiej pt. „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”, dotyczącego zmiany dyrektywy 95/46/WE w kierunku zwiększenia spójności ram prawnych w zakresie ochrony danych oraz zapewnienia takich rozwiązań instytucjonalnych, aby zapewnić skuteczniejsze egzekwowanie przepisów o ochronie danych osobowych. Ponadto zapowiedziane zostały także działania pozalegislacyjne, mające na celu wzmocnienie ochrony danych osobowych w Unii Europejskiej. GIODO czuwa nad tym, aby proces zmian w prawie o ochronie danych osobowych był jak najbardziej odpowiadający potrzebom wynikającym ze stanu ustawodawstwa polskiego i europejskiego oraz praktyki jego stosowania. Dokłada też starań, aby efekty jego działalności w pełni przeniknęły do świadomości społecznej, przyczyniając się do wzrostu kultury prawnej.

Pierwszym krokiem w kierunku skutecznej realizacji ochrony danych w Polsce powinien stać się przegląd ustawodawstwa pod kątem zarówno spójności przepisów prawa o ochronie danych osobowych, jak i przeanalizowanie ich i – być może – znowelizowanie, w związku z potrzebą dostosowania ich do nowych technologii informacyjno-komunikacyjnych. W szczególności w kwestii zwiększenia świadomości podmiotów przetwarzających dane osobowe w Internecie oraz osób prywatnych korzystających z sieci. Istnieje bowiem wciąż wiele regulacji prawnych wymagających zmiany, celem zapewnienia prawidłowego przetwarzania danych osobowych w sektorze publicznym



jak i prywatnym. Podkreślenia wymaga, że ustawa o ochronie danych osobowych powstała 13 lat temu i odpowiada stanowi techniki z początku lat 90-tych. Nie przewidywała powszechności Internetu, ani istnienia, np. portali społecznościowych. Przed GODO stoi więc zadanie wprowadzenia kolejnych zmian w znowelizowanej w 2010 r. ustawie o ochronie danych osobowych, tak, aby zrealizowane zostały potrzeby i oczekiwania społeczne w tym zakresie, oraz dokonana została implementacja zapowiadanych zmian w przepisach dyrektywy 95/46/WE. Ważnym etapem tych prac będzie określenie grup zagadnień, które wymagają przedyskutowania i przeanalizowania pod kątem ewentualnej zmiany dotyczących ich przepisów. Konferencją „Reforma ochrony prywatności”, która odbyła się w 6 grudnia 2010 r. zainaugurowana już została publiczna dyskusja na ten temat.

Kolejną istotną kwestią, która wymaga uregulowania przez organ ds. ochrony danych osobowych, jest usprawnienie pracy inspektorów GODO poprzez możliwość uzyskiwania przez nich certyfikatów dostępu do informacji niejawnych, co stwarzałoby możliwość kontrolowania służb specjalnych. Z mocy prawa GODO pozbawiony jest dostępu do informacji niejawnych gromadzonych przez służby specjalne. Mamy w tym względzie jedno z najbardziej restrykcyjnych praw w Europie. W innych krajach też są pewne wyłączenia, ale nie jest tak, żeby wyłączono spod kontroli organów ochrony danych osobowych **wszystkie** dane zbierane przez służby specjalne. Zwrócił na to uwagę również Naczelny Sąd Administracyjny stwierdzając, że GODO nie może z góry przyjmować, że wszystko, co służby gromadzą o obywatelach jest tajne, więc nie podlega jego kontroli. Konsekwencje tego wyroku są takie, że GODO ma prawo i obowiązek zajmować się gromadzeniem danych przez służby specjalne tam, gdzie nie są one tajne. Ale można też pójść w innym kierunku i w zapowiadanej kolejnej nowelizacji ustawy o ochronie danych osobowych ustawowo upoważnić inspektorów GODO do przeprowadzania kontroli tych służb przyznając im wspomniane certyfikaty. Pociągnie to za sobą pewne skutki finansowe i organizacyjne. Dla GODO oznacza to konieczność stworzenia odrębnej jednostki organizacyjnej Biura, składającej się z pracowników, którzy mają dostęp do informacji niejawnych i tym samym będą mogli przeprowadzać kontrole w służbach specjalnych.

We wszystkich swoich wystąpieniach Generalny Inspektor Ochrony Danych Osobowych zwraca szczególną uwagę przedstawicieli władz i społeczeństwa na problemy związane z praktyką stosowania prawa o ochronie danych osobowych oraz występujący dualizm przepisów krajowych, co nie sprzyja przejrzystości prawa. Wskazuje na potrzebę pełnej implementacji tych przepisów unijnych, które mogą przyczynić się do sprawniejszego wykonywania ustawowych obowiązków przez inne podmioty, np. organów ścigania – zwłaszcza w odniesieniu do przestępstw dokonywanych z wykorzystaniem nowoczesnych technologii internetowych. Ale z drugiej strony uczula na inne kwestie, jak nieuregulowana ustawowo problematyka **wideonadзору, danych geolokalizacyjnych**, czy zakres **retencji danych telekomunikacyjnych**, który stał się powodem niepokoju wszystkich rzeczników ochrony prywatności. W odniesieniu do **retencji danych** sprawą podstawową jest tu

kwestia interpretacji zapisów dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej. Dyrektywa ta nakłada obowiązek retencji danych teleinformatycznych, która jest trudna do wdrożenia bez łamania konstytucyjnego prawa do prywatności. W chwili obecnej wśród państw członkowskich brak jest harmonii w implementacji dyrektywy. Poszczególne państwa przyjęły rozbieżne reguły w każdym właściwie aspekcie – od czasu przechowywania danych, poprzez zakres i cele retencji, aż po reguły dostępu do zebranych danych. Dla przykładu, Polska na tle innych krajów ma jeden z najdłuższych okresów przechowywania danych – 2 lata i bardzo liberalne zasady dostępu do nich. W opinii Generalnego Inspektora Ochrony Danych Osobowych trzeba zrewidować wdrożenie dyrektywy retencyjnej do polskiego prawa w takim kierunku, że tylko popełnienie najcięższych przestępstw powinno uzasadniać wykorzystanie danych na temat ruchu w sieci przez służby specjalne i doprowadzić do tego, aby we wszystkich krajach unijnych obowiązywały zbliżone przepisy w tej kwestii.

Natomiast główny problem z **monitoringiem wizyjnym** to brak kompleksowej regulacji prawnej w formie ustawy. Istnieją jedynie uregulowania cząstkowe, m.in. o wykorzystaniu monitoringu w więzieniach czy podczas imprez masowych. Brakuje ich tam, gdzie monitoring rozwija się dynamicznie – w sektorze prywatnym. Ustawa o ochronie danych osobowych z wielu względów nie może pełnić takiej funkcji. Po pierwsze jest problem z ustaleniem, w jakich okolicznościach informacje z kamer stanowią dane osobowe, czyli pozwalają na zidentyfikowanie osoby bez nadmiernego wysiłku. Po drugie, są różne technologie monitoringu i nie zawsze dochodzi do rejestracji obrazu, co jeszcze utrudnia ustalenie, na ile mamy do czynienia z przetwarzaniem danych. Wreszcie ustawa nie ma w ogóle zastosowania do osób fizycznych w zakresie, w jakim przetwarzane są dane wyłącznie w celach „osobistych lub domowych”. Podobnie jest z danymi **geolokalizacyjnymi**. Polskie przepisy nie są wystarczająco precyzyjne i umożliwiają różnorodną ich interpretację, która najczęściej idzie drogą wskazywaną przez Policję i służby specjalne. Budzi to niepokój organu ds. ochrony danych. Informacje o tym, co o nas gromadzi Policja i służby specjalne korzystające z GPS, monitoringu wizyjnego, mikrofonów kierunkowych, programów komputerowych kojarzących dane z różnych źródeł, itp. są poza kontrolą Generalnego Inspektora Ochrony Danych Osobowych. Dyskusją na ten temat zainteresowana jest również Rzecznik Praw Obywatelskich. Dlatego konieczny jest przegląd stanu prawnego pod kątem m.in. tych analizowanych zagadnień. Ich uregulowanie to kolejne ważne zadanie stojące przed Generalnym Inspektorem Ochrony Danych Osobowych.

Priorytetem wśród zadań GIODO na 2011 rok będzie także konieczność uregulowania zasad funkcjonowania serwisów społecznościowych, usług typu *cloud computing*, sieci semantycznych, tzw. Internetu przedmiotów, wyszukiwarek i domyślnych ustawień przeglądarek tak, aby chroniły dane osobowe i prawo do prywatności. Ważne jest też, by polskie regulacje o ochronie danych wprowadziły

„prawo do bycia zapomnianym”. W tym miejscu GIODO wskazuje na pilną potrzebę zdefiniowania na nowo pojęcia prawa do prywatności, które w dobie nowoczesnych technologii powinno być ujmowane bardziej dynamicznie, jako pewien proces, zmienny w czasie i przestrzeni oraz zależny od otoczenia społecznego jednostki. I choć w tradycyjnym ujęciu prywatność określa się jako obszar, który jednostka rezerwuje wyłącznie dla siebie, to dyskusja o prywatności w usługach zbudowanym dzięki nowym technologiom powinna pójść w zupełnie innym kierunku. Prywatność jest dwustronnym procesem zakreszania granic, sterowanym zarówno przez jednostkę, jak i przez osoby, z którymi ona wchodzi w relacje. Prywatność podlega nieustannym negocjacjom, której granice przesuwają się zależnie od okoliczności, intencji i oczekiwań uczestników relacji oraz celu, jaki chcą osiągnąć. W związku z tym w rozważaniach nad konkretnymi produktami i usługami IT należy umiejętnie wyważyć - z jednej strony ich cele, przydatność, atrakcyjność dla użytkownika, a z drugiej - zagrożenia dla prawa do prywatności i ochrony danych osobowych, jakie mogą z tego wynikać. Stąd pilna potrzeba nieustannego edukowania społeczeństwa i uświadamiania, aby ta wymiana była zarówno pożyteczna, jak i sprawiedliwa. Opracowanie nowego modelu ochrony prywatności to zadanie wszystkich organów odpowiedzialnych za ochronę danych osobowych w Unii Europejskiej, a także poza jej granicami. Podejmowane w tym obszarze inicjatywy Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności (ICDPPC), która od 32 lat stanowi najważniejsze europejskie forum dla międzynarodowego środowiska ochrony danych, sprawiło, że 10 marca 2010 r. trzynastcie organów odpowiedzialnych za egzekwowanie przepisów regulujących ochronę prywatności utworzyło **Światową Sieć Egzekwowania Przepisów o Ochronie Prywatności (GPEN)**. Podstawowym zadaniem tej międzynarodowej sieci jest podejmowanie działań w celu wzmocnienia ochrony danych i prawa do prywatności w wymiarze globalnym. Polski organ ds. ochrony danych od listopada 2010 r. stał się oficjalnym członkiem GPEN.

To tylko kilka wybranych przykładów problemów, które pojawiły się wraz z rozwojem nowoczesnych technologii. Znalezienie sposobów na ich rozwiązanie będzie należało do najważniejszych zadań Generalnego Inspektora na 2011 r.

Generalny Inspektor Ochrony Danych Osobowych prowadzi szeroko zakrojoną współpracę nie tylko z organami ochrony danych w innych krajach, ale również z tymi państwami, które takiej ochrony nie gwarantują. GIODO wychodzi bowiem z założenia, że ochrona danych osobowych ma charakter niepodzielny, a łamanie zasad ochrony danych osobowych w innych krajach może stanowić zagrożenie dla ich realizacji również w naszym kraju. Stąd tak duże zaangażowanie polskiego organu w działania upowszechniające idee ochrony danych osobowych oraz w opracowywanie optymalnych strategii współpracy z państwami spoza Europejskiego Obszaru Gospodarczego. Przykładem jest wypracowany w porozumieniu z Komisją Europejską program „Safe Harbour” umożliwiający

amerykańskim podmiotom gospodarczym sprostanie wymaganiom dyrektywy 95/46/WE i tym samym prowadzenie wymiany handlowej pomiędzy państwami Unii Europejskiej a Stanami Zjednoczonymi.

Przed Generalnym Inspektorem Ochrony Danych Osobowych stoją także inne zadania. W związku z przygotowaniami do objęcia przez Polskę z dniem 1 lipca 2011 r. Przewodnictwa w Radzie Unii Europejskiej (tzw. Prezydencja), również organ ds. ochrony danych osobowych zobowiązany został do podjęcia pewnych działań w związku z organizacją tego procesu. Przede wszystkim wzmocnił współpracę z organami administracji rządowej, zwłaszcza z Ministerstwem Spraw Wewnętrznych i Administracji, które jest m. in. resortem wiodącym w odniesieniu do Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX). W związku z rozpoczęciem przez Komisję Europejską prac nad przyszłymi ramami ochrony danych osobowych w UE, w posiedzeniach ww. Grupy Roboczej będzie brał udział przedstawiciel Biura GODO, udzielając polskiej delegacji merytorycznego wsparcia.

Podczas Prezydencji Polska stanie się gospodarzem większości unijnych wydarzeń. Kalendarz przygotowań do Prezydencji polskiej w Radzie UE przewiduje aktywny udział Generalnego Inspektora Ochrony Danych Osobowych w spotkaniach na najwyższym szczeblu z przedstawicielami istotnych z punktu widzenia ochrony praw podstawowych resortów i instytucji. Tematyka uzgodnień odnosić się będzie do dziedziny szeroko rozumianej problematyki społeczeństwa informacyjnego, a w szczególności poszanowania prawa do życia prywatnego oraz ochrony danych osobowych. Wśród nich jako jedno z pierwszych działań Prezydencji polskiej będzie aktywne uczestnictwo w pracach nad nowym europejskim aktem legislacyjnym dotyczącym ochrony danych osobowych.

**ZAŁĄCZNIKI:****Załącznik nr 1**

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych  
w roku 2010 o charakterze generalnym do centralnych organów państwa i do innych podmiotów  
z sektora publicznego**

<b>Lp.</b>	<b>Nazwa podmiotu, do którego skierowano wystąpienie</b>	<b>Data wystąpienia/ Sygnatura sprawy</b>	<b>Przedmiot wystąpienia</b>
1.	Ministerstwo Infrastruktury	7.01.2010 DOLiS-035-4/10/555	Wystąpienie o podjęcie działań legislacyjnych mających na celu zmianę obowiązującego wzoru wniosku o wydanie prawa jazdy, stanowiącego załącznik nr 1 do rozporządzenia Ministra Infrastruktury z dnia 21 stycznia 2004 r. w sprawie wydawania uprawnień do kierowania pojazdami (Dz.U. z 2004 r. Nr 24 poz. 215 z późn. zm.), by ten był zgodny z przepisami ustawy o ochronie danych osobowych.
2.	Szkoła Podstawowa Nr 9 im. Orędowników Pokoju w Oświęcimiu	13.01.2010 DOLiS-035-62/10/1459	Wystąpienie o zachowanie szczególnej staranności w procesie zabezpieczenia danych osobowych uczniów, stosownie do przepisów ustawy o ochronie danych osobowych w związku z powziętą przez GIODO informacją, że w dn. 13.11.2009 r. na terenie szkoły przedstawiciel Akademii Szybkiego Czytania „Sokrates” z Krakowa pozyskał za pomocą ulotek i dołączonych do nich kuponów dane osobowe uczniów i ich rodziców.
3.	Wójt Gminy Koło	18.01.2010 440-938/09/1996/10	Wystąpienie o podjęcie odpowiednich działań mających na celu wyeliminowanie w przyszłości praktyk nie znajdujących uzasadnienia w przepisach ustawy o ochronie danych osobowych w związku z upublicznieniem na stronie internetowej Gminy Koło w BIP oświadczeń majątkowych Wójta Gminy Koło, Zastępcy Wójta oraz Skarbnika.
4.	Starosta Chełmski	25.01.2010 DOLiS-440-805/09/3178/10	Wystąpienie o uwzględnienie w działalności Starostwa Powiatowego w Chełmie przepisów ustawy o ochronie danych osobowych, zwłaszcza jej art. 26 ust. 1 pkt 1 stanowiącego o ciążącym na administratorze obowiązku przetwarzania danych zgodnie z prawem.
5.	Dyrektor Naczelny Miejskiego Ośrodka Sportu i Rekreacji w Ostrowcu Świętokrzyskim	25.01.2010 DOLiS-035-137/10/3163	Wystąpienie w związku z informacją, że w Miejskim Ośrodku Sportu i Rekreacji w Ostrowcu Świętokrzyskim stosowana jest praktyka polegająca na umieszczeniu kamer w przebieralni męskiej. Zwrócona została uwaga, iż praktyka powyższa może prowadzić do postawienia zarzutu naruszenia prawa do prywatności.
6.	Minister Spraw Wewnętrznych i Administracji	27.01.2010 DOLiS-440-373/09/3742/10	Wystąpienie o podjęcie działań zapewniających lepszą jakość danych osobowych przetwarzanych w centralnej ewidencji pojazdów, a zwłaszcza ich merytoryczną poprawność, o której stanowi art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych oraz art. 6 ust. 1 lit. d Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dn. 24.10.1995r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995).

7.	Minister Finansów	28.01.2010 DOLiS-072-3/10/3990	Wystąpienie z prośbą o opinię w przedmiocie konieczności przechowywania informacji/danych osobowych o osobie fizycznej, która odstąpiła od podpisania umowy w związku z prowadzonym przez GIODO postępowaniem administracyjnym dotyczącym ewentualnych nieprawidłowości w procesie przetwarzania danych osobowych przez jeden z banków.
8.	Minister Sprawiedliwości Prokurator Generalny RP	1.02.2010 DOLiS-035-183/10/4274	Wystąpienie z prośbą o podjęcie działań mających na celu wyeliminowanie stosowanej przez prokuratury praktyki polegającej na nieuwzględnianiu obowiązujących przepisów ustawy o ochronie danych osobowych, która przejawia się przy merytorycznym rozstrzygnięciu prowadzonych przez te prokuratury postępowań karnych.
9.	Prezes Narodowego Funduszu Zdrowia	1.02.2010 DOLiS-440-964/09/4282/10	Wystąpienie z prośbą o podjęcie stosownych działań celem zapobieżenia udostępnianiu danych osobowych kandydatów na pracowników NIZ w ogłoszeniach o naborze i zatrudnieniu umieszczanych w BIP publikowanym na stronie internetowej NFZ przez okres dłuższy niż jest to niezbędne, stosownie do przepisu art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych.
10.	Minister Infrastruktury	11.02.2010 DOLiS-035-287/10/5937	Wystąpienie z prośbą o rozważenie zmiany rozporządzenia Ministra Transportu z dn. 25.09.2007 r. w sprawie warunków i trybu rejestracji odbiorników radiofonicznych i telewizyjnych (Dz. U. 2007 r. Nr 187, poz. 1342) w toku ewentualnych prac legislacyjnych, poprzez usunięcie klauzuli zgody na przetwarzanie danych osobowych z załączników powyższego rozporządzenia.
11.	Burmistrz Miasta Biłgoraj	11.02.2010 DOLiS-035-286/10/5938	Wystąpienie o wyjaśnienia w związku z pozyskaniem przez GIODO informacji wskazującej, iż dane osobowe dzieci i ich rodziców przekazywane przez placówki oświatowe do Urzędu Miasta Biłgoraj w celu obliczenia wysokości dotacji, wykorzystywane są również do nakłaniania tych rodziców do zmiany przedszkoli.
12.	Minister Infrastruktury	11.02.2010 DOLiS-035-287/10/5937	Wystąpienie z prośbą o rozważenie zmiany rozporządzenia Ministra Transportu z dn. 25.09.2007r. w sprawie warunków i trybu rejestracji odbiorników radiofonicznych i telewizyjnych (Dz U. 2007 r. Nr 187, poz. 1342) w toku ewentualnych prac legislacyjnych, poprzez usunięcie klauzuli zgody na przetwarzanie danych osobowych z załączników do powyższego rozporządzenia.
13.	Burmistrz Miasta Łask	24.02.2010 DOLiS-440-967/09/7922/10	Wystąpienie o podjęcie stosownych działań mających na celu wyeliminowanie nieprawidłowości w związku z uzyskaniem przez GIODO informacji, z której wynika, iż na stronie internetowej Urzędu Miejskiego w Łasku udostępniono dane osoby fizycznej zawarte w uchwale nr VI/45/07 Rady Miejskiej w Łasku z dn. 07.03.2007 r.
14.	Przedszkole Miejskie w Radzynie Podlaskim	5.03.2010 DOLiS-035-25/10/9401/9404	Wystąpienie o zmianę stosowanej praktyki w związku z upublicznieniem na drzwiach zewnętrznych przedszkola, danych osobowych rodziców dzieci uczęszczających do tego przedszkola w zakresie imienia, nazwiska, adresu zamieszkania, ponieważ prowadzi ona do naruszenia zasady ochrony danych osobowych.

15.	Szef Kancelarii Prezydenta RP	24.03.2010 DOLiS-440-983/12603/10	Wystąpienie z prośbą o podjęcie działań w celu dostosowania procesu pozyskiwania danych osobowych dziennikarzy przez Kancelarię Prezydenta RP podczas rejestracji w przeznaczonym dla mediów dziale serwisu prezydent.pl do wymogów ustawy o ochronie danych osobowych.
16.	Minister Spraw Wewnętrznych i Administracji	24.03.2010 DOLiS-035-2114/09/12599/10	Wystąpienie z prośbą o rozważenie możliwości zainicjowania przez MSWiA prac legislacyjnych mających na celu unormowanie w przepisach rangi ustawowej ogólnych zasad dotyczących wideonadzoru.
17.	Prokurator Generalny	1.04.2010 DOLiS-035-800/10/13757	Wystąpienie w celu zasygnalizowania zastrzeżeń do prowadzenia przez podległe Prokuratorowi Generalnemu prokuratury, postępowań przygotowawczych wszczętych na podstawie zawiadomień kierowanych przez GİODO, a polegających na nieuzasadnionym umarzaniu przedmiotowych postępowań lub odmowie ich wszczęcia, co nasuwa wątpliwości odnośnie poprawności interpretacji przepisów ustawy o ochronie danych osobowych, a w konsekwencji prowadzi do lekceważenia praw osób, których dane są przetwarzane.
18.	Dyrektor Zespołu Szkół Muzycznych im. Feliksa Nowowiejskiego w Szczecinie	19.04.2010 DOLiS-035-115/10/16392	Wystąpienie (ponowne) o uwzględnienie przepisów powszechnie obowiązującego prawa i odstąpienie od wprowadzenia w Zespole Szkół elektronicznego systemu kontroli dostępu na teren placówki, który odczytuje/skanuje obraz linii papilarnych nauczycieli, pracowników i uczniów.
19.	Prezes Sądu Rejonowego dla Warszawy Mokotowa	25.05.2010 DOLiS-440-94/09/21542/10	Wystąpienie z prośbą o podjęcie działań mających na celu zapobieżenie praktyce udostępniania przez komornika sądowego danych osobowych związanych z osobą dłużnika na rzecz osób nieupoważnionych jako niezgodnej z przepisami ustawy o ochronie danych osobowych.
20.	Minister Gospodarki	31.05.2010 DOLiS-035-1332/10/22227	Wystąpienie z prośbą o dostosowanie procesu przetwarzania danych osobowych do zasad wynikających z przepisów ustawy o ochronie danych osobowych, w związku z informacjami w odniesieniu do zakresu danych osobowych pozyskiwanych na potrzeby przeprowadzenia konkursu na funkcję dyrektora jednostki badawczo-rozwojowej o nazwie Instytut Mechaniki Precyzyjnej w Warszawie.
21.	Areszt Śledczy Warszawa-Mokotów	11.06.2010 DOLiS-440-241/10/23761	Wystąpienie o zmianę stosowanej praktyki w związku z udostępnianiem na drzwiach cel znajdujących się w oddziale szpitalnym Aresztu, danych osobowych więźniów tam przebywających, w zakresie informacji o terminach planowanych wobec nich zabiegów oraz dietach.
22.	Wójt Gminy Dobryszyce	14.06.2010 DOLiS-440-164/10/24013	Wystąpienie o zmianę praktyki i dostosowanie jej do obowiązujących przepisów prawa, w związku z załączaniem do pism z prowadzonego postępowania administracyjnego przez Wójta Gminy Dobryszyce wykazu zawierającego dane osobowe stron postępowania.
23.	Burmistrz Miasta Giżycko	15.06.2010 DOLiS-440-138/10/24223	Wystąpienie o przedsięwzięcie stosownych działań zapewniających pełne poszanowanie przepisów ustawy o ochronie danych osobowych w związku z realizowanymi przez organy gminy obowiązkami określonymi w ustawie z dn. 6.09.2001 r. o dostępie do informacji publicznej.

24.	Minister Spraw Wewnętrznych i Administracji	25.06.2010 DOLiS-440-20/10/25634	Wystąpienie z prośbą o rozważenie zasadności podjęcia działań legislacyjnych mających na celu nowelizację przepisów regulujących przetwarzanie danych osobowych w Krajowym Systemie Informacji Policji (KSIP), poprzez wprowadzenie do nich regulacji precyzyjnie określających okresy, w których Policja może przetwarzać w KSIP pozyskane dane osobowe.
25.	Komendant Straży Miejskiej w Zabrzu	01.07.2010 DOLiS-440-93/10/26459,26465	Wystąpienie o dostosowanie procesu przetwarzania przez Straż Miejską w Zabrzu danych osobowych gromadzonych poprzez system monitoringu wizyjnego miasta Zabrze, w związku z zawartym z Prezydentem Miasta porozumieniem, co do wymogów ustawy o ochronie danych osobowych – poprzez jednoznaczne wskazanie w treści ww. umowy zakresu danych osobowych powierzonych na jej mocy do przetwarzania przez Komendanta Straży Miejskiej na rzecz Prezydenta Miasta.
26.	Dyrektor Radomskiego Szpitala Specjalistycznego im. dr T. Chałubińskiego	12.07.2010r. DOLiS-440-567/09/27919/10	Wystąpienie o zmianę praktyki prowadzącej do naruszenia przepisów ustawy o ochronie danych osobowych w związku z udostępnieniem przez Szpital osobom nieupoważnionym danych osobowych pracowników.
27.	Minister Edukacji Narodowej	23.07.2010 DIS-K-421/56/10	Podjęcie działań mających na celu zapewnienie, aby placówki oświatowe prowadziły dzienniki zgodnie z przepisami o ochronie danych osobowych.
28.	Prezes Sądu Rejonowego w Opolu	27.07.2010 DOLiS-440-401/10/29849	Wystąpienie o rozważenie zasadności podjęcia stosownych działań mających na celu zbadanie prawidłowości działań egzekucyjnych podejmowanych przez komornika sądowego w związku z pozyskaniem przez GODO informacji o podjęciu przez niego działania niezgodnego z przepisami ustawy o ochronie danych osobowych.
29.	Minister Finansów	3.08.2010 DOLiS-035-1858/10/30789	Wystąpienie z prośbą o podjęcie prac legislacyjnych mających na celu zawężenie zakresu publikacji danych określonych w art. 76g ust. 1 ustawy z dn. 29.09.1994 r. o rachunkowości (Dz. U. z 2009 r. Nr 152, poz. 1223).
30.	Przewodniczący Komisji Nadzoru Finansowego	16.08.2010 DOLiS-074-4/10/32310	Wystąpienie o rozważenie podjęcia stosownych czynności wynikających z ustawy z dn. 29.08.1997r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 1119 z późn. zm), celem zbadania skali zjawiska i wyeliminowania ew. nieprawidłowości w związku z docierającymi do GODO sygnałami dot. praktyki banków w zakresie prowadzenia akcji marketingowych, polegających na przysyłaniu swoim klientom spersonalizowanych, nieaktywnych kart kredytowych.
31.	Prezes Agencji Rynku Rolnego	26.08.2010 DOLiS-035-2059/10/33730	Wystąpienie o dostosowanie procesu przetwarzania danych osobowych do zasad wynikających z przepisów ustawy o ochronie danych osobowych w związku z pozyskaniem przez GODO informacji w odniesieniu do zakresu danych osobowych pozyskiwanych na potrzeby przeprowadzania konkursu na stanowisko specjalisty/starszego specjalisty.
32.	Minister Edukacji Narodowej Minister Spraw Wewnętrznych i Administracji	25.08.2010 DOLiS-035-2099/10/34028, DOLiS-035-2100/10/34034	Wystąpienia o rozważenie możliwości zainicjowania przez Ministerstwo Edukacji Narodowej prac legislacyjnych, mających na celu unormowanie w przepisach rangi ustawowej zasad pozyskiwania oraz określenie zakresu danych osobowych



			przetwarzanych przy rekrutacji do publicznych szkół i przedszkoli.
33.	Minister Spraw Wewnętrznych i Administracji	01.09.2010 DOLiS-440-696/10/34865	Wystąpienie o podjęcie działań mających na celu określenie ustawowych kryteriów weryfikacji danych osobowych zawartych w zasobach Krajowego Systemu Informacyjnego Policji (KSIP) w związku z kierowanymi do GIODO skargami na przetwarzanie danych osobowych w KSIP.
34.	Komendant Główny Policji	22.09.2010 DOLiS-440-696/10/37853	Wystąpienie sygnalizujące konieczność rozważenia zasadności podjęcia działań legislacyjnych, mających na celu nowelizację przepisów regulujących przetwarzanie przez Policję danych osobowych w KSIP, poprzez wprowadzenie do nich regulacji precyzyjnie określających okresy, w których Policja może przetwarzać w KSIP pozyskane dane osobowe.
35.	Dyrektor Powiatowego Urzędu Pracy w Bydgoszczy	9.10.2010 DOLiS-035-2809/10/44465	Wystąpienie o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych do wymogów określonych w ustawie o ochronie danych osobowych w związku z powzięciem przez GIODO informacji o sposobie przetwarzania danych osobowych zawartych w ankietach zgłoszeniowych wypełnianych przez bez-robotnych wraz z wnioskiem o skierowanie na szkolenie w trybie indywidualnym przez Centrum Aktywizacji Zawodowej w Powiatowym Urzędzie Pracy w Bydgoszczy.
36.	Minister Zdrowia	11.10.2010 DIS-K-421/127/10	Podjęcie działań mających na celu zalegalizowanie przetwarzania danych osobowych w Krajowym Rejestrze Nowotworów oraz w wojewódzkich rejestrach nowotworów.
37.	Minister Finansów	11.10.2010 DIS-K-421/97/10, DIS-K-421/100/10, DIS-K-421/102/10, DIS-K-421/103/10, DIS-K-421/117/10, DIS-K-421/119/10, DIS-K-421/120/10, DIS-K-421/122/10, DIS-K-421/124/10, DIS-K-421/125/10	Podjęcie działań zmierzających do dostosowania systemu informatycznego funkcjonującego w urzędach kontroli skarbowej, do wymogów określonych w § 7 ust. 1 pkt 1 i pkt 2 oraz w § 7 ust. 3 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
38.	Minister Zdrowia	14.10.2010 DIS-K-421/115/10	Zwrócenie uwagi na praktykę stosowaną przez podmioty świadczące usługi optyczne (prowadzące salony optyczne) przy przetwarzaniu danych osobowych.
39.	Powiatowy Inspektor Nadzoru Budowlanego w Kraśniku	01.12.2010 DOLiS-440-977/09/47633/10	Wystąpienie o podjęcie stosownych działań celem wyeliminowania wypadków udostępniania danych osobowych utrwalonych w aktach postępowań administracyjnych prowadzonych przez PINB w Kraśniku, w sytuacji braku określonych przepisami ustawy o ochronie danych osobowych podstaw prawnych dla takiego udostępnienia.

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych  
w roku 2010 do podmiotów prywatnych**

Lp.	Nazwa podmiotu, do którego skierowano wystąpienie	Data wystąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	ITI Neovision Sp. z o.o.	05.01.2010 DOLiS-035-1/10/252	Wystąpienie o zmianę formularza zamieszczonego na stronie internetowej <a href="http://n.pl/nskleo/promocja_full.html">http://n.pl/nskleo/promocja_full.html</a> służącego do dokonania zamówienia usługi i sprzętu w sklepie internetowym celem dostosowania do przepisów ustawy o ochronie danych osobowych.
2.	Zarząd Wspólnoty Mieszkaniowej „Stryjeńskich 6”	08.01.2010 DOLiS-440-72/09/864/10	Wystąpienie o przestrzeganie przepisów ustawy o ochronie danych osobowych w związku z faktem zamieszczenia przez zarząd Wspólnoty na klatkach schodowych, danych osobowych jej członków.
3.	Prezes Zarządu Zakładu Przewozów i Spedycji SPEDOKS” Sp. z o.o.	19.01.2010 DOLiS-440-262/09/ 2327/10	Wystąpienie z prośbą o dołożenie w trakcie udostępniania danych osobowych szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w związku z uzyskaniem przez GODO informacji o udostępnianiu przez Zakład danych osobowych pracowników na rzecz Międzyzakładowej Organizacji Związkowej NSZZ „SOLIDARNOŚĆ” Koksowni „Przyjaźń”.
4.	Prezes Zarządu Polkomtel S.A.	21.01.2010 DOLiS-440- 939/09/2671/10	Wystąpienie o podjęcie stosownych działań celem wyeliminowania nieprawidłowości, w związku z uzyskaniem przez GODO informacji, iż Polkomtel S.A. przetwarzał dane osobowe w celach marketingowych, pomimo wniesienia sprzeciwu w tym zakresie.
5.	Prezes Zarządu Banku Pekao S.A.	25.01.2010 DOLiS-440- 193/09/3177/10	Wystąpienie z wnioskiem o wszczęcie stosownego postępowania dyscyplinującego wobec osoby, która swoim zachowaniem doprowadziła do powstania uchybień w procesie przetwarzania przez Bank danych osobowych Pani M.G.
6.	Prezes Zarządu PGE Zakład Energetyczny Białystok S.A.	26.01.2010 DOLiS-440- 793/09/3587/10	Wystąpienie o zastosowanie odpowiednich środków technicznych i organizacyjnych, które zapewnią odpowiednią ochronę przetwarzanych danych osobowych, w związku z uzyskaniem przez GODO informacji, iż dane osobowe przetwarzane przez PGE Zakład Energetyczny BIAŁYSTOK S.A. nie są należycie chronione przed dostępem osób nieupoważnionych.
7.	Kierownik Programu „Psychologiczne przyczyny i następstwa wypadków drogowych” TRAKT Interdyscyplinarne Centrum Genetyki Zachowania Uniwersytet Warszawski	11.02.2010 DOLiS-035-285/10/5903	Wystąpienie o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych osobowych do wymogów określonych w ustawie o ochronie danych osobowych, w związku z powzięciem przez GODO informacji o przetwarzaniu danych osobowych osób poszkodowanych w wypadkach drogowych.
8.	Prezes Zarządu Gold Finance Sp. z o.o.	09.03.2010 DOLiS-440- 880/08/9888/10	Wystąpienie o podjęcie działań mających na celu dostosowanie procesu przetwarzania przez Spółkę danych osobowych gromadzonych przy pomocy elektronicznego formularza umożliwiającego kontakt z doradcą dostępnego za pośrednictwem

			strony internetowej <a href="http://www.bankier.pl/cf/goldfinance">www.bankier.pl/cf/goldfinance</a>
9.	Prezes Zarządu Nordea Powszechne Towarzystwo Emerytalne S.A.	09.03.2010 DOLiS-440-422/09 DOLiS-440-428/09/ 9913/10	Wystąpienie o uwzględnienie w działalności Nordea Otwartego Funduszu Emerytalnego zasad wynikających z ustawy o ochronie danych osobowych w odniesieniu do przetwarzania danych osobowych w związku z prowadzoną przez Fundusz działalnością akwizycyjną.
10.	Prezes Zarządu Polskiego Górnictwa Naftowego i Gazownictwa S.A.	10.03.2010 DOLiS-440- 269/09/10152/10	Wystąpienie o podjęcie działań w celu dostosowania treści stosowanych przez PGNiG wzorców formularzy „Umowy kompleksowej dostarczania paliwa gazowego” służących do aktualizacji umów sprzedaży paliwa zawartych przed 1 lipca 2007 r. oraz stosowanych w procesie obsługi klientów formularzy „Wniosku o zawarcie umowy o przyłączenie do sieci gazowej” oraz „Oświadczenia dotyczącego tytułu prawnego do korzystania z lokalu/obiektu/nieruchomości...” do wymogów ustawy o ochronie danych osobowych.
11.	Kierownik Filii Centrum Likwidacji Szkód PZU S.A. w Warszawie	11.03.2010 DOLiS-035-10/10/10425	Wystąpienie z prośbą o zastosowanie odpowiednich środków technicznych i organizacyjnych, w związku ze zgłaszaniem szkód komunikacyjnych przez klientów.
12.	KOKSZTYS Kancelaria Prawa Gospodarczego Sp. k.	11.03.2010 DOLiS-035-09/10/10423	Wystąpienie o uwzględnienie zasad ochrony danych osobowych w działalności Spółki i zaprzestanie udostępniania danych osobowych osobom nieupoważnionym.
13.	Kierownik Administracji Osiedla Jana III Sobieskiego Poznańskiej Spółdzielni Mieszkaniowej	22.03.2010 DOLiS-035-92/10/11856	Wystąpienie, w nawiązaniu do materiałów prasowych „Śsiedzkie oko obserwuje” oraz „Przedłużenie oka”, które ukazały się w Głosie Wielkopolski w dn. 17.02.2010 r. dotyczących umieszczenia na osiedlu kamer, celem zwrócenia uwagi, iż naruszane może być konstytucyjne prawo do prywatności.
14.	Prezes Małej Spółdzielni Mieszkaniowej „Eliza” we Wrocławiu	16.04.2010 DOLiS-035- 2316/09/15967	Wystąpienie w sprawie odstąpienia od praktyki umieszczania przez Spółdzielnię na tablicy informacyjnej listy jej członków.
15.	Prezes Spółdzielczej Kasy Oszczędnościowo Kredytowej im. F. Stefczyka	19.04.2010 DOLiS-440- 734/09/16294/10	Wystąpienie o przedsięwzięcie stosownych działań zapewniających niezwłoczne respektowanie przez SKOK im. F. Stefczyka złożonych przez jej klientów oświadczeń o sprzeciwie wobec przetwarzania ich danych osobowych dla realizowanych przez SKOK celów marketingowych.
16.	Prezes Zarządu Niepublicznego Zakładu Opieki Zdrowotnej MEDICUS Sp. z o.o. z Nakła nad Notecią	21.04.2010 DOLiS-035- 948/10/16762	Wystąpienie w sprawie zastosowania odpowiednich środków technicznych i organizacyjnych przy rejestracji pacjentów.
17.	Prezes Zarządu Wydawnictwa C.H. Beck Sp. z o.o.	24.05.2010 DOLiS-440- 473/09/21247/10	Wystąpienie o podjęcie stosownych działań mających na celu wyeliminowanie nieprawidłowości w związku z przetwarzaniem danych osobowe w celach marketingowych, pomimo wniesienia sprzeciwu w tym zakresie.
18.	Pierwszy Wiceprezes Zarządu Banku PEKAO S.A.	27.05.2010 DOLiS-440-23/10/21879	Wystąpienie o respektowanie przepisów prawa, w związku z nieprawidłowościami w realizacji obowiązku informacyjnego, wynikającego z art. 33 ustawy o ochronie danych osobowych.
19.	Prezes Zarządu Klubu Piłkarskiego Legia Warszawa S.S.A.	23.06.2010 DOLiS-440-86/10/25251	Wystąpienie w sprawie dostosowania formularza karty kibica do wymogów określonych w ustawie o ochronie danych osobowych.
20.	Prezes Zarządu Castorama Polska Sp. z o.o.	07.07.2010 DOLiS-035-	Wystąpienie z prośbą marketingowych zastosowanie odpowiednich środków technicznych

		1613/10/27333	i organizacyjnych, w związku z pozyskiwaniem danych osobowych od klientów w procesie wystawiania faktur.
21.	Prezes Zarządu World Class Health Academy Polska Sp. z o.o.	11.08.2010 DOLiS-035-1956/10/31825	Wystąpienie o dostosowanie formularza „Zgłoszenie uczestnictwa” do zasad wynikających z przepisów ustawy o ochronie danych osobowych w zakresie obowiązku informacyjnego.
22.	Prezes Zarządu Spółdzielni Mieszkaniowej „Batory – Wschód” w Warszawie	14.09.2010 DOLiS-440-472/10/36710	Wystąpienie o przestrzeganie przepisów ustawy o ochronie danych osobowych, w związku z uzyskaniem przez GIODO informacji, iż Spółdzielnia wywiesiła w miejscu powszechnie dostępnym wykaz zawierający informacje o numerach lokali, których lokatorzy zalegają z należnościami z tytułu opłat eksploatacyjnych.
23.	Prezes Zarządu UPC Polska Sp. z o.o.	29.09.2010 DOLiS-440-561/10/38500	Wystąpienie o przedsięwzięcie stosownych działań zapewniających niezwłoczne respektowanie złożonych Spółce przez jej klientów oświadczeń o sprzeciwie wobec przetwarzania ich danych osobowych w celach marketingowych.
24.	Hotel Czarny Potok w Zakopanem	02.11.2010 DOLiS-035-2709/10/43197	Wystąpienie o podjęcie działań prowadzących do zapewnienia zgodności procesu przetwarzania danych osobowych do wymogów określonych przepisami ustawy o ochronie danych osobowych oraz w ustawie z dn. 10.04.1974 r. o ewidencji ludności i dowodach osobistych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), w związku ze stosowaną w Hotelu praktyką zatrzymywania dowodów osobistych gości przez personel.
25.	Prezes Zarządu Deutsche Bank PBC S.A.	02.11.2010 DOLiS-440-596/10/43256	Wystąpienie w sprawie respektowanie przepisów ustawy o ochronie danych osobowych, w związku z uzyskaniem przez GIODO informacji, iż Bank nie wypełnił obowiązku informacyjnego wynikającego z art. 33 ustawy w przewidzianym w tym przepisie zakresie i terminie.
26.	Prezes Zarządu Dolnośląskiej Organizacji Turystycznej	20.12.2010 DOLiS-440-548/50328	Wystąpienie o dostosowanie procesu przetwarzania danych osobowych do wymogów ustawy o ochronie danych osobowych, w związku ze skargą dot. działania w przedmiocie przetwarzania danych osobowych zgromadzonych na komputerze służbowym udostępnionym firmie serwisowej.

## Wykaz kontroli przeprowadzonych w 2010 r.

L.p.	Data / Sygnatura kontroli	Nazwa i miejsce podmiotu kontrolowanego	Inicjatywa kontroli	Rozstrzygnięcie oraz/lub data i sygnatura decyzji
1.	13-15.01.2010 DIS-K-421/1/10	Wyższa Szkoła Ekologii i Zarządzania w Warszawie, Warszawa, ul. Wawelska 14	z urzędu	nie stwierdzono uchybień
2.	13-15.01.2010 18-19.01.2010 DIS-K-421/2/10	Szkoła Główna Gospodarstwa Wiejskiego w Warszawie, Warszawa, ul. Nowoursynowska 166	z urzędu	nie stwierdzono uchybień
3.	13-15.01.2010 DIS-K-421/3/10	Wyższa Szkoła Turystyki i Rekreacji im. M. Orłowicza, Warszawa, ul. Marymoncka 34	z urzędu	17.05.2010 decyzja DIS/DEC-587/20305/10
4.	13-15.01.2010 19.01.2010 DIS-K-421/4/10	Szkoła Wyższa Psychologii Społecznej, Warszawa, ul. Chodakowska 19/31	z urzędu	27.05.2010 decyzja DIS/DEC-655/21899/10
5.	18-20.01.2010 DIS-K-421/5/10	Wyższa Szkoła Pedagogiczna Związku Nauczycielstwa Polskiego, Warszawa, ul. Smulikowskiego 6/8	z urzędu	2010-04-27, decyzja DIS/DEC-512/17644/10
6.	18-20.01.2010 DIS-K-421/6/10	Burmistrz Miasta Halinów - Urząd Miejski w Halinowie, Halinów, ul. Spółdzielcza 1	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
7.	19-21.01.2010 DIS-K-421/7/10	Polski Związek Felinologiczny, Warszawa, ul. Potocka 116/36	DOLiS	przywrócono stan zgodny z prawem
8.	20-22.01.2010 DIS-K-421/8/10	Hays Poland Sp. z o. o., Warszawa, ul. Złota 59	DOLiS	27.04.2010 decyzja DIS/DEC-514/17649/10
9.	23.01.2010 DIS-K-421/15/10	Urząd Celny I w Warszawie, Warszawa, ul. 17 Stycznia 49	z urzędu	23.07.2010 decyzja DIS/DEC-961/29613/10
10.	25-28.01.2010 DIS-K-421/9/10	Duda - Watin S.A. Poznań, ul. Ptasia 4	DRZDO	nie stwierdzono uchybień
11.	25-28.01.2010 DIS-K-421/13/10	Prezydent Miasta Kalisza, Kalisz, ul. Główny Rynek 20	DRZDO	14.04.2010 decyzja DIS/DEC-423/15625/10
12.	25-28.01.2010 DIS-K-421/14/10	Zespół Szkół w Szamocinie, Szamocin, ul. 19 Stycznia 29	Prokuratura Rejonowa w Środzie Wlkp.	nie stwierdzono uchybień
13.	25-29.01.2010 DIS-K-421/11/10	Alicja Kaszuba prowadząca działalność gospodarczą pod nazwą „Salon Gier ALA”, Kraków, ul. Strzelców 23/21	DOLiS	27.05.2010 decyzja DIS/DEC-651/21887/10
14.	25-29.01.2010 DIS-K-421/10/10	Sky Club Sp. z o. o. Kraków, ul. Dukatów 10	DOLiS	nie stwierdzono uchybień
15.	26-29.01.2010 DIS-K-421/12/10	Przedsiębiorstwo Handlowo - Usługowe „HETMAN” Sp. z o. o., Katowice, Al. W. Korfańskiego 51/9a	DOLiS	18.03.2010 zawiadomienie o przestępstwie
16.	03-05.02.2010 DIS-K-421/16/10	Izba Celna w Warszawie, Warszawa, ul. Erazma Ciołka 14 A	DOLiS	16.06.2010 decyzja DIS/DEC-727/24348/10
17.	08-12.02.2010 DIS-K-421/17/10	Uniwersytet Warszawski, Warszawa, ul. Krakowskie Przedmieście 26/28	z urzędu	nie stwierdzono uchybień
18.	08-12.02.2010 DIS-K-421/18/10	Warszawski Uniwersytet Medyczny, Warszawa, ul. Żwirki i Wigury 61	z urzędu	27.05.2010 decyzja DIS/DEC-654/21894/10
19.	08-12.02.2010 DIS-K-421/19/10	Wojskowa Akademia Techniczna im. J. Dąbrowskiego, Warszawa, ul. Gen. Sylwestra Kaliskiego 2	z urzędu	27.05.2010 decyzja DIS/DEC-653/21892/10
20.	08-12.02.2010 DIS-K-421/20/10	Akademia Wychowania Fizycznego im. Józefa Piłsudskiego, Warszawa,	z urzędu	29.06.2010 decyzja DIS/DEC-831/26029/10

		ul. Marymoncka 34		
21.	15-19.02.2010 DIS-K-421/21/10	Szkoła Główna Handlowa w Warszawie, Warszawa, Al. Niepodległości 162	z urzędu	01.07.2010 decyzja DIS/DEC-856/26446/10
22.	15-19.02.2010 DIS-K-421/22/10	Akademia Teatralna im. Aleksandra Zelwerowicza, w Warszawie, ul. Miodowa 22/24	z urzędu	14.05.2010 decyzja DIS/DEC-585/20169/10
23.	17-19 i 22.02.2010 DIS-K-421/23/10	Dom Maklerski Banku Ochrony Środowiska S.A., Warszawa, ul. Marszałkowska 78/80	z urzędu	nie stwierdzono uchybień
24.	17-19.02.2010 DIS-K-421/24/10	Wyższa Szkoła Stosunków Międzynarodowych i Amerykanistyki, Warszawa, ul. Rozłogi 10	z urzędu	23.07.2010 decyzja DIS/DEC-960/29609/10
25.	22-26.02.2010 DIS-K-421/25/10	Dom Maklerski TMS Brokers S.A., Warszawa, Al. Jerozolimskie 123 A	z urzędu	27.05.2010 decyzja DIS/DEC-513/17646/10
26.	22-26.02.2010 DIS-K-421/26/10	Dom Maklerski Banku Handlowego S.A. w Warszawie, ul. Chałbińskiego 8	z urzędu	nie stwierdzono uchybień
27.	22-26.02.2010 DIS-K-421/27/10	Alior Bank S.A., Warszawa, Al. Jerozolimskie 94	z urzędu	nie stwierdzono uchybień
28.	22-26.02.2010 DIS-K-421/28/10	Bank Gospodarki Żywnościowej S.A., Warszawa, ul. Kasprzaka 10/16	z urzędu	01.07.2010 decyzja DIS/DEC-857/26450/10
29.	22-26.02.2010 DIS-K-421/29/10	Akademia Sztuk Pięknych w Warszawie, Warszawa, ul. Krakowskie Przedmieście 5	z urzędu	27.05.2010 decyzja DIS/DEC-652/21890/10
30.	23-26.02.2010 DIS-K-421/30/10	Wyższa Szkoła Handlu i Prawa im. Ryszarda Łazarskiego, Warszawa, ul. Świeradowska 43	z urzędu	30.06.2010 decyzja DIS/DEC-840/26161/10
31.	02-05.03.2010 DIS-K-421/31/10	Wyższa Szkoła Społeczno - Ekonomiczna w Warszawie, Warszawa, ul. Kasprzaka 29/31	z urzędu	10.05.2010 decyzja DIS/DEC-560/19221/10
32.	03-05.03.2010 DIS-K-421/32/10	Andrzej Kollwitz prowadzący działalność gospodarczą pod nazwą „Andrzej Kollwitz LENDER”, Warszawa, ul. Targowa 66 paw. 31	DOLiS	29.07.2010 decyzja DIS/DEC-978/30221/10
33.	08-11.03.2010 DIS-K-421/36/10	Fundacja Kupfranki.org , Poznań, ul. Rubież 46 lok. C4/66	DOLiS	brak przetwarzania danych osobowych
34.	08-12.03.2010 DIS-K-421/33/10	Wyższa Szkoła Przedsiębiorczości i Administracji w Lublinie, Lublin, ul. Bursaki 12	z urzędu	10.06.2010 decyzja DIS/DEC-703/23707/10
35.	08-12.03.2010 DIS-K-421/34/10	Burmistrz Miasta Złotowa – Urząd Miasta Złotowa, Złotów, Aleja Piasta 1	z urzędu	nie stwierdzono uchybień
36.	08-12.03.2010 DIS-K-421/35/10	Wyższa Szkoła Informatyki w Łodzi, Łódź, ul. Rzgowska 17 A	z urzędu	11.06.2010 decyzja DIS/DEC-706/23841/10
37.	12 i 15-18.03.2010 DIS-K-421/37/10	Collegium Civitas, Warszawa, Plac Defilad 1	z urzędu	08.06.2010 decyzja DIS/DEC-692/23433/10
38.	15-19.03.2010 DIS-K-421/38/10	Zarząd Transportu Zbiorowego w Rybniku, Rybnik, ul. Budowlanych 6	w związku z kontrolą DIS-K- 421/154/09	03.09.2010 decyzja DIS/DEC- 1053/35065,35070/10
39.	15-19.03.2010 DIS-K-421/39/10	Miejski Ośrodek Sportu i Rekreacji, Rybnik, ul. Gliwicka 72	w związku z kontrolą DIS-K- 421/154/09	nie stwierdzono uchybień
40.	15-19.03.2010 DIS-K-421/40/10	Wyższa Szkoła Umiejętności im. St. Staszica w Kielcach, Kielce, ul. Wesoła 52	z urzędu	30.06.2010 decyzja DIS/DEC-842/26168/10
41.	15-19.03.2010 DIS-K-421/41/10	Centrum Rekreacji i Rehabilitacji „Bushido”, Rybnik, ul. Floriańska 1	w związku z kontrolą DIS-K- 421/154/09	nie stwierdzono uchybień

42.	15-19.03.2010 DIS-K-421/42/10	Rybnickie Służby Komunalne, Rybnik, ul. Jankowicka 41 b	w związku z kontrolą DIS-K- 421/154/09	29.07.2010 decyzja DIS/DEC-977/30220/10
43.	22-26.03.2010 DIS-K-421/43/10	BRE Wealth Management S.A., Warszawa, ul. Królewska 14	z urzędu	25.06.2010 decyzja DIS/DEC-800/25660/10
44.	22-26.03.2010 DIS-K-421/44/10	Akademia Muzyczna im. Grażyny i Kiejstuta Bacewiczów w Łodzi, Łódź, ul. Gdańska 32	z urzędu	nie stwierdzono uchybień
45.	22-26.03.2010 DIS-K-421/45/10	Skandia Życie Towarzystwo Ubezpieczeń S.A., Warszawa, ul. Cybernetyki 7	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
46.	22-26.03.2010 DIS-K-421/46/10	Specjalistyczny Szpital im. dr Alfreda Sokołowskiego, Wałbrzych, ul. Sokołowskiego 4	DOLIS	24.09.2010 decyzja DIS/DEC-1133/37986/10
47.	29-31.03.2010 DIS-K-421/47/10	Dom Maklerski Amerbrokers S.A., Warszawa, Al. Jerozolimskie 123 A	z urzędu	nie stwierdzono uchybień
48.	29.03-01.04.2010 DIS-K-421/48/10	Dom Inwestycyjny BRE Banku S.A., Warszawa, ul. Wspólna 47/49	z urzędu	nie stwierdzono uchybień
49.	29.03-01.04.2010 DIS-K-421/49/10	Copernicus Securities S.A., Warszawa, ul. Grójecka 5	z urzędu	17.05.2010 decyzja DIS/DEC-588/20308/10
50.	29.03-01.04.2010 DIS-K-421/50/10	DB Securities S.A., Warszawa, Al. Armii Ludowej 26	z urzędu	08.06.2010 decyzja DIS/DEC-693/23436/10
51.	30.03-02.04.2010 DIS-K-421/51/10	Cargoforte Sp. z o.o., Warszawa, ul. Modularna 17	DRZDO	20.07.2010 decyzja DIS/DEC-943/29154/10
52.	06-09.04.2010 DIS-K-421/52/10	Centralny Dom Maklerski Pekao S.A., Warszawa, ul. Wołoska 18	z urzędu	21.06.2010 decyzja DIS/DEC-754/24870/10
53.	06-09.04.2010 DIS-K-421/53/10	Erste Securities Polska S.A., Warszawa, ul. Królewska 16	z urzędu	30.06.2010 decyzja DIS/DEC-838/26157/10
54.	07-09.04.2010 DIS-K-421/54/10	AXA Życie Towarzystwo Ubezpieczeń S.A., Warszawa, ul. Chłodna 51	z urzędu	07.06.2010 decyzja DIS/DEC-689/23129/10
55.	12-15.04.2010 DIS-K-421/57/10	„Real, - Sp. z o.o. i Spółka” Spółka Komandytowa, Warszawa, Al. Krakowska 61	DOLiS	15.10.2010 decyzja DIS/DEC-1206/40994/10
56.	12-16.04.2010 DIS-K-421/55/10	Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, Kraków, Al. Mickiewicza 21	z urzędu	27.08.2010 decyzja DIS/DEC-1034/34110/10
57.	12-16.04.2010 DIS-K-421/56/10	ProgMan S.A., Gdynia, Al. Zwycięstwa 96/98	DRZDO	23.07.2010 decyzja DIS/DEC-959/29604/10, wystąpienie do Ministra Edukacji Narodowej
58.	12-16.04.2010 DIS-K-421/58/10	Polskie Towarzystwo Walki z Mukowiscydą w Rabce – Zdroju, Rabka - Zdrój ul. Prof. Jana Rudnika 3 B	z urzędu	13.09.2010 decyzja DIS/DEC-1099/36435/10
59.	12-15.04.2010 DIS-K-421/59/10	Dom Maklerski UniCredit CA IB Poland S.A. Warszawa, ul. E. Plater 53	z urzędu	nie stwierdzono uchybień
60.	14-16.04.2010 DIS-K-421/60/10	Polskie Górnictwo Naftowe i Gazownictwo S.A. Warszawa, ul. Kasprzaka 25	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
61.	19-22.04.2010 DIS-K-421/63/10	Towarzystwo Ubezpieczeń Compensa S.A., Warszawa, Al. Jerozolimskie 162	z urzędu	nie stwierdzono uchybień
62.	19-22.04.2010 DIS-K-421/64/10	Generali Towarzystwo Ubezpieczeń S.A. Warszawa, ul. Postępu 15 B	z urzędu	22.07.2010 decyzja DIS/DEC-958/29559/10
63.	19-23.04.2010 DIS-K-421/61/10	4 Fun Tour Wojciech Baluch, Sławomir Króliczek, Grzegorz Pietraszewski s.c., Kraków, ul. Czarnowiejska 41/50	DRZDO	zaprzeszono przetwarzania danych osobowych
64.	19-23.04.2010 DIS-K-421/62/10	Grzegorz Błażewicz prowadzący działalność gospodarczą pod nazwą	DRZDO	nie stwierdzono uchybień

		„Benhauer”, Kraków, ul. Piłsudskiego 28 A		
65.	19-23.04.2010 DIS-K-421/65/10	Politechnika Białostocka, Białystok, ul. Wiejska 45 A	z urzędu	30.06.2010 decyzja DIS/DEC-839/26159/10
66.	19-23.04.2010 DIS-K-421/66/10	Comp S.A., Warszawa, ul. Jutrzenki 116	DOLiS	ustalenia wykorzystane w postępowaniu DIS-K-421/114/10
67.	26-29.04.2010 DIS-K-421/72/10	Towarzystwo Ubezpieczeń Allianz Polska S.A., Warszawa, ul. Rodziny Hiszpańskich 1	z urzędu	17.08.2010 decyzja DIS/DEC-1021/32677/10
68.	26-29.04.2010 DIS-K-421/73/10	Chartis Europe S.A. Oddział w Polsce, Warszawa, ul. Marszałkowska 111	z urzędu	nie stwierdzono uchybień
69.	26-29.04.2010 DIS-K-421/67/10	Millennium Dom Maklerski S.A., Warszawa, ul. St. Żaryna 2 A	z urzędu	nie stwierdzono uchybień
70.	26-30.04.2010 DIS-K-421/68/10	Jednostka Obsługi Finansowej Gospodarki Nieruchomościami, Zabrze, ul. Targowa 2	z urzędu	26.10.2010 decyzja DIS/DEC-1222/42400/10
71.	26-30.04.2010 DIS-K-421/69/10	Bohdan Tomaszewski prowadzący działalność gospodarczą pod nazwą "Dziecięce Centrum Edukacyjno - Sportowe Tomaszewski Bohdan", Wrocław, ul. Przyjaźni 38 a lok. 3	z urzędu	21.09.2010 decyzja DIS/DEC-1123/37610/10
72.	26-30.04.2010 DIS-K-421/70/10	Wyższa Szkoła Europejska im. ks. Józefa Tischnera, Kraków, ul. Westerplatte 11	z urzędu	10.11.2010 decyzja DIS/DEC-1258/44627/10
73.	28-30.04.2010 DIS-K-421/71/10	Beata Drózdź prowadząca działalność gospodarczą pod nazwą "Akademia Smart - Start", Radomierzyce, ul. Sadowa 8	z urzędu	08.11.2010 decyzja DIS/DEC-1253/44154/10
74.	05-06.05.2010 DIS-K-421/74/10	Fundacja "Azyl", Łódź, ul. Polna 21 a	DOLiS	16.09.2010 decyzja DIS/DEC-1116/37005/10
75.	05-07.05.2010 DIS-K-421/75/10	Towarzystwo Ubezpieczeń na Życie Cardif Polska S.A., Warszawa, ul. Nowogrodzka 11	z urzędu	15.09.2010 decyzja DIS/DEC-1114/36862/10
76.	05-07.05.2010 DIS-K-421/76/10	Powszechny Zakład Ubezpieczeń na Życie S.A., Warszawa, Al. Jana Pawła II 24	z urzędu	17.08.2010 decyzja DIS/DEC-1021/32677/10
77.	10-13.05.2010 DIS-K-421/80/10	Przedsiębiorstwo Handlowe A-T S.A., Krotoszyn, ul. Zacisze 2	z urzędu	30.06.2010 decyzja DIS/DEC-843/26172/10
78.	10-13.05.2010 DIS-K-421/82/10	Fundacja Instytut Edukacji Społecznej i Religijnej im. Ks. Piotra Skargi, Kraków, ul. Augustiańska 28	DOLiS	nie stwierdzono uchybień
79.	10-13.05.2010 DIS-K-421/77/10	X - Trade Brokers Dom Maklerski S.A. Warszawa, ul. Ogrodowa 58	z urzędu	30.06.2010 decyzja DIS/DEC-841/26163/10
80.	10-14.05.2010 DIS-K-421/79/10	Wyższa Szkoła Menedżerska w Warszawie, Warszawa, ul. Kawęczyńska 36	z urzędu	nie stwierdzono uchybień
81.	11-12.05.2010 DIS-K-421/78/10	Okręgowy Zarząd Polskiego Związku Działkowców w Częstochowie, Częstochowa, ul. Bór 201	DOLiS	przywrócono stan zgodny z prawem
82.	17-19.05.2010 DIS-K-421/81/10	Polska Telefonia Komórkowa Centertel Sp. z o. o., Warszawa, ul. Skierniewicka 10 a	z urzędu	19.10.2010 decyzja DIS/DEC-1212/41382/10
83.	17-19.05.2010 DIS-K-421/85/10	BENEFIA Towarzystwo Ubezpieczeń na Życie Vienna Insurance Group, Warszawa, ul. Rydygiera 21	z urzędu	16.09.2010 decyzja DIS/DEC-1115/36951/10
84.	17-20.05.2010 DIS-K-421/83/10	Media Regionalne Sp. z o.o., Warszawa, ul. Prosta 51	DOLiS	03.02.2011 DIS/DEC-63/4537/11
85.	17-21.05.2010 DIS-K-421/84/10	Uniwersytet Muzyczny Fryderyka Chopina, Warszawa, ul. Okólnik 2	z urzędu	29.07.2010 decyzja DIS/DEC-979/30224/10



86.	17-21.05.2010 DIS-K-421/86/10	Akademia Górniczo - Hutnicza im. St. Staszica w Krakowie, Kraków, Al. Mickiewicza 30	DOLiS	17.08.2010 decyzja DIS/DEC-1018/32575/10
87.	17-21.05.2010 DIS-K-421/87/10	Dolsat Sp. z o.o., Bełchatów, ul. Wojska Polskiego 23 C	z urzędu	13.01.2011 decyzja DIS/DEC-13/1114/11
88.	24-27.05.2010 DIS-K-421/88/10	Dotpay S.A., Kraków, ul. Wielicka 72	DOLiS	20.07.2010 decyzja DIS/DEC-945/29158/10
89.	24-28.05.2010 DIS-K-421/89/10	Europejska Wyższa Szkoła Prawa i Administracji, Warszawa, ul. Grodzieńska 21/29	z urzędu	01.10.2010 decyzja DIS/DEC-1149/38892/10
90.	24-28.05.2010 DIS-K-421/90/10	PKO Bank Polski S.A., Warszawa, ul. Puławska 15	z urzędu	nie stwierdzono uchybień
91.	26-28.05.2010 DIS-K-421/91/10	MetLife Towarzystwo Ubezpieczeń na Życie S.A., Warszawa, ul. Puławska 17	z urzędu	nie stwierdzono uchybień
92.	26-28.05.2010 DIS-K-421/92/10	Polska Telefonia Cyfrowa Sp. z o.o., Warszawa, Al. Jerozolimskie 181	z urzędu	nie stwierdzono uchybień
93.	26-28.05.2010 DIS-K-421/94/10	Google Poland Sp. z o.o., Warszawa, ul. E. Plater 53	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
94.	07-09.06.2010 DIS-K-421/95/10	AVIVA Towarzystwo Ubezpieczeń na Życie S.A., Warszawa, ul. Prosta 70	z urzędu	nie stwierdzono uchybień
95.	07-10.06.2010 DIS-K-421/97/10	Dyrektor Urzędu Kontroli Skarbowej w Łodzi, Łódź, ul. Ks. Brzóska 24	z urzędu	01.12.2010 decyzja DIS/DEC-1324/47593/10
96.	08 i 11.06.2010 DIS-K-421/96/10	Tomasz Bieniek prowadzący działalność gospodarczą pod nazwą "Tomasz Bieniek", Warszawa, ul. Fletniowa 24 D	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
97.	09-11.06.2010 DIS-K-421/98/10	Polkomtel S.A., Warszawa, ul. Postępu 3	z urzędu	04.11.2010 decyzja DIS/DEC-1244/43775/10
98.	10-11.06.2010 DIS-K-421/99/10	Szef Urzędu do Spraw Cudzoziemców, Warszawa, ul. Koszykowa 16	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
99.	14-16.06.2010 DIS-K-421/101/10	Nordea Polska Towarzystwo Ubezpieczeń na Życie S.A., Warszawa, Al. Jana Pawła II 2	z urzędu	nie stwierdzono uchybień
100.	14-17.06.2010 DIS-K-421/102/10	Dyrektor Urzędu Kontroli Skarbowej w Bydgoszczy, Bydgoszcz, ul. Dr K. Marcinkowskiego 7	z urzędu	01.12.2010 decyzja DIS/DEC-1325/47595/10
101.	14-17.06.2010 DIS-K-421/103/10	Dyrektor Urzędu Kontroli Skarbowej w Kielcach, Kielce, ul. Sandomierska 105	z urzędu	03.12.2010 decyzja DIS/DEC-1330/47863/10
102.	14-18.06.2010 DIS-K-421/100/10	Dyrektor Urzędu Kontroli Skarbowej w Warszawie, Warszawa, ul Cybernetyki 19 B	z urzędu	przywrócono stan zgodny z prawem
103.	16-18.06.2010 DIS-K-421/104/10	PRAMERICA Życie Towarzystwo Ubezpieczeń i Reasekuracji S.A., Warszawa, Al. Jana Pawła II 23	z urzędu	nie stwierdzono uchybień
104.	21-24.06.2010 DIS-K-421/106/10	Loyalty Partner Polska Sp. z o.o., Warszawa, Al. Jerozolimskie 148	z urzędu	10.09.2010 decyzja DIS/DEC-1098/36246/10
105.	21-25.06.2010 DIS-K-421/105/10	Grupa Onet.pl S.A., Kraków, ul. G. Zapolskiej 44	DOLiS	18.01.2011 decyzja DIS/DEC- 27/2040,2042,2046/11
106.	28-29.06.2010 DIS-K-421/107/10	StarGraphics Sp. z o.o. Warszawa, ul. Sarmacka 7b/2	DOLiS	17.08.2010 decyzja DIS/DEC-1022/32681/10
107.	28-30.06.2010 DIS-K-421/108/10	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	z urzędu	15.12.2010 decyzja DIS/DEC-1375/49785/10
108.	05-08.07.2010	K2 Doradcy Finansowi	DOLiS	przywrócono stan zgodny z prawem

	DIS-K-421/111/10	Sp. z o.o., Warszawa, ul. Domaniewska 41		
109.	05-09.07.2010 DIS-K-421/109/10	Nasza Klasa Sp. z o.o., Wrocław, ul. Gen. J. Bema 2	DOLiS	w toku
110.	05-09.07.2010 DIS-K-421/110/10	Zarząd Transportu Miejskiego w Lublinie, Lublin, Al. Kraśnicka 25	w związku z kontrolą DIS-K- 421/113/09	21.08.2010 decyzja DIS/DEC-1126/37825/10
111.	06-08.07.2010 DIS-K-421/112/10	Finlop Rohr Sp. z o.o., Warszawa, ul. Nocznickiego 33	DOLiS	06.10.2010 decyzja DIS/DEC-1158/39560/10
112.	06-08.07.2010 DIS-K-421/113/10	Makro Cash and Carry Polska S.A., Warszawa, Al. Krakowska 61	DOLiS	04.10.2010 decyzja DIS/DEC-1152/39023/10
113.	07-09.07.2010 DIS-K-421/114/10	Ministerstwo Sprawiedliwości, Warszawa, Al. Ujazdowskie 11	w związku z kontrolą DIS-K- 421/66/10	29.10.2010 decyzja DIS/DEC- 1232/42977,42983/10
114.	07-09.07.2010 DIS-K-421/115/10	Vision Express SP Sp. z o.o., Warszawa, Al. Jerozolimskie 200	DOLiS	30.09.2010 decyzja DIS/DEC-1144/38747/10; 14.10.2010 wystąpienie do Ministra Zdrowia
115.	16-20.08.2010 DIS-K-421/116/10	Zakład Ubezpieczeń Społecznych III Oddział w Warszawie, Warszawa, ul. Senatorska 6/8	DOLiS	nie stwierdzono uchybień
116.	17-20.08.2010 DIS-K-421/117/10	Dyrektor Urzędu Kontroli Skarbowej w Białymstoku, Białystok, Al. 1000-lecia Państwa Polskiego 8	z urzędu	201.12.010 decyzja DIS/DEC-1323/47590/10
117.	17-20.08.2010 DIS-K-421/118/10	Piotr Dulowski prowadzący działalność gospodarczą pod nazwą "Kinesis - Rehabilitacja Piotr Dulowski", Warszawa, ul. Rokosowska 10	DOLiS	15.10.2010 decyzja DIS/DEC-1207/40996/10
118.	17-20.08.2010 DIS-K-421/119/10	Dyrektor Urzędu Kontroli Skarbowej w Gdańsku, Gdańsk, ul. Chłopska 3	z urzędu	01.12.2010 decyzja DIS/DEC-1321/47592/10
119.	17-20.08.2010 DIS-K-421/120/10	Dyrektor Urzędu Kontroli Skarbowej w Katowicach, Katowice, ul. I. Paderewskiego 32 b	z urzędu	01.12.2010 decyzja DIS/DEC-1322/47589/10
120.	18-20.08.2010 DIS-K-421/121/10	Orbis Casino Sp. z o.o., Warszawa, ul. Jubilerska 10	DRZDO	07.10.2010 decyzja DIS/DEC-1160/39738/10
121.	23-27.08.2010 DIS-K-421/122/10	Dyrektor Urzędu Kontroli Skarbowej w Olsztynie, Olsztyn, ul. Lubelska 37	z urzędu	03.12.2010 decyzja DIS/DEC-1329/47846/10
122.	23-27.08.2010 DIS-K-421/123/10	Gmina Stara Kiszewa, Stara Kiszewa, ul. Ogrodowa 1	DOLiS	w toku
123.	23-27.08.2010 DIS-K-421/124/10	Dyrektor Urzędu Kontroli Skarbowej w Lublinie, Lublin, ul. Lubomelska 1-3	z urzędu	03.12.2010 decyzja DIS/DEC-1331/47871/10
124.	23-27.08.2010 DIS-K-421/125/10	Dyrektor Urzędu Kontroli Skarbowej w Poznaniu, Poznań, ul. Strzelecka 2/6	z urzędu	01.12.2010 decyzja DIS/DEC-1320/47585/10
125.	24-26.08.2010 DIS-K-421/126/10	Bank Polskiej Spółdzielczości S.A., Warszawa, ul. Płocka 9/11B	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
126.	24-27.08.2010 DIS-K-421/127/10	Centrum Onkologii - Instytut im. M. Sklódowskiej Curie w Warszawie, Warszawa, ul. W. K. Roentgena 5	DOLiS	11.10.2010 wystąpienie do Ministra Zdrowia i Głównego Urzędu Statystycznego
127.	06-07.09.2010 DIS-K-421/129/10	GTS Energis Sp. z o.o., Warszawa, Al. Niepodległości 69	z urzędu	nie stwierdzono uchybień
128.	06-08.09.2010 DIS-K-421/128/10	Polkomtel S.A., Warszawa, ul. Postępu 3	DOLiS	nie stwierdzono uchybień
129.	07-10.09.2010 DIS-K-421/130/10	Aster Sp. z o.o., Warszawa, ul. Domaniewska 50	z urzędu	nie stwierdzono uchybień
130.	07-10.09.2010	Zakład Gospodarki Komunalnej w	z urzędu	nie stwierdzono uchybień

	DIS-K-421/131/10	Konstancinie – Jeziornie, Konstancin – Jeziorna, ul. Warecka 22		
131.	09.09.2010 DIS-K-421/132/10	Google Poland Sp. z o.o., Warszawa, ul. E. Plater 53	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
132.	13-16.09.2010 DIS-K-421/133/10	Cyfrowy Polsat S.A., Warszawa, ul. Łubinowa 4 a	z urzędu	nie stwierdzono uchybień
133.	13-17.09.2010 DIS-K-421/134/10	InPost Sp. z o.o., Kraków, ul. Malborska 130	DOLiS	nie stwierdzono uchybień
134.	14-17.09.2010 DIS-K-421/135/10	COBICO Sp. z o.o., Kraków ul. Grzegórzecka 77	DRZDO	15.12.2010 decyzja DIS/DEC-1376/49787/10
135.	15-17.09.2010 DIS-K-421/136/10	Omnigence Sp. z o.o., Warszawa, ul. Bukowińska 22 B	z urzędu	15.12.2010 decyzja DIS/DEC-1377/49788/10
136.	15-17.09.2010 DIS-K-421/137/10	Sferia S.A., Warszawa, ul. Pawia 55	z urzędu	nie stwierdzono uchybień
137.	20-21.09.2010 DIS-K-421/141/10	Artegence Sp. z o.o., Warszawa, ul. Bukowińska 22 B	w związku z kontrolą DIS-K-421/136/10	15.12.2010 decyzja DIS/DEC-1377/49788/10
138.	20-23.09.2010 DIS-K-421/138/10	Zespół Szkół Rolniczych Centrum Kształcenia Praktycznego i Centrum Kształcenia Ustawicznego im. St. Staszica w Miętnej, Miętne, ul. Główna 49	DOLiS	21.02.2011 DIS-DEC-119/7194/11
139.	20-23.09.2010 DIS-K-421/139/10	UPC Polska Sp. z o.o., Warszawa, Al. Jana Pawła II 27	z urzędu	07.04.2011 DIS/DEC-289/15964/11
140.	20-23.09.2010 DIS-K-421/140/10	Zarząd Gospodarki Mieszkaniowej w Otwocku, Otwock, ul. Wawerska 8	z urzędu	w toku
141.	27.09.2010 DIS-K-421/143/10	Media Regionalne Sp. z o.o., Warszawa, ul. Prosta 51	w związku z kontrolą DIS-K-421/83/10	02.03.2011 DIS/DEC-63/4537/11
142.	27-29.09.2010 DIS-K-421/146/10	Hydrosfera Józefów Sp. z o.o., Józefów, ul. Drogowców 20	z urzędu	20.12.2010 decyzja DIS/DEC-1382/50257/10
143.	27-29.09.2010 DIS-K-421/144/10	Miejski Zakład Oczyszczania w Wołominie, Wołomin, ul. Łukasiewicza 4	z urzędu	26.11.2010 decyzja DIS/DEC-1309/46925/10
144.	27-30.09.2010 DIS-K-421/142/10	TelePolska Sp. z o.o., Warszawa, Al. Jerozolimskie 123 a	z urzędu	08.12.2010 decyzja DIS/DEC-1350/48487/10
145.	28-30.09.2010 DIS-K-421/145/10	Związek Banków Polskich, Warszawa, ul. Kruczkowskiego 8	DOLiS	nie stwierdzono uchybień
146.	04-06.10.2010 DIS-K-421/147/10	INFOR Biznes Sp. z o.o., Warszawa, ul. Okopowa 58/72	DOLiS	20.12.2010 decyzja DIS/DEC-1381/50253/10
147.	05-06.10.2010 DIS-K-421/148/10	Mobyland Sp. z o.o., Warszawa, ul. Lwowska 19	z urzędu	nie stwierdzono uchybień
148.	05-07.10.2010 DIS-K-421/150/10	Plagiat.pl Sp. z o.o., Warszawa, ul. Przanowskiego 32 lok.53	DOLiS	w toku
149.	05-08.10.2010 DIS-K-421/149/10	Zakład Wodociągów i Kanalizacji Sp. z o.o., Nowy Dwór Mazowiecki, ul. Gen. Berlinga 100	z urzędu	10.03.2011 DIS/DEC-194/10396/11
150.	11.10.2010 DIS-K-421/153/10	Carrefour Polska Sp. z o.o., Warszawa, ul. Targowa 72	z urzędu	brak przetwarzania danych osobowych
151.	11-14.10.2010 DIS-K-421/151/10	Zakład Gospodarki Komunalnej w Grodzisku Mazowieckim, Grodzisk Mazowiecki, ul. Sportowa 29	z urzędu	21.02.2011 DIS-DEC-118/7190/11
152.	11-14.10.2010 DIS-K-421/152/10	GG Networks S.A., Warszawa, ul. Kamionkowska 45	z urzędu	11.01.2011 decyzja DIS/DEC-14/1117/11
153.	11-15.10.2010 DIS-K-421/154/10	Radarsystem Sp. z o.o., Gdańsk, ul. Diamentowa 11	w związku z kontrolą DIS-K-421/123/10	w toku
154.	18-21.10.2010 DIS-K-421/155/10	Polskie Technologie Internetowe Sp. z o.o., Sopot, Al. Niepodległości 705/5	DOLiS	nie stwierdzono uchybień

155.	18-22.10.2010 DIS-K-421/156/10	Blue Media S.A., Sopot, ul. Haffnera 6	DOLiS	nie stwierdzono uchybień
156.	19-22.10.2010 DIS-K-421/158/10	Zakład Gospodarki Komunalnej i Mieszkaniowej w Milanówku, Milanówek, ul. Fiderkiewicza 41	z urzędu	31.03.2011 DIS/DEC-265/14679/11
157.	20-22.10.2010 DIS-K-421/157/10	Zakład Gospodarowania Nieruchomościami Dzielnicy Białołęka m. st. Warszawy, Warszawa, ul. Marywilska 44	z urzędu	11.04.2011 DIS/DEC-292/16555,16557/11
158.	25-28.10.2010 DIS-K-421/160/10	Gminna Gospodarka Komunalna Ochota Sp. z o. o., Warszawa, ul. Grójecka 184	z urzędu	nie stwierdzono uchybień
159.	26-29.10.2010 DIS-K-421/159/10	Miejski Zakład Wodociągów i Kanalizacji w Sulejówku, Sulejówek, ul. Wodociągowa 10	z urzędu	29.03.2011 DIS/DEC-250/14068/11
160.	26-29.10.2010 DIS-K-421/161/10	NetPartner Polska Sp. z o. o., Warszawa, ul. Wilcza 31/1	z urzędu	nie stwierdzono uchybień
161.	26-29.10.2010 DIS-K-421/162/10	Przedsiębiorstwo Gospodarki Komunalnej w Zielonce Sp. z o.o., Zielonka, ul. Krzywa 18	z urzędu	nie stwierdzono uchybień
162.	27-28.10.2010 DIS-K-421/163/10	Telekomunikacja Polska S.A., Warszawa, ul. Twarda 18	z urzędu	15.12.2010 decyzja DIS/DEC-1374/49782/10
163.	02.11.2010 DIS-K-421/166/10	Zakład Unieszkodliwiania Stałych Odpadów Komunalnych, Warszawa, ul. Gwarków 9	z urzędu	nie stwierdzono uchybień
164.	02-05.11.2010 DIS-K-421/164/10	Okręgowy Zarząd Podkarpacki Polskiego Związku Działkowców, Rzeszów, ul. Hanasiewicza 6 a	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
165.	02-05.11.2010 DIS-K-421/165/10	Rodzinny Ogród Działkowy "Nasz Gaj", Rzeszów, Al. Powstańców Warszawy	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
166.	03-04.11.2010 DIS-K-421/167/10	Zarząd Transportu Miejskiego, Warszawa, ul. Senatorska 37	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
167.	03-05.11.2010 DIS-K-421/168/10	CP Telecom Sp. z o.o., Warszawa, ul. Bytomska 3	z urzędu	11.04.2011 DIS/DEC-293/16559/11
168.	08-09.11.2010 DIS-K-421/171/10	Castorama Polska Sp. z o.o., Warszawa, ul. Krakowiaków 78	DOLiS	nie stwierdzono uchybień
169.	08-09.11.2010 DIS-K-421/169/10	BRE Bank S.A., Warszawa, ul. Senatorska 18	DOLiS	przywrócono stan zgodny z prawem
170.	08-10.11.2010 DIS-K-421/170/10	HSBC Bank Polska S.A., Warszawa, ul. Marszałkowska 89	DRZDO	29.03.2011 DIS/DEC-249/14067/11
171.	08-10.11.2010 DIS-K-421/172/10	Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych, Warszawa, Al. Jana Pawła II 13	DOLiS	nie stwierdzono uchybień
172.	15-18.11.2010 DIS-K-421/174/10	Zakład Gospodarowania Nieruchomościami w Dzielnicy Wawer m. st. Warszawy, Warszawa, ul. Trakt Lubelski 353	z urzędu	10.03.2011 DIS/DEC-192/10392/11
173.	15-18.11.2010 DIS-K-421/175/10	Zakład Gospodarowania Nieruchomościami w Dzielnicy Targówek m. st. Warszawy, Warszawa, ul. Gościeradowska 5	z urzędu	31.03.2011 DIS/DEC-258/14575/11
174.	15-19.11.2010 DIS-K-421/173/10	Główny Urząd Statystyczny, Warszawa, Al. Niepodległości 208	z urzędu	29.03.2011 DIS/DEC-252/14105/11
175.	22-25.11.2010 DIS-K-421/176/10	Miejskie Przedsiębiorstwo Usług Komunalnych Sp. z o.o., Warszawa, ul. Redutowa 25	z urzędu	przywrócono stan zgodny z prawem
176.	23-26.11.2010 DIS-K-421/177/10	Przedsiębiorstwo Usług Komunalnych Sp. z o.o., Mińsk Mazowiecki ul. Tuwima 1	z urzędu	29.03.2011 DIS/DEC-251/14090/11

177.	24-26.11.2010 DIS-K-421/178/10	Michał Skrzyński prowadzący działalność gospodarczą pod nazwą "Impessa Michał Skrzyński", Warszawa, ul. Cybernetyki 13 m 66	z urzędu	w toku
178.	03.12.2010 DIS-K-421/179/10	Akademia Sztuk Pięknych w Warszawie, Warszawa, ul. Krakowskie Przedmieście 5	z urzędu	wykonano decyzję DIS/DEC-652/21890/10
179.	03.12.2010 DIS-K-421/180/10	Andrzej Kollwitz prowadzący działalność gospodarczą pod firmą Andrzej Kollwitz "LENDER", Warszawa, ul. Targowa 66 paw. 31	z urzędu	wykonano decyzję DIS/DEC-978/30221/10
180.	03.12.2010 DIS-K-421/181/10	Piotr Tyc Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Śródmieścia, Kancelaria Komornicza, Warszawa, ul. Śniadeckich 17	z urzędu	wykonano decyzję DIS/DEC-276/11299/10
181.	06-07.12.2010 DIS-K-421/182/10	Szkoła Wyższa Psychologii Społecznej, Warszawa, ul. Chodakowska 19/31	z urzędu	wykonano decyzję DIS/DEC-655/21899/10
182.	06-08.12.2010 DIS-K-421/183/10	Komendant Główny Policji, Warszawa, ul. Puławska 148/150	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
183.	08-09.12.2010 DIS-K-421/184/10	Johnnson & Johnson Poland Sp. z o.o., Warszawa, ul. Hłeczka 24	DRZDO	nie stwierdzono uchybień
184.	08-09.12.2010 DIS-K-421/186/10	Holiday Travel Center Sp. z o.o., Warszawa, ul. Klarysewska 49 a	DOLiS	11.04.2011 DIS/DEC-291/16553/11
185.	08-10.12.2010 DIS-K-421/185/10	ITI Neovision Sp. z o.o., Warszawa, ul. Kłobucka 23	DOLiS	w toku
186.	13.12.2010 DIS-K-421/190/10	Janssen-Cilag Polska Sp. z o.o., Warszawa, ul. Hłeczka 24	ORZDO	nie stwierdzono uchybień
187.	13-14.12.2010 DIS-K-421/187/10	Szef Urzędu do Spraw Cudzoziemców, Warszawa, ul. Koszykowa 16	DOLiS	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
188.	13-14.12.2010 DIS-K-421/189/10	Anmark B. Kryńska i Wspólnicy sp.j., Warszawa, ul. Fasolowa 1 Kontrola sprawdzająca DIS/DEC-1089/39969/10	z urzędu	nie stwierdzono uchybień
189.	15-17.12.2010 DIS-K-421/194/10	Fundacja Faktu "Od Serca", Warszawa, ul. Domaniewska 52	DRZDO	w toku
190.	15-20.12.2010 DIS-K-421/188/10	Instytut Kardiologii im. Prymasa Tysiąclecia Stefana Kardynała Wyszyńskiego, Warszawa, ul. Alpejska 42	DOLiS	nie stwierdzono uchybień
191.	16.12.2010 DIS-K-421/191/10	Multikino S.A., Warszawa, ul. Wiertnicza 166	z urzędu	wykonano decyzję DIS/DEC-1002/37026/10
192.	16.12.2010 DIS-K-421/192/10	BRE Bank S.A., Warszawa, ul. Senatorska 18	z urzędu	wykonano decyzję DOLiS/DEC-1220/10/42383, 42388, 42391
193.	17.12.2010 DIS-K-421/193/10	Akademia Teatralna im. Aleksandra Zelwerowicza, Warszawa, ul. Miodowa 22/24	z urzędu	wykonano decyzję DIS/DEC-585/20169/10
194.	20.12.2010 DIS-K-421/195/10	Centralny Dom Maklerski Pekao S.A., Warszawa, ul. Wołoska 18	z urzędu	wykonano decyzję DIS/DEC-754/24870/10
195.	20.12.2010 DIS-K-421/196/10	Biuro Maklerskie Banku Gospodarki Żywnościowej S.A., Warszawa, ul. Żurawia 6/12	z urzędu	wykonano decyzję DIS/DEC-857/26450/10
196.	20.12.2010 DIS-K-421/197/10	Akademia Wychowania Fizycznego im. Józefa Piłsudskiego, Warszawa, ul. Marymoncka 34 Kontrola sprawdzająca - DIS/DEC-831/26029/10	z urzędu	w toku

**Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie  
i Naczelnego Sądu Administracyjnego wydanych w 2010 r.  
w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych**

<b>L.p.</b>	<b>Data/ sygnatura orzeczenia WSA w Warszawie lub NSA</b>	<b>Sygnatura rozstrzygnięcia GIODO</b>	<b>Przedmiot sprawy</b>	<b>Rozstrzygnięcie WSA w Warszawie lub NSA</b>
1.	05.01.2010 I OSK 399/09	DIS/DEC- 353/14514/08	Pozyskiwanie do zbioru danych w celach marketingowych danych osobowych potencjalnych klientów bez ich zgody	oddalenie skargi kasacyjnej
2.	08.01.2010 II S.A./Wa 069/09	DOLiS/DEC-63/09/ 16256,16261,16264	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
3.	18.01.2010 II S.A./Wa 613/09	DOLiS/DEC-61/09/ 28396,28395	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	odrzućenie skargi
4.	19.01.2010 I OSK 491/09	DOLiS/DEC-60/08/ 19685,19691	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
5.	26.01.2010 II SA/Wa1686/09	DOLiS/DEC-53/09/ 28118,28121, 28123,28127	Skarga na decyzję w przedmiocie odmowy udostępnienia danych	uchylenie zaskarżonej decyzji
6.	27.01.2010 II SA/Wa 1671/09	DOLiS/DEC-59/09/ 28307,28308	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
7.	27.01.2010 II SA/Wa 1672/09	DOLiS/DEC-69/09/ 28681,28684	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
8.	27.01.2010 II SA/Wa 1104/09	DOLiS/DEC-18/09/ 14465,14471	Skarga na decyzję w przedmiocie uchylenia decyzji dotyczącej umorzenia postępowania w sprawie przetwarzania danych osobowych	odrzućenie skargi
9.	10.02.2010 II SA/Wa 1783/09	DOLiS/DEC-02/09/ 29178,29180, 29181,19185	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych	oddalenie skargi
10.	25.02.2010 II S.A./Wa 150/10	DIS/DEC- 1092/39983, 39986/09	Zaprzestanie pozyskiwania danych osobowych na „Formularzach wizyty serwisowej” przetwarzanych w celach marketingowych, bez zgody osób, których dane dotyczą i usunięcie danych osobowych pozyskanych na tych formularzach w celach marketingowych, bez zgody osób, których dane dotyczą	wstrzymanie wykonania decyzji w części dotyczącej nakazu usunięcia danych osobowych pozyskanych na „Formularzach wizyty serwisowej” i oddalenie wniosku w pozostałej części
11.	03.03.2010 II SA/Wa 1349/08	DOLiS/DEC-79/08/ 20756,20759	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ochrony danych osobowych	uchylenie zaskarżonej decyzji
12.	10.03.2010 II S.A./Wa 110/10	GI-DOLiS-30/4/07/ 4297,4298,4299	Skarga na postanowienie w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego postanowienia

13.	10.03.2010 II SA/Wa 1857/09	DOLiS/DEC-58/09/ 34487,3488	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
14.	11.03.2010 II S.A./Wa 953/09	GI-DEC-DOLiS- 131/07/ 2904,2905,2906	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
15.	15.03.2010 I OSK 756/09	DOLiS/DEC-479/08/ 20756,20759	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie umorzenia postępowania w sprawie ochrony danych osobowych	oddalenie skargi kasacyjnej
16.	24.03.2010 II S.A./Wa 86/09	DOLiS/POST- 351/08/ 32706,32709	Skarga na postanowienie z przedmiocie stwierdzenia niedopuszczalności wniosku o ponowne rozpatrzenie sprawy	uchylenie zaskarżonego postanowienia
17.	31.03.2010 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	podjęcie zawieszonego postępowania przez WSA w Warszawie
18.	01.04.2010 II SA/Wa 23/10	DOLiS/DEC- 1137/09/ 41674,41675,41676	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	odrzućcie skargi
19.	13.04.2010 I OSK 1156/09	DOLiS/DEC-903/08/ 35920,35923	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
20.	14.04.2010 II SA/Wa 2130/09	DOLiS/DEC- 1103/09/ 40498,40499,40502	Sprawa ze skargi na decyzję w przedmiocie umorzenia postępowania	uchylenie zaskarżonej decyzji
21.	16.04.2010 I OSK 572/10	DOLiS/DEC-761/09/ 28396,28395	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	oddalenie skargi kasacyjnej
22.	19.04.2010 II SA/Wa 251/10	DOLiS/DEC- 1249/09/ 46504,46508,46510	Skarga na postanowienie w przedmiocie ochrony danych osobowych	odrzućcie skargi
23.	21.04.2010 II SA/Wa 80/10	DIS/DEC-1069/ 39458/09	Usunięcie z urzędu sensytmetycznego danych osobowych skarżącego	uchylenie zaskarżonej decyzji
24.	22.04.2010 I OSK 623/10	DOLiS/DEC-285/09/ 12865,12867	Wniosek o wstrzymanie wykonania decyzji	wstrzymanie wykonania zaskarżonej decyzji
25.	27.04.2010 II SA/Wa 316/09	GI-DS-430/867/05/ 3397/07/DOLiS	Skarga na postanowienie w przedmiocie odmowy przywrócenia terminu do złożenia wniosku o ponowne rozpatrzenie sprawy	uchylenie zaskarżonego postanowienia
26.	29.04.2010 II SA/Wa 219/10	DOLiS/DEC- 1182/09/ 43667,43669	Skarga na decyzję w przedmiocie nakazu usunięcia uchybień przy przetwarzaniu danych osobowych	uchylenie zaskarżonej decyzji
27.	11.05.2010 II SA/Wa 292/10	DOLiS/DEC- 1240/09/ 46218,46221, 46224,46226	Skarga na decyzję z przedmiocie odmowy stwierdzenia nieważności decyzji nakazującej udostępnienie danych osobowych	odmowa przywrócenia terminu do wniesienia skargi
28.	11.05.2010 I OSK 693/10	DOLiS/POST-42/09/ 4677,4680,4683, 4687	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na postanowienie w przedmiocie uwzględnienia wniosku	uchylenie zaskarżonego wyroku

29.	11.05.2010 I OSK 963/09	DOLiS/DEC-531/08/ 23734,23735	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie udostępnienia danych	oddalenie skargi kasacyjnej
30.	12.05.2010 II SA/Wa 652/10	DIS/DEC- 229/8625/10	Skarga na odmowę udostępnienia informacji publicznej	odrzućcie skargi
31.	13.05.2010 II SAB/Wa 3/10	DOLiS-440-714/09	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku dotyczącego przetwarzania danych osobowych	oddalenie skargi
32.	13.05.2010 II SA/Wa 1016/09	DOLiS/DEC-347/09/ 15420,15421	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	oddalenie skargi
33.	14.05.2010 II SA/Wa 150/10	DIS/DEC-1092/ 39983,39986/09	Zaprzestanie pozyskiwania danych osobowych na „Formularzach wizyty serwisowej” przetwarzanych w celach marketingowych, bez zgody osób, których dane dotyczą i usunięcie danych osobowych pozyskanych na „Formularzach wizyty serwisowej” przetwarzanych w celach marketingowych, bez zgody osób, których dane dotyczą	stwierdzenie nieważności zaskarżonej decyzji
34.	21.05.2010 II SA/Wa 331/10	DOLiS/DEC- 1276/09/ 47685,47691	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
35.	25.05.2010 II SA/Wa 365/10	DOLiS/DEC- 1324/09/ 48315,48317	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
36.	27.05.2010 II SA/Wa 358/10	DOLiS/DEC- 1265/09/ 47082,47084	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	oddalenie skargi
37.	28.05.2010 I OSK 1058/09	DOLiS/DEC-488/08/ 21517,21518, 21519,21520	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie umorzenia postępowania	uchylenie zaskarżonego wyroku
38.	11.06.2010 II SA/Wa 23/10	DOLiS/DEC- 1137/09/41674, 41675,41676	Wniosek o przywrócenie terminu do uiszczenia wpisu od skargi na decyzję w przedmiocie nakazu udostępnienia danych	odmowa przywrócenia terminu do uiszczenia wpisu
39.	11.06.2010 II SA/Wa 784/09	DOLiS/DEC-217/09/ 9959,9960,9962, 9964,9966,9967, 9970,9973,9978, 9981,9984,9987, 9993	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
40.	14.06.2010 II SA/Wa 953/09	GI-DEC-DOLiS- 113/07/2904,2905, 2906	Wniosek o wykładnię wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych	odmowa wykładni wyroku
41.	15.06.2010 II SA/Wa 1130/09	DOLiS/POST- 101/09/ 14892,14893	Wniosek o przywrócenie terminu w sprawie ze skargi na postanowienie w przedmiocie odmowy uwzględnienia wniosku	przywrócenie terminu do wniesienia skargi
42.	15.06.2010 r. II SA/Wa 556/10	DOLiS/DEC-110/10/ 3760,3762	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
43.	15.06.2010 II SA/Wa 1494/08	DOLiS/DEC-494/08/ 21626,21628	Skargą na decyzję z przedmiocie ochrony danych osobowych	oddalenie skargi
44.	21.06.2010 II SA/Wa 1771/09	DOLiS/DEC-750/09/ 27846,27854, 27859,27862	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi



45.	22.06.2010 II SAB/Wa 64/10	DOLiS-440-504/09	Skarga na bezczynność w przedmiocie ochrony danych osobowych	umorzenie postępowania w sprawie
46.	23.06.2010 II SA/Wa 872/10	DOLiS/DEC-309/10/ 12985,12994	Skarga na decyzję w przedmiocie nakazu usunięcia uchybień w procesie przetwarzania danych osobowych	odrzućcie skargi
47.	24.06.2010 II SA/Wa 790/10	DOLiS/DEC- 249/10/9573	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	odrzućcie skargi
48.	28.06.2010 II SA/Wa 769/10	DOLiS/POST-42/09/ 4677,4680,4683, 4687	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku	odrzućcie skargi
49.	01.07.2010 II SA/Wa 744/20	DOLiS-440-711/08/ 10775/10	Skarga na pismo	odrzućcie skargi
50.	08.07.2010 II SA/Wa 304/09	DOLiS/DEC-64/09/ 2530,2532	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
51.	08.07.2010 II SA/Wa 247/10	DIS/DEC- 1206/44991/09	Przetwarzanie danych osobowych kandydatów do pracy na stanowisko magazyniera lub kuriera, pozyskanych za pomocą testów przeprowadzanych w systemach informatycznych	uchylenie zaskarżonej decyzji
52.	13.07.2010 I OSK 1224/09	GI-DEC-DOLiS- 148/07/ 3926,3927	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego wyroku
53.	13.07.2010 I OSK 1260/09	GI-DS-430/867/05/ 3397/07/DOLiS	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na postanowienie w przedmiocie odmowy przywrócenia terminu do złożenia wniosku o ponowne rozpatrzenie sprawy	oddalenie skargi kasacyjnej
54.	13.07.2010 I OSK 1395/09	DOLiS/DEC-494/08/ 21626,21628	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
55.	14.07.2010 II SA/Wa 329/10	DOLiS/DEC- 1293/09/ 48041,48042,48046	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
56.	15.07.2010 I OSK 1079/10	DOLiS/DEC-109/09/ 4751,4752	Wniosek o wstrzymanie wykonania decyzji	wstrzymanie wykonania zaskarżenia decyzji
57.	21.07.2010 I OZ 545/10	DOLiS/POST- 101/09/ 14892,14893	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku	oddalenie zażalenia
58.	28.07.2010 II SAB/Wa 191/10	DOLiS-440-835/09	Skarga na bezczynność w przedmiocie umorzenia postępowania	umorzenie postępowania
59.	29.07.2010 II SA/WA 539/10	DOLiS/DEC-27/10/ 1591,1598,1602	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
60.	04.08.2010 II SA/Wa 2041/09	DOLiS/DEC-987/09/ 36100,36102,36104	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	oddalenie skargi
61.	10.08.2010 II SA/Wa 2122/09	DOLiS/DEC- 1052/09/ 38669,38673	Skarga na decyzję w przedmiocie odmowy uchylenia decyzji odmawiającej uwzględnienia wniosku w sprawie przetwarzania danych osobowych	oddalenie skargi
62.	17.08.2010 II SA/Wa 796/10	DOLiS/DEC-258/10/ 1097,10202,10205	Wniosek o zawieszenie postępowania	odmowa zawieszenia postępowania

63.	17.08.2010 I OSK 1426/09	DOLiS/DEC-731/08/ 31085,31088	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie umorzenia postępowania w sprawie wniosku o podjęcie działań przewidzianych ustawą o ochronie danych osobowych	uchylenie zaskarżonego wyroku
64.	18.08.2010 II SAB/Wa 83/10	DOLiS-440-714/09	Zwrot wpisu od skargi na bezczynność w przedmiocie rozpatrzenia wniosku dotyczącego przetwarzania danych osobowych	zwrot uiszczonego wpisu od skargi
65.	19.08.2010 II SA/Wa 386/10	DOLiS/DEC-94/10/ 3315,3319	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
66.	09.09.2010 II SA/Wa 790/10	DOLiS/DEC-249/10/ 9573	Skarga kasacyjna od postanowienia WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	odrzućenie skargi kasacyjnej
67.	14.09.2010 I OSK 1491/09	DOLiS/POST- 351/08/ 32706,32709	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na postanowienie w przedmiocie stwierdzenia niedopuszczalności wniosku o ponowne rozpatrzenie sprawy	oddalenie skargi kasacyjnej
68.	14.09.2010 I OSK 1529/09	DOLiS/DEC-10/09/ 372,376,379,381	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
69.	14.09.2010 I OSK 1479/09	DOLiS/DEC-64/09/ 2530,2532	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi kasacyjnej
70.	14.09.2010 I OSK 1464/09	DOLiS/DEC-900/08/ 35916,35912	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na nieprawidłowości w procesie przetwarzania danych osobowych	uchylenie zaskarżonego wyroku
71.	15.09.2010 II SA/Wa 1408/10	DOLiS/DEC-217/09/ 9959,9960,9962, 9964,9966,9967, 9970,9973,9978, 9981,9984,9987, 9993	Skarga o wznowienie postępowania zakończonego wyrokiem WSA w Warszawie oddalającym skargę na decyzję w przedmiocie przetwarzania danych osobowych	odrzućenie skargi o wznowienie postępowania
72.	15.09.2010 II SA/Wa 687/10	DOLiS/POST-34/10/ 7590,7593,7595	Skarga na postanowienie w przedmiocie wyłączenia z akt postępowania pisma	uchylenie zaskarżonego postanowienia
73.	23.09.2010 II SA/Wa 666/10	DOLiS/DEC-231/10/ 8744,8748,8757	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
74.	23.09.2010 II SA/Wa 543/10	DOLiS/DEC-135/10/ 5028,5029	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
75.	06.10.2010 II SA/Wa 446/10	GI-DEC-DS-117/05/ 330,331,332	Skarga o wznowienie postępowania w sprawie zakończonej postanowieniem WSA w Warszawie odrzucającym skargę na decyzję w przedmiocie ochrony danych osobowych	odrzućenie skargi o wznowienie postępowania
76.	08.10.2010 II SA/Wa 1378/10	DRZDO- POST/114/10/ 25973 dot. DRZDO- 401/004287/06	Odmowa przywrócenia terminu do uzupełnienia zgłoszenia zbioru danych osobowych	odrzućenie skargi
77.	12.10.2010 II SA/Wa 857/10	DOLiS/DEC-277/10/ 11458,11462,11466	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
78.	20.10.2010	DOLiS/DEC-459/10/	Skarga na decyzję w przedmiocie	odrzućenie skargi

	II SA/Wa 937/10	16901,16092,16906	udostępnienia danych osobowych	
79.	28.10.2010 II SA/Wa 786/10	DOLiS/DEC-515/08/ 22854,22857	Skarga na niewykonanie wyroku WSA w Warszawie wydanego w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	umorzenie postępowania
80.	29.10.2010 II SA/Wa 754/10	DOLiS/POST-41/10/ 8991,8992,8994, 8995,8996.	Skarga na postanowienie w przedmiocie odmowy sporządzenia i przesłania uwierzytelnionych kserokopii dokumentów z akt sprawy	uchylenie zaskarżonego postanowienia
81.	29.10.2010 II SA/Wa 1092/10	DOLiS/DEC-531/10/ 17993,17996,18002, 18008,18015	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
82.	29.10.2010 II SA/Wa 1562/10	DOLiS/DEC- 1008/10/31665	Skarga na decyzję w przedmiocie dostępu do informacji publicznej	odrzućenie skargi
83.	29.10.2010 II SA/Wa 1612/10	DOLiS/DEC- 1019/10/32609, 32620,32622	Skarga na decyzję w przedmiocie ochrony danych osobowych	odrzućenie skargi
84.	02.11.2010 II SA/Wa 1019/10	DOLiS/DEC-571/10/ 199486,19489,19493	Wniosek o sporządzenie uzasadnienia wyroku WSA w Warszawie	odmowa sporządzenia uzasadnienia wyroku
85.	03.11.2010 II SA/Wa 1118/10	DOLiS/DEC-553/10/ 18885,18894,18906	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
86.	05.11.2010 II SA/Wa 964/10	DOLiS/DEC-424/10/ 15798,15801,15805	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
87.	05.11.2010 II SA/Wa 965/10	DOLiS/POST-63/10/ 15823,15826,15829	Skarga na postanowienie w przedmiocie odmowy wydania dokumentów z akt postępowania dotyczącego ochrony danych	Uchylenie zaskarżonego postanowienia
88.	10.11.2010 II SA/Wa 786/10	DOLiS/DEC-515/08/ 22854,22857	Skarga na niewykonanie wyroku WSA w Warszawie wydanego w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	uchylenie punktu drugiego sentencji postanowienia
89.	15.11.2010 II SA/Op 515/10	DOLiS-035-1479/10/ 28746	Skarga na pismo w przedmiocie ochrony danych osobowych	przekazanie sprawy według właściwości
90.	15.11.2010 II SA/Wa 1477/10	DOLiS/DEC-731/08/ 31085,31088	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie wniosku o podjęcie działań przewidzianych ustawą o ochronie danych osobowych	uchylenie zaskarżonej decyzji
91.	19.11.2010 II SAB/Wa 220/10	DOLiS-440-152/10	Skarga na bezczynność w przedmiocie rozpoznania skargi w sprawie przetwarzania danych osobowych	zobowiązanie do rozpoznania skargi
92.	23.11.2010 II SA/Wa 1307/10	DOLiS/DEC-695/10/ 23507,23509,23510, 23511,23512	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie udostępnienia danych osobowych	uchylenie zaskarżonej decyzji
93.	01.12.2010 II SA/Wa 1212/10	DOLiS/DEC-835/10/ 26031,26035	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
94.	14.12.2010 II SAB/Wa 228/10	DOLiS-440-185/10	Skarga na bezczynność w przedmiocie rozpoznania skargi dotyczącej ochrony danych osobowych	zobowiązanie do rozpoznania skargi
95.	29.12.2010 II SAB/Wa 281/10	DOLiS-440-067- 09/10	Skarga na bezczynność w przedmiocie rozpoznania wniosku o udostępnienie informacji publicznej dotyczącej funkcjonowania organu	odrzućenie skargi

**Informacje przekazane przez organy ścigania  
w sprawach skierowanych w 2010 r.  
przez Generalnego Inspektora Ochrony Danych Osobowych  
zawiadomień o popełnieniu przestępstwa**

<b>Informacja</b>	<b>Rok 2008</b>	<b>Rok 2009</b>	<b>Rok 2010</b>
Umorzenie dochodzenia	18	11	14
Umorzenie dochodzenia w części	-	-	-
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	-	1	-
Umorzenie dochodzenia i odmowa podjęcia go na nowo	-	2	1
Wszczęcie dochodzenia	-	3	10
Odmowa wszczęcia dochodzenia	8	3	3
Wszczęcie śledztwa i jego umorzenie	-	-	-
Zawieszenie dochodzenia	-	-	1
Skierowanie sprawy do sądu	-	-	1
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	-	-	1
Brak informacji	5	-	1

## Wykaz szkoleń przeprowadzonych przez GIODO w 2010 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	11.01.2010	Warszawa	Kancelaria Sejmu RP
2.	12.01.2010	Warszawa	Dyrektorzy warszawskich placówek oświatowych
3.	18.01.2010	Warszawa	Dyrektorzy warszawskich placówek oświatowych
4.	18.01.2010	Warszawa	Ministerstwo Spraw Zagranicznych
5.	19.01.2010	Warszawa	Dyrektorzy warszawskich placówek oświatowych
6.	08.02.2010	Warszawa	Kancelaria Sejmu
7.	05.03.2010	Warszawa	Kancelaria Prezesa Rady Ministrów
8.	06.03.2010	Gliwice	Gliwicki Ośrodek Metodyczny
9.	09.03. 2010	Warszawa	Kancelaria Sejmu RP
10.	12.03.2010	Warszawa	Prokuratura Okręgowa w Warszawie
11.	16.03.2010	Warszawa	Urząd ds. Cudzoziemców
12.	18.03.2010	Warszawa	Urząd Komunikacji Elektronicznej
13.	19.03.2010	Kielce	Samorządowy Ośrodek Doradztwa Metodycznego i Doskonalenia Nauczycieli
14.	23.03.2010	Warszawa	Urząd ds. Cudzoziemców
15.	29.03.2010	Warszawa	Prokuratura Okręgowa w Warszawie
16.	01.04.2010	Warszawa	Kancelaria Prezesa Rady Ministrów
17.	09.04.2010	Warszawa	Prokuratura Okręgowa w Warszawie
18.	09.04.2010	Warszawa	Wojewódzki Urząd Pracy w Warszawie
19.	13.04.2010	Warszawa	Ministerstwo Finansów
20.	16.04.2010	Warszawa	Kancelaria Sejmu RP
21.	19.04.2010	Warszawa	Ministerstwo Spraw Zagranicznych
22.	22.04.2010	Warszawa	Prokuratura Okręgowa w Warszawie
23.	23.04.2010	Warszawa	Wojewódzki Urząd Pracy w Warszawie
24.	10.05.2010	Warszawa	Kancelaria Sejmu RP
25.	10.05.2010	Warszawa	Ministerstwo Spraw Wewnętrznych i Administracji
26.	13.05.2010	Warszawa	Ministerstwo Finansów, Departament Służby Celnej
27.	17.05.2010	Warszawa	Biuro Edukacji m. st. Warszawy
28.	18.05.2010	Warszawa	Narodowy Bank Polski
29.	20.05.2010	Gdańsk	Izba Skarbowa w Gdańsku
30.	20.05.2010	Gdynia	Izba Celna w Gdyni
31.	20.05.2010	Warszawa	Ministerstwo Finansów, Departament Izby Celnej
32.	24.05.2010	Warszawa	Kancelaria Sejmu RP

33.	25.05.2010	Warszawa	Kancelaria Sejmu RP
34.	26.05.2010	Warszawa	Ministerstwo Finansów, Departament Służby Celnej
35.	28.05.2010	Zgierz	Urząd Miasta Zgierz
36.	07.06.2010	Warszawa	Kuratorium Oświaty w Warszawie
37.	07.06.2010	Warszawa	Kancelaria Sejmu RP
38.	10.06.2010	Warszawa	Ministerstwo Finansów, Departament Służby Celnej
39.	11.06.2010	Warszawa	Ministerstwo Spraw Zagranicznych
40.	22.06.2010	Warszawa	Ministerstwo Finansów, Departament Kontroli Skarbowej
41.	30.06.2010	Warszawa	Kancelaria Sejmu RP
42.	06.07.2010	Warszawa	Mazowiecka Jednostka Wdrażania Programów Unijnych
43.	27.07.2010	Łódź	Izba Celna w Łodzi
44.	31.08.2010	Warszawa	Narodowe Centrum Kultury
45.	06.09.2010	Warszawa	Prokuratura Okręgowa Warszawa Praga
46.	07.09.2010	Warszawa	Prokuratura Okręgowa Warszawa Praga
47.	08.09.2010	Warszawa	Prokuratura Okręgowa Warszawa Praga
48.	15.09.2010	Warszawa	Ministerstwo Spraw Zagranicznych
49.	22.09.2010	Popowo	Służba Więzienna
50.	28-29.10.2010	Warszawa	Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji
51.	28-29.10.2010	Przemyśl	Sąd Okręgowy w Przemyślu
52.	03.11.2010	Warszawa	Kancelaria Prezesa Rady Ministrów
53.	15.11.2010	Warszawa	Okręgowa Izba Radców Prawnych w Lublinie
54.	22.11.2010	Warszawa	Ministerstwo Spraw Zagranicznych
55.	13.12.2010	Warszawa	Ministerstwo Spraw Zagranicznych

**Wykaz decyzji Generalnego Inspektora Ochrony Danych Osobowych  
wydanych w 2010 roku w sprawach o wyrażenie zgody  
na przekazanie danych osobowych do państwa trzeciego**

L.p.	Data wydania decyzji/postanowienia	Nazwa podmiotu	Sygnatura decyzji/postanowienia
1.	26.02.2010	ABN AMRO Bank Polska S.A.	DESIWM/DEC-226/8260/10 umorzenie postępowania
2.	16.03.2010	Bristol Myers Squibb Services Sp. z o.o.	DESIWM/DEC-274/11152/10 częściowe umorzenie postępowania ze względu na zbieranie zgód od osób, których dane dotyczą; w pozostałym zakresie zgoda na przekazanie danych
3.	16.03.2010	Bristol Myers Squibb Polska Sp. z o.o.	DESIWM/DEC-275/11155/10 częściowe umorzenie postępowania ze względu na zbieranie zgód od osób, których dane dotyczą; w pozostałym zakresie zgoda na przekazanie danych
4.	02.07.2010	Unilever Polska Sp. z o.o.	DESIWM/DEC-862/26544/10 zgoda na przekazanie danych
5.	02.07.2010	Unilever Polska S.A.	DESIWM/DEC-863/26545/10 zgoda na przekazanie danych
6.	02.07.2010	Unilever Poland Services Sp. z o.o.	DESIWM/DEC-864/26546/10 zgoda na przekazanie danych
7.	14.07.2010	Bird & Bird Maciej Gawroński Sp. K.	DESIWM/DEC-923/28317/10 zgoda na przekazanie danych
8.	14.07.2010	Bird & Bird Maciej Gawroński Sp. K.	DESIWM/DEC-922/28316/10 zgoda na przekazanie danych
9.	20.07.2010	Quad/Winkowski Sp. z o.o.	DESIWM/DEC-942/29117/10 zgoda na przekazanie danych
10.	29.07.2010	Skandia Życie Towarzystwo Ubezpieczeń S.A.	DESIWM/DEC-975/30184/10 zgoda na przekazanie danych
11.	10.08.2010	SMI Poland Sp. z o.o.	DESIWM/DEC-1009/31721/10 zgoda na przekazanie danych
12.	01.09.2010	American Express Poland S.A.	DESIWM/DEC-1052/34872/10 zgoda na przekazanie danych
13.	05.11.2010	Amgen Sp. z o.o.	DESIWM/DEC-1252/43926/10 zgoda na przekazanie danych
14.	05.11.2010	Flextronics International Poland Sp. z o.o.	DESIWM/DEC-1251/43916/10 zgoda na przekazanie danych
15.	05.11.2010	Bristol-Myers Squibb Services Sp. z o.o.	DESIWM/DEC-1250/43907/10 częściowe umorzenie postępowania ze względu na zbieranie zgód od osób, których dane dotyczą; w pozostałym zakresie zgoda na przekazanie danych
16.	05.11.2010	Bristol-Myers Squibb Polska Sp. z o.o.	DESIWM/DEC-1249/43865/10 częściowe umorzenie postępowania ze względu na zbieranie zgód od osób, których dane dotyczą; w pozostałym zakresie zgoda na

			przekazanie danych
17.	05.11.2010	PwC Polska Sp. z o.o.	DESIWM/DEC-1245/43944/10 częściowe umorzenie postępowanie w zakresie przekazania danych do: <ul style="list-style-type: none"> <li>• podmiotów, mających siedziby w Republice Bułgarii, w Republice Cypryjskiej, w Królestwie Niderlandów, w Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej, na Gibraltarze, na Nowej Kaledonii, na Polinezji Francuskiej, w Baliwacie Guernsey, w Baliwacie Jersey,</li> <li>• podmiotu należącego do amerykańskiego programu „bezpiecznej przystani” (ang. <i>Safe Harbour</i>),</li> <li>• podmiotu, mającego siedzibę w Meksykańskich Stanach Zjednoczonych, względem którego została już wcześniej wydana decyzja;</li> </ul> w pozostałym zakresie zgoda na przekazanie danych
18.	05.11.2010	PricewaterhouseCoopers Polska Sp. z o.o.	DESIWM/DEC-1246/43937/10 jak w pkt. 17 wykazu
19.	205.11.010	PricewaterhouseCoopers Sp. z o.o.	DESIWM/DEC-1248/43932/10 jak w pkt. 17 wykazu
20.	05.11.2010	Printpack Poland Sp. z o.o.	DESIWM/DEC-1247/43919/10 zgoda na przekazanie danych
21.	18.11.2010	Bird & Bird Maciej Gawroński Sp. K.	DESIWM/DEC-1272/45464/10 zgoda na przekazanie danych
22.	18.11.2010	UBS AG Przedstawicielstwo w Polsce	DESIWM/DEC-1273/45468/10 zgoda na przekazanie danych
23.	18.11.2010	UBS Service Centre (Poland) Sp. z o.o.	DESIWM/DEC-1274/45481/10 zgoda na przekazanie danych
24.	18.11.2010	UBS Fund Services (Luxembourg) S.A. Oddział w Polsce	DESIWM/DEC-1275/45491/10 zgoda na przekazanie danych
25.	24.11.2010	Pewlett-Packard Polska Sp. z o.o.	DESIWM/DEC-1296/46437/10 zgoda na przekazanie danych
26.	24.11.2010	Global E-Business Operations Sp. z o.o.	DESIWM/DEC-1297/46455/10 zgoda na przekazanie danych
27.	25.11.2010	Hewitt Associates Sp. z o.o.	DESIWM/DEC-1304/46667/10 zgoda na przekazanie danych
28.	20.12.2010	Mars Polska Sp. z o.o.	DESIWM/DEC-1384/50313/10 Zgoda na przekazanie danych
29.	20.12.2010	IBM Polska Sp. z o.o.	DESIWM/DEC-1385/50319/10 częściowe umorzenie postępowanie w zakresie przekazania danych do: <ul style="list-style-type: none"> <li>• podmiotów, mających siedziby w Republice Argentyńskiej oraz w Kanadzie,</li> <li>• podmiotu należącego do amerykańskiego programu „bezpiecznej przystani” (ang. <i>Safe Harbour</i>);</li> </ul> w pozostałym zakresie zgoda na przekazanie danych
30.	20.12.2010	IBM Polska Business Services Sp. z o.o.	DESIWM/DEC-1386/50332/10 jak w pkt. 29 wykazu
31.	20.12.2010	IBM BTO Business Consulting Services Sp. z o.o.	DESIWM/DEC-1387/50339/10 jak w pkt. 29 wykazu
32.	20.12.2010	IBM Global Services Delivery Centre Polska Sp. z o.o.	DESIWM/DEC-1389/50349/10 jak w pkt. 29 wykazu
33.	30.12.2010	3M Poland Sp. z o.o. Oddział w Rabce	DESIWM/DEC-1415/51760/10



			częściowe umorzenie postępowanie w zakresie przekazania kategorii danych wykraczających poza art. 22 <sup>1</sup> ustawy z dnia 26 czerwca 1974 r. Kodeks pracy – Dz. U. z 1974 r., Nr 24 poz. 141 z późn. zm; w pozostałym zakresie zgoda na przekazanie danych
34.	30.12.2010	3M Poland Sp. z o.o. Oddział w Janowie	DESiWM-DEC-1416/51768/10 jak w pkt. 33 wykazu
35.	30.12.2010	3M Wrocław Sp. z o.o.	DESiWM/DEC-1417/51763/10 zgoda na przekazanie danych
36.	30.12.2010	3M Poland Sp. z o.o.	DESiWM/DEC-1418/51764/10 jak w pkt. 33 wykazu
37.	30.12.2010	3M Poland Sp. z o.o. Oddział we Wrocławiu	DESiWM/DEC-1419/51765/10 jak w pkt. 33 wykazu