

**Generalny Inspektor
Ochrony Danych Osobowych**

**SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH
W ROKU 2011**

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 osobowych¹.

¹ Niniejsze *Sprawozdanie* obejmuje okres działalności Generalnego Inspektora Ochrony Danych Osobowych od 1 stycznia 2011 r. do 31 grudnia 2011 r.

SPIS TREŚCI

Wprowadzenie	5
Część I. Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych	7
1. Informacje ogólne	7
2. Biuro Generalnego Inspektora Ochrony Danych Osobowych	9
2.1. Struktura organizacyjna	9
2.2. Pracownicy Biura GIODO	10
2.3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2011 rok	11
Część II. Stan wiedzy i przestrzegania przepisów o ochronie danych osobowych	12
1. Informacje ogólne	12
2. Kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych	14
2.1. Czynności kontrolne	14
2.2. Kontrola przetwarzania danych osobowych w wybranych obszarach	15
1) Administracja publiczna	15
2) Bezpieczeństwo publiczne	17
3) Banki i inne instytucje finansowe	19
4) Służba zdrowia	21
5) Zatrudnienie	24
6) Imprezy masowe organizowane na stadionach	28
7) Telekomunikacja	30
8) Przedszkola	34
9) Inne	37
2.3. Systemy informatyczne służące do przetwarzania danych osobowych	42
2.4. Wyniki kontroli w zakresie wypełnienia obowiązków formalnych i organizacyjnych	43
2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych	46
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych	50
3.1. Wydawanie decyzji	50
3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa	51

3.3.	Rozpatrywanie skarg	53
4.	Prowadzenie rejestru zbiorów danych osobowych oraz udzielanie informacji o zarejestrowanych zbiorach	78
5.	Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych	90
6.	Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych	140
6.1.	Interpretacja przepisów	141
6.1.1.	Odpowiedzi na pytania traktujące o danych wrażliwych nt. zdrowia	141
6.1.2.	Przetwarzanie danych osobowych – wybrane problemy	150
6.1.3.	Wystąpienia	160
6.2.	Działalność informacyjna	177
6.2.1.	Współpraca ze środkami masowego przekazu	178
6.2.2.	Publikacje	183
6.2.3.	Szkolenia	184
6.2.4.	Konkursy	186
6.2.5.	Projekty i programy	187
6.2.6.	Konferencje, seminaria, spotkania	190
6.2.7.	Internet	199
6.2.8.	Porozumienia o współpracy	200
6.2.8.	Inne informacje	201
7.	Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych	202
7.1.	Międzynarodowe spotkania i konferencje	208
7.2.	Wizyty robocze	215
7.3.	Międzynarodowe warsztaty	215
Część III.	Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2011 roku	217
Część IV.	Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych	246

Załączniki

Załącznik nr 1	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2011 o charakterze generalnym do centralnych organów państwa i do innych podmiotów sektora publicznego	260
Załącznik nr 2	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2011 do podmiotów prywatnych	263
Załącznik nr 3	Wykaz kontroli przeprowadzonych w 2011 roku	265
Załącznik nr 4	Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2011 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych	275
Załącznik nr 5	Informacje przekazane przez organy ścigania w sprawach skierowanych w 2011 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa	282
Załącznik nr 6	Wykaz szkoleń przeprowadzonych przez GIODO w 2011 r.	283
Załącznik nr 7	Wykaz wydarzeń objętych patronatem GIODO w 2011 r.	285
Załącznik nr 8	Wykaz konferencji, seminariów i spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2011 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty	287
Załącznik nr 9	Wykaz konferencji, seminariów i spotkań międzynarodowych z udziałem GIODO lub jego przedstawicieli, które odbyły się w 2011 r. za granicą	291
Załącznik nr 10	Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych wydanych w 2011 r. w sprawach o wyrażenie zgody na przekazanie danych osobowych za granicę	293

SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2011

Wprowadzenie

Rok 2011, pierwszy pełny rok kalendarzowy działalności Generalnego Inspektora Ochrony Danych Osobowych IV kadencji, obfitował w ważne wydarzenia związane z ideą i misją organu ds. ochrony danych osobowych. Pierwszym z nich było wejście w życie z dniem 7 marca 2011 r. – po prawie trzech latach intensywnych prac - znowelizowanej ustawy o ochronie danych osobowych.

Pierwsze zmiany w ustawie o ochronie danych osobowych wprowadziła ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), obowiązująca od 2 stycznia 2011 r. Zmiany te dotyczyły rejestracji zbiorów, odmowy udostępnienia danych i obowiązku informacyjnego. Natomiast przepisy, które weszły w życie 7 marca 2011 r. przyznały Generalnemu Inspektorowi Ochrony Danych Osobowych uprawnienia organu egzekucyjnego w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym (art. 12 pkt 3), prawo kierowania do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, jak również innych jednostek organizacyjnych oraz do osób fizycznych i prawnych, wystąpień zmierzających do zapewnienia skutecznej ochrony danych osobowych, a także prawo występowania do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Podmioty, do których zostało skierowane przez GODO wystąpienie lub wnioski będą zobowiązane ustosunkować się do nich w terminie 30 dni od daty jego otrzymania. Ponadto za udaremnianie lub utrudnianie wykonywania czynności kontrolnych przez inspektorów GODO będzie groziła kara grzywny, ograniczenia wolności albo pozbawienia wolności do 2 lat. Nowe regulacje wprowadzone zostały ustawą z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. Nr 229, poz. 1497).

Drugim ważnym wydarzeniem, którego uczestnikiem był organ ds. ochrony danych osobowych, było zakończenie w 2011 r. trwających ponad dwa lata konsultacji nad strategią poprawy skuteczności unijnych przepisów dotyczących ochrony danych, opracowaną przez Komisję Europejską. Strategia ta zakładała przemodelowanie istniejących na poziomie Unii Europejskiej ram prawnych w zakresie ochrony danych osobowych, tj. dyrektywy 95/46/WE o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnym przepływie tych danych, a także

podjęcie działań pozalegisłacyjnych mających na celu skuteczniejszą ochronę danych osobowych w UE (np. poprzez wspieranie kampanii na rzecz podnoszenia świadomości w zakresie ochrony danych i korzystania z nich, jak również ewentualne inicjatywy w zakresie samoregulacji podejmowane przez sektor przemysłu). Planowane działania stanowiły odpowiedź na wyzwania związane z rozwojem nowoczesnych technologii informatycznych oraz procesami globalizacji, wymuszając niejako modernizację unijnej polityki ochrony danych osobowych w kierunku wzmocnienia praw jednostek, przy jednoczesnym zapewnieniu swobodnego przepływu danych w ramach jednolitego rynku UE poprzez znoszenie barier biurokratycznych.

W wyniku tych prac przygotowany został pakiet zmian regulacji UE w zakresie ochrony danych osobowych. Wśród nich planowane jest zastąpienie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych **rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych**. Rozporządzenie to obowiązywać będzie bezpośrednio w krajach członkowskich, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Dzięki jego wprowadzeniu nastąpiłaby pełna harmonizacja prawa materialnego w ramach UE i swobodnego przepływu tych danych. Natomiast nowością w polskim systemie prawnym będzie **dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych**. Zasady zawarte w zaprezentowanym projekcie nie są obecne w istniejących dziś polskich przepisach prawa.

Generalny Inspektor Ochrony Danych Osobowych jest konstytucyjnym organem do spraw ochrony danych osobowych i prawa do prywatności. Jego zadania i kompetencje wyznaczają przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.). W ich świetle GIODO jest uprawniony do:

- kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- zapewnienia wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z wydanych decyzji, przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.),
- prowadzenia rejestru zbiorów danych oraz udzielania informacji o zarejestrowanych zbiorach,

- opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenia w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

W przypadku naruszenia przepisów o ochronie danych osobowych, Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności: usunięcie uchybień, uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych, zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe, wstrzymanie przekazywania danych osobowych do państwa trzeciego, zabezpieczenie danych lub przekazanie ich innym podmiotom, usunięcie danych osobowych.

W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

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 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 225, poz. 1350). Rozporządzenie to było poprzedzone rozporządzeniem Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 203, poz. 1494), które utraciło moc z dniem 7 marca 2011 r. na podstawie art. 1 pkt 3 lit. B ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. Nr 229, poz. 1497).

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, które weszły 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.)².

Unijne przepisy z zakresu ochrony danych osobowych, w tym ww. dyrektywa 95/46/WE, służą ochronie podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych oraz swobodnego ich przepływu. Ta ogólna dyrektywa została uzupełniona innymi instrumentami prawnymi, takimi jak np. dyrektywą 2002/58/WE o prywatności i łączności elektronicznej. Istnieją poza tym przepisy szczególne dotyczące ochrony danych osobowych przetwarzanych w ramach współpracy policji i wymiaru sprawiedliwości w sprawach karnych (np. decyzja ramowa 2008/977/WSiSW). Prawo do ochrony danych osobowych zostało jednoznacznie uznane jako jedno z praw podstawowych w art. 8 Karty Praw Podstawowych Unii Europejskiej oraz w Traktacie

² Więcej na ten temat będzie mowa w dalszej części niniejszego Sprawozdania.

Lizbońskim. Art. 16 Traktatu stanowi podstawę prawną dla przepisów o ochronie danych osobowych odnośnie do wszystkich działań w ramach prawa UE.

Podkreślenia wymaga również, że na system ochrony danych osobowych składają się też przepisy szczególne innych ustaw, które regulują kwestie związane z przetwarzaniem danych osobowych przez różne podmioty. Podmioty publiczne, w myśl zasady praworządności wyrażonej w art. 7 Konstytucji Rzeczypospolitej Polskiej, działają wyłącznie na podstawie i w granicach prawa. Oznacza to, że mogą one przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu określonych prawem zadań, obowiązków i upoważnień.

2. Biuro Generalnego Inspektora Ochrony Danych Osobowych

2.1 Struktura organizacyjna

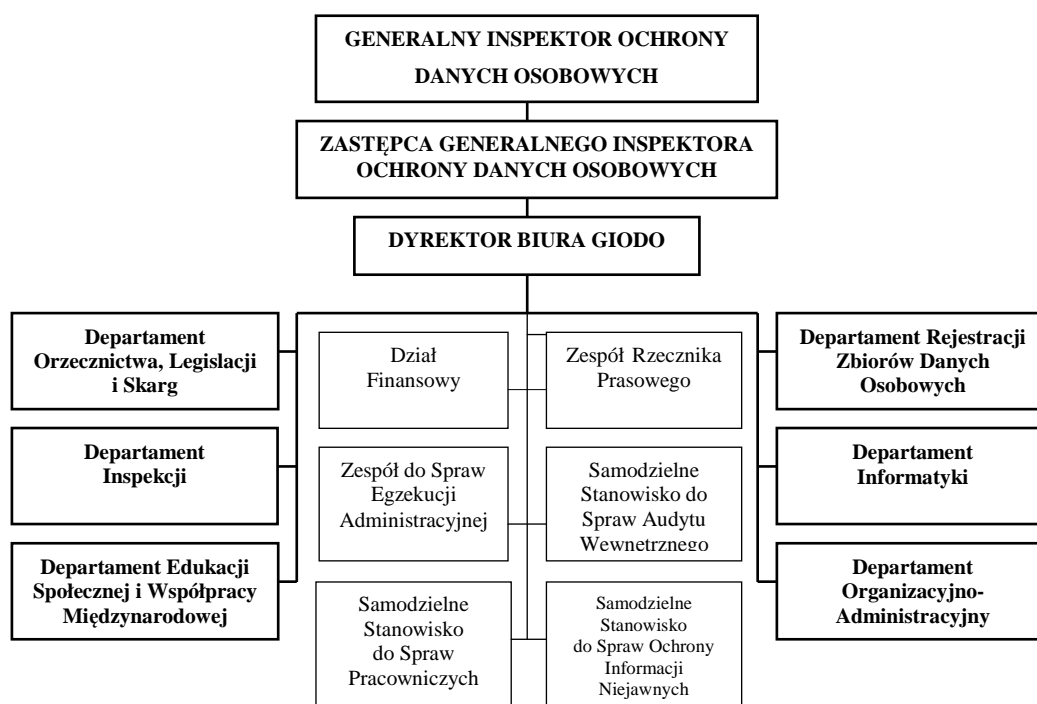
Zgodnie z art. 13 ust. 1 ustawy o ochronie danych osobowych, Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. W przypadkach uzasadnionych charakterem i liczbą spraw z zakresu ochrony danych osobowych na danym terenie, może wykonywać swoje zadania przy pomocy jednostek zamiejscowych. Tryb pracy Biura, a także organizację wewnętrzną i szczegółowy zakres zadań statutowych jednostek organizacyjnych oraz jednostek zamiejscowych Biura określa Generalny Inspektor w Regulaminie Organizacyjnym.

Prezydent Rzeczypospolitej Polskiej, po zasięgnięciu opinii Generalnego Inspektora, w drodze rozporządzenia nadaje statut Biuru, określając jego organizację, zasady działania, siedziby jednostek zamiejscowych oraz zakres ich właściwości terytorialnej, mając na uwadze stworzenie optymalnych warunków organizacyjnych do prawidłowej realizacji zadań Biura.

Organizacja oraz zasady działania Biura określone zostały w statucie stanowiącym załącznik do rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. 2011, Nr 225, poz. 1350). Na mocy tego aktu powołano nową jednostkę organizacyjną Biura GIODO – Zespół do Spraw Egzekucji Administracyjnej (ZEA), a także ustalone zostały siedziby oraz właściwość miejscowa jednostek zamiejscowych:

- 1) Jednostka Zamiejscowa Biura Ochrony Danych Osobowych w Katowicach, obejmująca obszar województwa śląskiego, opolskiego, dolnośląskiego, małopolskiego i podkarpackiego;
- 2) Jednostka Zamiejscowa Biura Ochrony Danych Osobowych w Gdańsku, obejmująca obszar województwa pomorskiego, warmińsko-mazurskiego i zachodniopomorskiego.

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



Struktura Biura Generalnego Inspektora Ochrony Danych Osobowych – stan na dzień składania Sprawozdania

Generalny Inspektor wykonuje swoje zadania bezpośrednio lub przy pomocy Dyrektora Biura, dyrektorów jednostek organizacyjnych Biura oraz innych osób wskazanych w Regulaminie Organizacyjnym.³

2.2. Pracownicy Biura GODO

Stan zatrudnienia w Biurze GODO w przeliczeniu na pełne etaty wynosił na dzień 1 stycznia 2011 r. – 126,9 etatów, zaś na dzień 31 grudnia 2011 r. – 126,5 etatów. Na stanowiskach merytorycznych zatrudnionych było 111 osób, a na stanowiskach pomocniczych 20 osób. Wyższe wykształcenie posiadało 116 pracowników, w tym 76 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GODO na koniec 2011 r. przedstawia się następująco:

- GODO - 1 osoba
- Zastępca GODO – 1 osoba
- Dyrektor Biura – 1 osoba
- Zespół Rzecznika Prasowego (ZRP) – 5 osób

³ Zarządzenie Nr 1/2012 Generalnego Inspektora Ochrony Danych Osobowych z dnia 04 stycznia 2012 r. w sprawie wprowadzenia Regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych.

- Departament Edukacji Społecznej i Współpracy Międzynarodowej (DESiWM) – 10 osób
- Departament Informatyki (DIF) – 15 osób,
- Departament Inspekcji (DIS) – 18 osób,
- Departament Orzecznictwa, Legislacji i Skarg (DOLiS) – 34 osoby,
- Departament Rejestracji Zbiorów Danych Osobowych (DRZDO) – 17 osób,
- Departament Organizacyjno-Administracyjny (DOA) – 17 osób,
- Dział Finansowy – 3 osoby
- Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby
- Samodzielne Stanowisko ds. Pracowniczych – 2 osoby
- Samodzielne Stanowisko ds. Audytu – 1 osoba
- Radcy Prawni – 2 osoby

Przedstawiona powyżej struktura zatrudnienia pracowników w poszczególnych jednostkach organizacyjnych Biura GIODO dotyczy stanu z dnia 31 grudnia 2011 r. Z uwagi na to, że nowy Regulamin Organizacyjny Biura Generalnego Inspektora Ochrony Danych Osobowych stanowiący załącznik nr 1 do Zarządzenia Nr 1/2012 wszedł w życie z dniem 4 stycznia 2012 r.⁴, nie ma w niej wyodrębnionej nowej jednostki organizacyjnej – Zespołu do Spraw Egzekucji Administracyjnej (ZEA).

Obecny stan zatrudnienia w Biurze Generalnego Inspektora Ochrony Danych Osobowych umożliwia realizowanie zadań powierzonych ustawowo, lecz zauważalny wzrost liczby prowadzonych spraw powoduje, że mimo podwyższenia w znaczącym stopniu sprawności prowadzenia postępowań, w najbliższym czasie muszą nastąpić opóźnienia w wydawaniu decyzji i postanowień oraz w wykonywaniu działań materialno-technicznych.

Należy bowiem zwrócić uwagę, że **przy braku wzrostu zatrudnienia w Biurze w ostatnim roku:**

- **o 50 % wzrosła** liczba wydanych decyzji w postępowaniach zainicjowanych skargami (z 359 w 2010 r. do 539 w 2011 r.),
- **o 11 % wzrosła** liczba zgłoszonych skarg w ostatnim roku (z 1114 w 2010 r. do 1271 w 2011 r.) i **o 59 % w ciągu ostatnich 5 lat** (z 796 w 2007 r.)

⁴ Z tym dniem straciło moc 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.

- o **89 % wzrosła** liczba zbiorów zgłoszonych do rejestracji (z 8260 w 2010 r. do 15.643 w 2011 r.), a w ciągu ostatnich 5 lat nastąpił **ponad trzykrotny wzrost** liczby zgłaszanych rocznie zbiorów (z 4850 w 2007 r.⁵).

Poważnym problemem dla Biura jest również fakt, że brak możliwości motywowania najlepszych pracowników zmianami w wynagrodzeniu powoduje stały odpływ najlepszych urzędników – w szczególności prawników i informatyków do sektora prywatnego z chęcią korzystającego z dobrze wykształconych pracowników zajmujących się newralgiczną dziedziną jaką jest bezpieczeństwo informacyjne.

2.3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2011 rok

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2011 r. wynosił: **14 700** tys. zł, w tym:

wynagrodzenia i pochodnie od wynagrodzeń	10 764 tys. zł
wydatki majątkowe	400 tys. zł
pozostałe wydatki	3 536 tys. zł

Wydatki zrealizowane przez GIODO w 2011 roku w kwocie **14 435** tys. zł obejmowały:

wynagrodzenia i pochodne od wynagrodzeń	10 729 tys. zł
wydatki majątkowe	399 tys. zł
pozostałe wydatki	3 307 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

⁵ O tym, że podjęto w Biurze GIODO zmiany organizacyjne, które usprawniły rozpatrywanie spraw świadczyć może natomiast fakt, że liczba rejestrowanych rocznie zbiorów wzrosła w tym samym okresie z 2598 w 2007 r. do 11.845 w 2011 r. - wzrost o 356 %).

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 danych⁶. 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.

Ustawa daje obywatelom możliwość skorzystania z prawa do formalnej kontroli przetwarzania dotyczących ich danych, które ustanowione jest w rozdziale 4 ustawy. Mogą oni domagać się również: uzyskania informacji, czy zbiór danych istnieje, ustalenia administratora danych, adresu jego siedziby, uzyskania informacji o celu, zakresie i sposobie przetwarzania danych oraz informacji o źródle, z którego pochodzą, żądania uzupełnienia, uaktualnienia, sprostowania, a nawet czasowego lub stałego wstrzymania przetwarzania danych, jeżeli są one nieaktualne, niekompletne, nieprawdziwe lub zostały zebrane z naruszeniem prawa albo są już zbędne do realizacji celu, dla którego były zebrane. Ustawa przyznaje obywatelom także prawo do sprzeciwu, gdy administrator przetwarza dane w celach innych niż te, dla których były zbierane lub przekazuje je innemu administratorowi danych. W takiej sytuacji przysługuje im prawo żądania od administratora danych odpowiedniego zachowania się w przypadku nieprzestrzegania ustawy, a także prawo występowania do Generalnego Inspektora Ochrony Danych

⁶ 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.

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 obywateli 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).

Jak już była o tym mowa, zgodnie z brzmieniem art. 12 ustawy Generalny Inspektor w szczególności kontroluje zgodność przetwarzania danych z przepisami o ochronie danych osobowych, wydaje decyzje administracyjne i rozpatruje skargi w sprawach wykonania przepisów o ochronie danych osobowych, zapewnia wykonanie przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji przez stosowanie przewidzianych przepisami prawa środków egzekucyjnych określonych w ustawie o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.), prowadzi ogólnokrajowy, jawny rejestr zbiorów danych oraz udziela informacji o zarejestrowanych zbiorach, opiniuje projekty ustaw i rozporządzeń dotyczących ochrony danych osobowych, inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych, a także uczestniczy w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

Należy podkreślić, że wśród wymienionych zadań GIODO wynikających z art. 12 nowością są te dotyczące spraw egzekucji administracyjnej. Wskutek wspomnianej wcześniej nowelizacji ustawy o ochronie danych osobowych, Generalny Inspektor wykonuje zadania związane z wszczynaniem i prowadzeniem postępowań egzekucyjnych o charakterze niepieniężnym, oraz zadania związane z wszczynaniem i monitorowaniem postępowań egzekucyjnych o charakterze pieniężnym przy realizacji których współpracuje w tym zakresie z naczelnikami urzędów skarbowych.

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 przesłuchiwanie osób w zakresie niezbędnym do ustalenia stanu faktycznego, wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii, przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych, 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 uzasadniać żądanie wszczęcia postępowania dyscyplinarnego przeciwko osobom winnym dopuszczenia do uchybień.

2.2. Kontrola przetwarzania danych osobowych w wybranych obszarach

W 2011 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził łącznie **199 kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych.

1) Administracja publiczna

W 2011 r. przeprowadzono **21 kontroli w podmiotach należących do administracji publicznej**, w tym w szczególności w urzędach gmin, miast, powiatów i województw, urzędach centralnych oraz służbach.

Do bardzo interesujących kontroli należała kontrola jednego z urzędów gmin⁷. W jej toku ustalono, że gmina zawarła umowę z podmiotem prywatnym (spółką), w której zleciła świadczenie usług polegających na „wykonaniu dokumentacji pomocniczej dla dokumentacji prowadzonej przez Straż Gminną przy pomocy urządzenia do pomiarów i rejestracji prędkości w sprawie postępowania mandatowego prowadzonego w związku ze stwierdzonymi wykroczeniami polegającymi na przekraczaniu dozwolonej prędkości, zarejestrowanymi za pomocą urządzeń do samoczynnego pomiaru i rejestracji prędkości pojazdów”. Zgodnie z umową zleczone usługi obejmowały: 1) wygenerowanie cyfrowych zdjęć wizerunku kierowcy wraz z pojazdem, przy pomocy którego popełnił wykroczenie polegające na przekroczeniu dozwolonej prędkości, zarejestrowane za pomocą urządzenia do pomiaru i rejestracji prędkości, tzw. fotoradaru, 2) wydruk w dwóch egzemplarzach w/w fotografii wraz z następującymi informacjami tj.: tablicą rejestracyjną pojazdu, którym popełniono wykroczenie drogowe, miejscem zdarzenia, datą oraz godziną i minutą zdarzenia, zarejestrowaną prędkością pojazdu oraz prędkością dopuszczalną, obrazem twarzy kierowcy w przypadku pojazdów nadjeżdżających oraz danymi personalnymi właściciela pojazdu, 3) przygotowanie dokumentacji stwierdzonego zdarzenia, która będzie podstawą do wszczęcia postępowania mandatowego, i która składać się będzie z raportu ze zdarzenia (fotografia planu ogólnego przedstawiająca: twarz kierowcy, tablicę rejestracyjną pojazdu, czas i miejsce zdarzenia, prędkość dopuszczalną i zmierzoną, dane osobowe właściciela pojazdu) dla pojazdów nadjeżdżających j.w. lecz bez twarzy kierowcy, dla pojazdów odjeżdżających, wezwania właściciela pojazdu do złożenia wyjaśnień i oświadczeń, 4) wydruk treści mandatu na oryginalnych bloczkach mandatowych, 5) archiwizowanie wykonanych dokumentacji na nośnikach optycznych (CD) oraz przekazanie ich zamawiającemu, 6) użyczenie fotoradaru.

Jak ustalono, w związku z wykonywaniem czynności określonych w ww. umowie, pracownicy spółki mieli dostęp do danych osobowych pozyskanych przez Straż Gminną w wyniku

⁷ DIS-K-421/123/10

wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia drogowe, w tym do danych osobowych właścicieli pojazdów, którymi popełniono wykroczenie drogowe, sprawców tych wykroczeń oraz osób podejrzanych o ich popełnienie. Biorąc pod uwagę obowiązujące przepisy w tym zakresie Generalny Inspektor Ochrony Danych Osobowych podniósł, iż zlecone spółce czynności polegające na: przygotowywaniu zapytań do Centralnej Ewidencji Pojazdów i Kierowców (CEPIK) o dane właścicieli pojazdów, którymi popełniono wykroczenia drogowe, wprowadzaniu do systemu informatycznego danych osobowych użytkowników pojazdów, bądź sprawców wykroczeń przekazanych Straży Gminnej przez właścicieli pojazdów, a następnie przygotowywaniu dokumentacji dotyczącej stwierdzonego zdarzenia polegającego na przekroczeniu dozwolonej prędkości przez kierującego pojazdem, w tym m.in.: raportu ze zdarzenia, wezwania właściciela pojazdu do złożenia wyjaśnień i oświadczeń, które są następnie kierowane do użytkownika pojazdu lub domniemanego sprawcy wykroczenia, mają na celu bezpośrednio ustalenie tożsamości sprawcy wykroczenia drogowego w celu wystawienia mandatu karnego, ewentualnie skierowania wniosku o ukaranie sprawcy wykroczenia do sądu i stanowią tym samym czynności wyjaśniające w sprawach o wykroczenia. Tymczasem w świetle art. 12 ust. 1 pkt 4 i 5 ustawy z dnia 29 sierpnia 1997 r. o Strażach Gminnych (Dz. U. z 1997 r. Nr 123, poz. 779)⁸ zadania polegające m.in. na: prowadzeniu czynności wyjaśniających w sprawach o wykroczenia, przygotowywaniu mandatów karnych, przygotowywaniu wniosków o ukaranie do sądu w trybie i zakresie określonym w Kodeksie postępowania w sprawach o wykroczenia, w tym również ewidencjonowanie spraw prowadzonych przez Straż, są czynnościami zastrzeżonymi dla Straży Gminnej. Zlecenie tego rodzaju zadań podmiotowi prywatnemu było zatem pozbawione podstaw prawnych i doprowadziło do przekazania temu podmiotowi kompetencji Straży Gminnej w ww. zakresie. Podobnie Generalny Inspektor ocenił zlecenie podmiotowi prywatnemu zadań w zakresie przygotowywania (wypełniania) kart rejestracyjnych (PRD-5), do których wykonywania, w myśl obowiązujących przepisów prawa⁹ w Straży Gminnej uprawnieni są jedynie jej funkcjonariusze, którzy zastosowali postępowanie mandatowe lub prowadzą postępowanie w sprawie o naruszenie przepisów prawa.

W związku z tym, że wraz z przekazaniem spółce ww. zadań Straży Gminnej zostały jej przekazane dane osobowe pozyskane przez ten podmiot w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia drogowe, w tym m.in. dane właścicieli pojazdów, sprawców wykroczeń drogowych polegających na przekroczeniu dozwolonej prędkości oraz

⁸ Art. 12 ust. 1 pkt 4 i pkt 5. Strażnik wykonując zadania, o których mowa w art. 10 i art. 11, ma prawo do nakładania grzywnien w postępowaniu mandatowym za wykroczenia określone w trybie przewidzianym przepisami o postępowaniu w sprawach o wykroczenia; dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych – w trybie i zakresie określonym w Kodeksie postępowania w sprawach o wykroczenia.

⁹ § 4 ust. 10 w zw. z § 4 ust. 7 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 20 grudnia 2002 r. w sprawie postępowania z kierowcami naruszającymi przepisy ruchu drogowego, Dz. U. z 2002 r. Nr 236, poz. 1998.

osób podejrzanych o popełnienie tego rodzaju wykroczeń, w celu wykonywania zleconych zadań, Generalny Inspektor uznał, że dane te były przetwarzane niezgodnie z prawem, co stanowi naruszenie art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych¹⁰, bowiem dane były przetwarzane przez osoby do tego nieuprawnione.

Generalny Inspektor uznał natomiast, iż dopuszczalne jest powierzenie przetwarzania danych osobowych przez Straż Gminną podmiotowi prywatnemu jedynie w celu wykonywania czynności z zakresu obsługi techniczno-organizacyjnej, takich jak: użyczenie fotoradaru, przygotowanie fotoradaru do kontroli pod względem technicznym, zgranie obrazów z fotoradaru na dysk komputera obsługującego to urządzenie, utworzenie kopii nagrań zarejestrowanych przez fotoradar na płycie CD lub DVD, czy opracowanie zdjęć z fotoradaru pod względem graficznym. W toku kontroli ustalono, że weryfikacja zdjęć z fotoradarów pod kątem możliwości ich wykorzystania jako materiału dowodowego była zawsze dokonywana przez strażnika Straży Gminnej.

W związku z uchybieniami stwierdzonymi w toku kontroli wydana została decyzja¹¹, w której nakazano usunięcie uchybień w procesie przetwarzania danych osobowych oraz umorzono postępowanie w zakresie nieprawidłowości usuniętych przez jednostkę kontrolowaną w toku postępowania.

2) Bezpieczeństwo publiczne

W 2011 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził **10 kontroli przetwarzania danych osobowych w Krajowym Systemie Informatycznym (KSI)** umożliwiającym organom administracji publicznej i organom wymiaru sprawiedliwości wykorzystywanie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym.

Bardzo istotne znaczenie, jeśli chodzi o przetwarzanie danych osobowych w Krajowym Systemie Informatycznym, miała kontrola przeprowadzona u Komendanta Głównego Policji pełniącego rolę Centralnego Organu Technicznego KSI. Kontrola ta miała związek z uruchomieniem w dniu 11 października 2011 r. Wizowego Systemu Informacyjnego¹² przez państwa należące do strefy Schengen. Zgodnie z art. 34 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. Nr 1170, poz. 165 z późn. zm.), w przypadku dokonywania jakichkolwiek zmian w Krajowym Systemie Informatycznym po jego uruchomieniu, centralny organ techniczny Krajowego Systemu Informatycznego jest zobowiązany przed wdrożeniem tych zmian do uzyskania opinii Generalnego

¹⁰ Art. 26 ust. 1 pkt 1. 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.

¹¹ DIS/DEC-689/39637/11

¹² DIS-K-421/155/11

Inspektora Ochrony Danych Osobowych w zakresie i w trybie określonym w art. 29 – 32 wskazanej ustawy¹³. Na podstawie złożonego przez Komendanta Głównego Policji wniosku, o którym mowa w art. 34 powołanej ustawy, w związku z dokonywanymi zmianami w KSI polegającymi na uruchomieniu Wizowego Systemu Informacyjnego, została przeprowadzona kontrola, tak jak tego wymagają wskazane przepisy, w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 36-39 ustawy o ochronie danych osobowych oraz w przepisach wydanych na podstawie art. 39a tej ustawy, tj. dotyczących zabezpieczenia danych osobowych.

W opinii Generalnego Inspektora wydanej na podstawie art. 30 ust. 5 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym stwierdzono, że Krajowy System Informatyczny wykorzystywany jako interfejs krajowy Wizowego Systemu Informacyjnego spełniał wymogi określone we ww. przepisach.

W Komendzie Głównej Policji (w tym w Biurze SIRENE - jednostce wyodrębnionej w ramach struktury organizacyjnej Komendy Głównej Policji) zostały także przeprowadzone kontrole obejmujące zakresem przetwarzanie danych osobowych w Systemie Informacyjnym Schengen¹⁴. Wspomniane kontrole dotyczyły w szczególności stosowania art. 99 Konwencji, tj. gromadzenia danych do celów niejawnego nadzoru lub szczególnych kontroli, w celach ścigania przestępstw oraz zapobiegania zagrożeniom dla bezpieczeństwa publicznego, a także przetwarzania danych we wpisach wprowadzonych zgodnie z prawem krajowym na wniosek organów odpowiedzialnych za bezpieczeństwo narodowe. Na podstawie wyników przeprowadzonych kontroli zostało wszczęte postępowanie administracyjne zakończone wydaniem decyzji administracyjnej nakazującej, m.in. uzupełnienie dokumentacji stanowiącej politykę bezpieczeństwa.

W zakresie przetwarzania danych osobowych w Krajowym Systemie Informatycznym, w analizowanym 2011 roku zostały również dokonane czynności kontrolne w Urzędzie do Spraw Cudzoziemców¹⁵, w związku z wykonywaniem przez Generalnego Inspektora Ochrony Danych Osobowych obowiązków organu nadzorczego, o którym mowa w art. 114 ust. 1 Konwencji Wykonawczej do Układu z Schengen z dnia 14 czerwca 1985 roku między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. UE L z 2000 r. Nr 239, poz. 19 z późn. zm.), zwanej dalej Konwencją. Generalny Inspektor odpowiedzialny jest za sprawowanie niezależnego nadzoru nad danymi krajowego modułu Systemu Informacyjnego Schengen (SIS) oraz –

¹³ Art. 30 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Centralny organ techniczny KSI, przed uruchomieniem Krajowego Systemu Informatycznego (KSI), jest obowiązany do wystąpienia do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o przeprowadzenie kontroli w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz w przepisach wydanych na podstawie art. 39a tej ustawy.

¹⁴ DIS-K-421/137/11, DIS-K-421/146/11.

¹⁵ DIS-K-421/20/11

o czym stanowi również art. 8 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym - za kontrolę, czy przetwarzanie i wykorzystywanie danych wprowadzanych do SIS nie narusza praw osób, których dane te dotyczą. Zakresem kontroli objęto sprawdzenie, czy wykorzystywanie przez Szefa Urzędu do Spraw Cudzoziemców danych osobowych obywatela obcego państwa, przetwarzanych w Krajowym Systemie Informatycznym, nie narusza praw osób, których dane dotyczą, a w szczególności, na jakiej podstawie dokonano wpisu tych danych do SIS. Kontrola została przeprowadzona ze względu na konieczność uzupełnienia materiału dowodowego zebranego w toku postępowania administracyjnego w sprawie legalności przetwarzania danych ww. osoby w Systemie Informacyjnym Schengen, prowadzonego na skutek złożonej skargi. Kontrola wykazała, iż zachodziły określone w art. 96 Konwencji przesłanki dokonania przez Szefa Urzędu do Spraw Cudzoziemców wpisu danych dotyczących ww. obywateli obcego państwa do Systemu Informacyjnego Schengen. Dotyczący tej osoby wpis do celów odmowy wjazdu na terytorium RP został bowiem wprowadzony na podstawie krajowego wpisu wynikającego z decyzji podjętej przez właściwy organ administracji, zgodnie z zasadami proceduralnymi ustanowionymi przez prawo krajowe, tj. ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach (Dz. U. z 2006 r. Nr 234 poz. 1694 z późn. zm.).

3) Banki i inne instytucje finansowe

W 2011 r. przeprowadzono **15 kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w podmiotach świadczących usługi doradztwa podatkowego i finansowego**¹⁶. Zakresem kontroli objęto przetwarzanie przez kontrolowane podmioty danych osobowych osób korzystających z doradztwa podatkowego i finansowego oraz danych osobowych pracowników i kandydatów do pracy.

W powołanym zakresie kontrolowane jednostki przetwarzały dane osobowe własnych klientów, jak również dane osobowe na zlecenie innych podmiotów. Przetwarzanie danych osobowych na zlecenie innych podmiotów wynikało z realizacji umów agencyjnych zawartych przez kontrolowane podmioty. W związku z tymi umowami kontrolowane podmioty wykonywały czynności agencyjne polegające między innymi na pozyskiwaniu klientów, oferowaniu produktów finansowych banków, funduszy inwestycyjnych oraz towarzystw ubezpieczeniowych, a także na wykonywaniu czynności przygotowawczych zmierzających do zawarcia umów, zawieraniu umów i obsłudze umów już zawartych. Ponadto kontrolowane podmioty przetwarzały dane osobowe własnych pracowników i kandydatów do pracy.

W pojedynczych przypadkach kontrole wykazały uchybienia polegające na przetwarzaniu danych osobowych nieadekwatnych do celu w jakim zostały zebrane (np. przetwarzanie nr PESEL

¹⁶ np. kontrole: DIS-K-421/50/10, DIS-K-421/75/11, DIS-K-421/46/11, DIS-K-421/48/11.

potencjalnych klientów w celu przedstawienia tym osobom oferty w zakresie produktów i usług oraz nr NIP klientów w celu świadczenia doradztwa finansowego polegającego na oferowaniu, sprzedaży i obsłudze produktów oraz usług finansowych, na podstawie analizy sytuacji finansowej klienta i nieodpłatnego doradztwa inwestycyjnego) oraz przetwarzaniu danych osobowych z naruszeniem przepisów prawa, tj. osoby aplikujące na stanowiska kierownicze w podmiocie były poddawane badaniu o nazwie „PAPI-N™ Profil”, którego celem było zbadanie roli i hierarchii postaw pracownika/kandydata w miejscu pracy, w tym m.in. tego, czy uważa się za osobę pracowitą, jak ważny jest dla niego sukces, jak silnie nastawiony jest na dokończenie zadań, jak bardzo dba o szczegóły, czy też jak ważna jest dla niego potrzeba zmian. Oprócz kandydatów do pracy, badaniu poddawani byli również pracownicy, co do których przewidywana była możliwość awansu na stanowisko kierownicze. Na podstawie ustalonego stanu faktycznego, w oparciu o obowiązujące przepisy prawa stwierdzono, że przetwarzanie danych osobowych pracowników i kandydatów do pracy uzyskiwanych w wyniku poddania pracownika/kandydata do pracy badaniu „PAPI-N™ Profil”, odbywało się z naruszeniem przepisów prawa, tj. art. 22¹ Kodeksu pracy¹⁷.

Najczęściej występującymi uchybieniami stwierdzonymi podczas kontroli było niezapewnienie, aby systemy informatyczne służące do przetwarzania danych osobowych umożliwiały odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego te dane¹⁸, jak również niezapewnienie przez ww. systemy możliwości sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie powyższe informacje.

Wobec podmiotów winnych uchybień stwierdzonych w toku przeprowadzonych kontroli wszczęte zostały postępowania administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych, zakończone wydaniem decyzji administracyjnych nakazujących ich usunięcie oraz decyzji umarzających postępowania. Nakazy decyzji dotyczyły m.in.: zaprzestania pozyskiwania numeru PESEL potencjalnych klientów; usunięcia numeru PESEL potencjalnych klientów¹⁹; zabezpieczenia danych osobowych zawartych w dokumentacji przechowywanej na otwartych regałach przed ich

¹⁷ Art. 22¹ § 1. Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: 1) imię (imiona) i nazwisko, 2) imiona rodziców, 3) datę urodzenia, 4) miejsce zamieszkania (adres do korespondencji), 5) wykształcenie, 6) przebieg dotychczasowego zatrudnienia. § 2. Pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, także: 1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, 2) numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL). § 3. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa w § 1 i 2. § 4. Pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów. § 5. W zakresie nieuregulowanym w § 1-4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych.

¹⁸ § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

¹⁹ DIS/DEC-849/47675/11

udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem²⁰; zapewnienia, aby system informatyczny służący do przetwarzania danych osobowych odnotowywał datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane do systemu; zapewnienia, aby system informatyczny służący do przetwarzania danych osobowych sporządzał i drukował raport zawierający w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych²¹.

4) Służba zdrowia

W roku sprawozdawczym przeprowadzono **5 kontroli w podmiotach świadczących usługi w obszarze służby zdrowia**. Kontrolami objęto 2 publiczne zakłady opieki zdrowotnej (szpitale), 2 niepubliczne zakłady opieki zdrowotnej oraz Centrum Organizacyjno - Koordynacyjne do Spraw Transplantacji „Poltransplant” (dalej: Poltransplant).

W wyniku czynności kontrolnych przeprowadzonych w jednym ze szpitali²² stwierdzono, że szpital ten nie sprawuje kontroli nad przechowywaniem i zabezpieczeniem zaświadczeń lekarskich o czasowej niezdolności do pracy wystawionych pacjentom szpitala twierdząc, że obowiązek w tym zakresie spoczywa na lekarzach, którzy je wystawili. Biorąc pod uwagę obowiązujące przepisy²³

²⁰ DIS/DEC-475/27861/11

²¹ DIS/DEC-447/26291/11

²² DIS-K-421/125/11

²³ Art. 36 ust. 1 ustawy o ochronie danych osobowych. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Art. 55 ust. 1 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (tekst jednolity: Dz. U. z 2010 r. Nr 77, poz. 512 z późn. zm.). Zaświadczenie lekarskie o czasowej niezdolności do pracy z powodu choroby lub pobytu w stacjonarnym zakładzie opieki zdrowotnej, konieczności osobistego sprawowania przez ubezpieczonego opieki nad chorym członkiem rodziny, zwane dalej „zaświadczeniem lekarskim”, jest wystawiane na odpowiednim druku, według wzoru określonego w przepisach wydanych na podstawie art. 59 ust. 14. Art. 54 ust. 1 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa. Zakład Ubezpieczeń Społecznych upoważnia do wystawiania zaświadczeń lekarskich, o których mowa w art. 55, lekarza, lekarza dentystę, felczera i starszego felczera po złożeniu przez niego pisemnego oświadczenia, że zobowiązuje się do przestrzegania zasad orzekania o czasowej niezdolności do pracy i wykonywania obowiązków wynikających z przepisów ustawy. Zaświadczenie lekarskie jest poufne. Art. 58 ust. 1 pkt 1 i 3 ww. ustawy: Zaświadczenie lekarskie wystawia się z dwiema kopiami, 1) oryginał zaświadczenia lekarskiego wystawiający zaświadczenie przesyła, w ciągu 7 dni od dnia wystawienia zaświadczenia, bezpośrednio do terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych, 2) pierwszą kopię zaświadczenia otrzymuje ubezpieczony, 3) drugą kopię wystawiający zaświadczenie przechowuje przez okres 3 lat.; § 2 ust. 2 rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. z 2010 r. Nr 252, poz. 1697). Dokumentacja indywidualna obejmuje: 1) dokumentację indywidualną wewnętrzną - przeznaczoną na potrzeby podmiotu udzielającego świadczeń zdrowotnych; 2) dokumentację indywidualną zewnętrzną - przeznaczoną na potrzeby pacjenta korzystającego ze świadczeń zdrowotnych udzielanych przez podmiot; § 2 ust. 4 pkt 3 ww. rozporządzenia. Dokumentację indywidualną zewnętrzną stanowi w szczególności zaświadczenie, orzeczenie, opinia lekarska.

Generalny Inspektor Ochrony Danych Osobowych podniósł, że zaświadczenie o czasowej niezdolności do pracy wystawione przez uprawnionego lekarza pacjentowi zakładu opieki zdrowotnej (pod nagłówkową pieczęcią zakładu opieki zdrowotnej), stanowi dokument medyczny indywidualny zewnętrzny wytworzony przez zakład opieki zdrowotnej. Zatem szpital, jako administrator danych osobowych pacjentów szpitala, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę danych osobowych pacjentów znajdujących się na wystawionych im zaświadczeniach lekarskich o czasowej niezdolności do pracy, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Powyższe stanowisko Generalnego Inspektora Ochrony Danych Osobowych znajduje potwierdzenie w uzasadnieniu Trybunału Konstytucyjnego do postanowienia z dnia 15 lutego 2000 r.²⁴, w którym Trybunał stwierdził, iż: „Zarówno materiały dokumentujące historię choroby pacjenta, jak również druki zaświadczeń lekarskich należą do danych chronionych tajemnicą służbową. Zakład pracy obowiązany jest zabezpieczyć właściwy tryb postępowania związany z obiegiem, gromadzeniem i przechowywaniem tych dokumentów, aby uniemożliwić osobom nieupoważnionym zapoznanie się z treścią informacji zawartych w tych dokumentach. Obowiązek ten dotyczy również przekazywania zaświadczeń lekarskich do właściwej jednostki organizacyjnej ZUS. Nic w treści art. 58 ustawy nie wskazuje na to, by ustawodawca nakazywał lekarzowi zatrudnionemu w zakładzie opieki zdrowotnej osobiste wykonywanie wskazanych w tym przepisie obowiązków o charakterze organizacyjnym oraz obciążał go kosztami w tym względzie.”.

W związku z tym, że opisane działania szpitala polegały na niezastosowaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wobec danych osobowych znajdujących się na zaświadczeniach o niezdolności do pracy wystawionych pacjentom tego szpitala, Generalny Inspektor wszczął postępowanie administracyjne w zakresie stwierdzonych uchybień.

Do interesujących należała również kontrola Centrum Organizacyjno - Koordynacyjnego do Spraw Transplantacji „Poltransplant”, działającego jako jednostka budżetowa podległa Ministrowi Zdrowia²⁵. Zgodnie z przepisami ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. z 2005 r. Nr 169, poz. 1411 z późn. zm.) zwanej dalej „ustawą transplantacyjną”, Poltransplant prowadzi rejestr żywych dawców, krajową listę osób oczekujących na przeszczepienie i krajowy rejestr przeszczepień. Poltransplant powierzył prywatnemu

²⁴ sygn. T. 28/99

²⁵ DIS-K-421/121/11

podmiotowi przetwarzanie danych objętych zbiorem danych osobowych, który tworzą następujące rejestry: krajowy rejestr przeszczepień, centralny rejestr żywych dawców narządów oraz krajowa lista osób oczekujących na przeszczepienie. Ww. rejestry nie zostały zgłoszone do Generalnego Inspektora Ochrony Danych Osobowych z uwagi na to, iż w opinii Poltransplant dotyczą osób korzystających z usług medycznych finansowanych przez Poltransplant, zatem korzystają ze zwolnienia wskazanego w art. 43 ust. 1 pkt 5 ustawy o ochronie danych osobowych²⁶. Biorąc jednak pod uwagę, że „(...) zwolnione z obowiązku rejestracyjnego nie będą więc podmioty, które samodzielnie nie świadczą usług, lecz wyłącznie umożliwiają ich świadczenie innym podmiotom, czy też zarządzają procesem świadczenia usług.”²⁷, Generalny Inspektor stwierdził, że Poltransplant powinien zgłosić do rejestracji wskazane zbiory danych osobowych.

Przeprowadzona kontrola wykazała ponadto, że Poltransplant wydaje zgodę na wywóz szpiku, komórek krwiotwórczych krwi obwodowej i krwi pępowinowej oraz narządów ze zwłok ludzkich, zgodnie z przepisami ustawy transplantacyjnej²⁸. Wnioski o zgodę na przewóz i wywóz komórek krwiotwórczych krwi obwodowej, szpiku oraz narządów składają ośrodki pobierające lub przeszczepiające. Zgoda albo jej odmowa są wydawane niezwłocznie, na wniosek podmiotów wymienionych w przepisach wskazanej ustawy, każdorazowo w drodze decyzji administracyjnej. Decyzji nadaje się rygor natychmiastowej wykonalności. Od decyzji dyrektora Centrum Organizacyjno-Koordynacyjnego do Spraw Transplantacji „Poltransplant” przysługuje odwołanie do ministra właściwego do spraw zdrowia. Dane o ww. wywozach i przywozach gromadzi i przechowuje Poltransplant. Decyzje wpisywane są do spisu prowadzonego w systemie informatycznym. Decyzje zawierają dane osobowe dawców i biorców w zakresie identyfikatora dawcy, imienia i nazwiska, nr PESEL biorcy. Kopie decyzji ułożone są wg numeru i daty decyzji, odrębnie dla decyzji dotyczących wywozu i przywozu narządów oraz wywozu i przywozu krwiotwórczych komórek krwi obwodowej i komórek szpiku. W świetle powyższych ustaleń Generalny Inspektor stwierdził, że Poltransplant prowadzi zbiór danych osobowych zawartych w przedmiotowych decyzjach, zatem jest zobowiązany do zgłoszenia także i tego zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

²⁶ Art. 43 ust. 1 pkt 5. Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta.

²⁷ P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych, Komentarz, Wydawnictwo C.H. BECK, Warszawa 2009, s. 406.

²⁸ Art. 37a ust. 1. Wywóz szpiku, komórek krwiotwórczych krwi obwodowej i krwi pępowinowej z terytorium Rzeczypospolitej Polskiej i ich przywozu na terytorium Rzeczypospolitej Polskiej dokonuje podmiot leczniczy wykonujący pobranie lub przeszczepienie szpiku, komórek krwiotwórczych krwi obwodowej i krwi pępowinowej za zgodą dyrektora Centrum Organizacyjno - Koordynacyjnego do Spraw Transplantacji „Poltransplant”. Art. 37a ust. 4. Wywozu z terytorium Rzeczypospolitej Polskiej i przywozu tych narządów na terytorium Rzeczypospolitej Polskiej dokonuje podmiot leczniczy, wykonujący pobranie lub przeszczepienie narządów ze zwłok ludzkich, za zgodą dyrektora Centrum Organizacyjno - Koordynacyjnego do Spraw Transplantacji „Poltransplant”.

W związku z powyższym wobec Poltransplantu zostało wszczęte postępowanie administracyjne obejmujące swoim zakresem wskazane uchybienia, a także inne nieprawidłowości stwierdzone w toku kontroli, dotyczące funkcjonalności systemu informatycznego oraz dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

5) Zatrudnienie

W 2011 r. poddano kontroli sektor agencji pośrednictwa pracy. W ramach ww. sektora przeprowadzono **17 kontroli** zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych²⁹.

Zakresem kontroli objęto przetwarzanie danych osobowych przez podmioty poddane kontroli w związku z prowadzeniem agencji pośrednictwa pracy, tj. świadczeniem usług w zakresie: 1) pośrednictwa pracy, polegającego w szczególności na udzielaniu pomocy osobom w uzyskaniu odpowiedniego zatrudnienia lub innej pracy zarobkowej oraz pracodawcom w pozyskaniu pracowników o poszukiwanych kwalifikacjach zawodowych, pozyskiwaniu i upowszechnianiu ofert pracy, udzielaniu pracodawcom informacji o kandydatach do pracy, w związku ze zgłoszoną ofertą pracy, kierowaniu osób do pracy za granicą u pracodawców zagranicznych; 2) doradztwa personalnego, polegającego w szczególności na weryfikacji kandydatów pod względem oczekiwanych kwalifikacji i predyspozycji; 3) poradnictwa zawodowego, polegającego w szczególności na udzielaniu pomocy w wyborze odpowiedniego zawodu i miejsca zatrudnienia, udzielaniu informacji niezbędnych do podejmowania decyzji zawodowych w szczególności o zawodach, rynku pracy oraz możliwościach szkolenia i kształcenia; 4) pracy tymczasowej, polegającej na zatrudnianiu pracowników tymczasowych i kierowaniu tych pracowników oraz osób niebędących pracownikami do wykonywania pracy tymczasowej na rzecz i pod kierownictwem pracodawcy użytkownika, na zasadach określonych w przepisach o zatrudnianiu pracowników tymczasowych.

W wyniku przeprowadzonych kontroli ustalono, że w związku z prowadzeniem agencji zatrudnienia, podmioty poddane kontroli przetwarzają dane osobowe osób poszukujących pracy (kandydatów do pracy) oraz pracowników tymczasowych w rozumieniu ustawy z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych (Dz. U. z 2008 r. Nr 69 poz. 415 z późn. zm.).

Uchybienia w procesie przetwarzania danych osobowych stwierdzono w 15 skontrolowanych podmiotach. Nieprawidłowości dotyczyły m.in. sformułowania klauzuli zgody na przetwarzanie danych osobowych w sposób nieodpowiadający definicji zgody na przetwarzanie danych osobowych

²⁹ np. kontrole: DIS-K-421/3/11, DIS-K-421/9/11, DIS-K-421/14/11.

zawartej w art. 7 pkt 5 ustawy o ochronie danych osobowych³⁰, co skutkowało naruszeniem normy zawartej w art. 23 ust. 1 pkt 1 powołanej ustawy³¹. Zdarzały się też przypadki, iż ww. podmioty nie realizowały w pełnym zakresie obowiązku informacyjnego wobec kandydatów do pracy, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych³², i nie informowały tych osób o celu zbierania danych, o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, oraz o prawie dostępu do treści swoich danych oraz ich poprawiania. Ponadto w toku kontroli stwierdzano, iż kontrolowane podmioty przetwarzały z naruszeniem przepisów prawa: dane osobowe pracowników tymczasowych (zatrudnionych na stanowiskach monterów lub spawaczy) w zakresie obejmującym informacje na temat ich niekaralności (art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych); dane osobowe kandydatów do pracy w zakresie szerszym niż jest to niezbędne do realizacji celu, w jakim dane te są przetwarzane np. przetwarzanie danych dotyczącej stanu cywilnego kandydata w celu określenia jego dyspozycyjności (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych³³); przetwarzania bez zgody kandydatów do pracy ich danych osobowych pozyskiwanych za pośrednictwem aplikacji udostępnionej na stronie internetowej, w celu przeprowadzania procesów rekrutacyjnych na rzecz klientów agencji zatrudnienia (pracodawców), a także w celu informowania osób, których dane dotyczą, o nowych ofertach pracy.

Sporadycznie zdarzały się przypadki, iż agencje zatrudnienia nie zawarły umowy powierzenia przetwarzania danych, o której mowa w art. 31 ust. 1 ustawy o ochronie danych osobowych³⁴, z podmiotem, któremu zostały przekazane dane osobowe w celu ich przechowywania na serwerach oraz nie wskazywały w umowach powierzenia przetwarzania danych osobowych zakresu lub zakresu i celu przetwarzania powierzonych danych osobowych. Pojedyncze podmioty nie zgłosiły do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych osobowych kandydatów do pracy. Podmiot przetwarzający dane osobowe w ramach pośrednictwa pracy (agencji zatrudnienia), a nie jako przyszły pracodawca, nie jest bowiem zwolniony z obowiązku zgłoszenia zbioru danych do rejestracji, tak jak ma to miejsce w przypadku administratorów danych przetwarzanych dane w

³⁰ Art. 7 pkt 5. Ilekroć w ustawie jest mowa o zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

³¹ Art. 23 ust. 1 pkt 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych.

³² 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.

³³ Art. 26 ust. 1 pkt 3. 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 merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

³⁴ Art. 31 ust. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

związku z zatrudnieniem u nich lub świadczeniem im usług na podstawie umów cywilnoprawnych, których zbiory podlegają zwolnieniu na podstawie art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych³⁵.

W większości skontrolowanych podmiotów stwierdzono uchybienie polegające na niezabezpieczeniu danych osobowych za pomocą środków ochrony kryptograficznej podczas ich przesyłania poprzez sieć publiczną. Liczne nieprawidłowości stwierdzono także w zakresie prowadzonej przez administratorów danych dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, poprzez niezawarcie w niej wszystkich elementów 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 osobowych³⁶ (np. informacji o wszystkich systemach informatycznych użytkowanych przez administratora danych, wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opisu struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami).

Ponadto niektóre kontrole wykazały, że podmioty użytkowały systemy informatyczne służące do przetwarzania danych osobowych, które nie zapewniały realizacji wymogów wynikających z rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, np.: aby hasło użytkownika strony internetowej składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne (część B pkt VIII załącznika do rozporządzenia); aby hasła służące do uwierzytelniania użytkowników były

³⁵ Art. 43. ust. 1 pkt 4. Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się.

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

zmieniane nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia); aby system informatyczny służący do przetwarzania danych osobowych zapewniał dla każdej osoby, której dane są przetwarzane w tym systemie odnotowanie daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 1 pkt 1 i 2 rozporządzenia); aby system sporządzał i drukował raport zawierający w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 3 rozporządzenia). W dwóch przypadkach niezabezpieczono stacji roboczej wykorzystywanej do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

W wyniku przeprowadzonych kontroli w podmiotach prowadzących agencje zatrudnienia wszczęto 11 postępowań administracyjnych w sprawie przetwarzania danych osobowych. Zakresem postępowań objęto uchybienia w procesie przetwarzania danych osobowych stwierdzone w toku kontroli. Postępowania te zakończyły się wydaniem decyzji administracyjnych nakazujących usunięcie uchybień w procesie przetwarzania danych osobowych³⁷ (np. poprzez: dopełnienie obowiązku informacyjnego wynikającego z art. 24 ust. 1 pkt 2 i pkt 3 ustawy o ochronie danych osobowych; usunięcie danych osobowych byłych pracowników tymczasowych, którzy byli zatrudnieni na stanowisku montera lub spawacza, obejmujących informację na temat niekaralności; zabezpieczenie danych osobowych kandydatów do pracy podczas ich przesyłania przez sieć publiczną za pośrednictwem programu Ms Outlook poprzez zastosowanie środków kryptograficznej ochrony) lub decyzji umarzających postępowanie w sprawie. Przestanką umorzenia postępowań była ich bezprzedmiotowość spowodowana usunięciem uchybień w procesie przetwarzania danych osobowych stanowiących ich przedmiot w toku postępowań administracyjnych.

Cztery spośród podmiotów poddanych kontroli³⁸, w przypadku których stwierdzono nieprawidłowości w procesie przetwarzania danych osobowych, przywróciły stan zgodny z prawem w zakresie objętym kontrolą przed wszczęciem postępowania administracyjnego. W związku z powyższym, w odniesieniu do tych podmiotów Generalny Inspektor Ochrony Danych Osobowych nie skorzystał z prawa określonego w art. 18 ust. 1 ustawy o ochronie danych osobowych³⁹.

³⁷ np. decyzja DIS/DEC-688/39620/11

³⁸ np. kontrole DIS-K-421/31/11, DIS-K-421/24/11.

³⁹ Art. 18. 1. W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje 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.

6) Imprezy masowe organizowane na stadionach

W okresie sprawozdawczym przeprowadzono **14 kontroli** zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w podmiotach zajmujących się organizacją imprez masowych na stadionach, w tym 4 w ośrodkach sportu i rekreacji⁴⁰, 9 w klubach sportowych⁴¹ i 1 w spółce kapitałowej zarządzającej stadionem⁴². Zakresem kontroli objęto przetwarzanie przez ww. podmioty danych osobowych uczestników imprez masowych oraz informacji dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej.

Objęte kontrolami ośrodki sportu i rekreacji były właścicielami stadionów, na których odbywają się imprezy masowe. Ośrodki te nie organizowały imprez masowych, natomiast udostępniały stadiony w celu przeprowadzenia imprezy masowej innym podmiotom, przede wszystkim klubom sportowym. W toku przeprowadzonych kontroli ustalono, iż stadiony, na których organizowane były mecze piłki nożnej, wyposażone były w elektroniczne systemy kontroli wstępu na te imprezy. Obowiązek wyposażenia stadionów w powyższe systemy wynika z art. 13 ust. 2 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 z późn. zm.), zgodnie z którym stadiony, na których odbywają się mecze piłki nożnej, wyposażone są w systemy elektroniczne służące do identyfikacji osób, sprzedaży biletów, kontroli przebywania w miejscu i w czasie trwania meczu piłki nożnej, kontroli dostępu do określonych miejsc oraz weryfikacji informacji dotyczących osób objętych zakazem wstępu na imprezę masową (tzw. zakaz stadionowy), zakazem klubowym lub zakazem zagranicznym. Obowiązek powyższy ciąży na organizatorach imprez masowych – meczów piłki nożnej. W powyższych systemach przetwarzane są dane osobowe kibiców będących uczestnikami meczów piłki nożnej.

Jak ustalono, podmioty organizujące imprezy masowe - w tym mecze piłki nożnej - utrwalają przebieg organizowanych przez siebie imprez masowych za pomocą systemów monitoringu zainstalowanych na stadionach. Nagrania z systemu monitoringu zawierają zestawy informacji dotyczących uczestników imprez masowych tworzące zbiory danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych⁴³. Dostęp do tych danych był bowiem możliwy według czasu oraz miejsca nagrania. Ponadto ustalono, że dane te są przetwarzane wyłącznie w celu wskazanym w art. 11 ust. 9 ustawy o bezpieczeństwie imprez masowych, tj. wykorzystania zarejestrowanego obrazu i dźwięku w postępowaniu dowodowym w stosunku do osób zakłócających porządek podczas imprezy masowej.

⁴⁰ np. kontrole DIS-K-421/82/11, DIS-K-421/93/11.

⁴¹ np. kontrole DIS-K-421/90/11, DIS-K-421/96/11, DIS-K-421/110/11, DIS-K-421/154/11.

⁴² DIS-K-421/141/11

⁴³ Art. 7 pkt 1. Ilekroć w ustawie jest mowa o zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Ponadto podmioty kontrolowane prowadziły zbiory danych osób objętych zakazem wstępu na imprezę masową (tzw. zakaz stadionowy), zakazem klubowym lub zakazem zagranicznym. Dane te były przetwarzane w celu uniemożliwienia osobom objętym ww. zakazami wstępu na imprezę masową na podstawie przepisów ustawy o bezpieczeństwie imprez masowych. Dane te były przetwarzane zarówno w systemach elektronicznych, o których mowa w art. 13 ust. 2 powołanej ustawy, jak i w formie papierowej.

W tym miejscu należy podkreślić, że kibice są identyfikowani w systemach elektronicznych, o których mowa powyżej, na podstawie informacji zapisanych na elektronicznych kartach zbliżeniowych, tzw. kartach kibica. Karty kibica są zindywidualizowane, tzn. są przypisane do konkretnej osoby. Podczas wystawiania kart kibica niektóre podmioty pozyskiwały dane osobowe w szerszym zakresie (np. płeć, wykształcenie, stan cywilny, dzieci, status zawodowy, zainteresowania) niż wskazany w art. 13 ust. 4 ustawy o bezpieczeństwie imprez masowych. Zgodnie z art. 13 ust. 4 powołanej ustawy, zakres przetwarzanych danych identyfikujących osoby uczestniczące w meczu piłki nożnej obejmuje imię, nazwisko, numer PESEL oraz wizerunek. Ustalono też, iż pozyskane dane były wykorzystywane przez kluby sportowe także w celach marketingowych. Kontrole wykazały ponadto, iż na podstawie odrębnych umów zawartych pomiędzy bankami a organizatorami imprez masowych, karty kibica, jeżeli kibic wyrazi zgodę, mogą być wykorzystywane również w charakterze kart płatniczych. W związku z powyższym zaistniała wątpliwość, czy wyżej opisane praktyki są dopuszczalne w świetle przepisów o ochronie danych osobowych. Po przeanalizowaniu zagadnienia uznano, iż przetwarzanie przez kluby sportowe, jako organizatorów imprez masowych, danych osobowych w celu marketingowym, jest dopuszczalne, o ile osoby, których dane są przetwarzane, wyraziły na to zgodę. Uznano również, iż wykorzystywanie karty kibica w charakterze karty płatniczej nie narusza przepisów o ochronie danych osobowych pod warunkiem, że kibic zawarł z bankiem umowę o prowadzenie rachunku bankowego.

Większość organizatorów imprez masowych nie zgłosiła do rejestracji Generalnemu Inspektorowi zbiorów danych osobowych. Niektóre podmioty dokonały zgłoszenia kilku zbiorów danych na jednym formularzu zgłoszenia pomimo, iż zgodnie ze stanowiskiem Generalnego Inspektora na jednym formularzu zgłoszenia można dokonać zgłoszenia tylko jednego zbioru. Ponadto w kilku przypadkach polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym nie spełniały wymogów określonych w rozporządzeniu. Sporadycznie zdarzały się przypadki, iż zastosowane przez podmioty kontrolowane formy pozyskiwania zgody na przetwarzanie danych osobowych użytkowników nie zapewniały swobody w ich wyrażeniu lub niewyrażeniu (art. 23 ust. 1 pkt 1 w zw. z art. 7 pkt 5 ustawy), umowy powierzenia przetwarzania danych nie były zawarte w formie pisemnej, a także nie wyznaczono administratora bezpieczeństwa informacji.

Na podstawie stwierdzonych w toku kontroli uchybień w procesie przetwarzania danych osobowych, wobec podmiotów wszczęte zostały postępowania administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych, zakończone wydaniem decyzji administracyjnych nakazujących usunięcie nieprawidłowości oraz decyzji umarzających postępowania. Przesłanką umorzenia postępowania była ich bezprzedmiotowość spowodowana usunięciem uchybień w procesie przetwarzania danych osobowych stanowiących przedmiot postępowania administracyjnego. Jeden spośród podmiotów poddanych kontroli, w przypadku którego stwierdzono nieprawidłowości w procesie przetwarzania danych osobowych, przywrócił stan zgodny z prawem w zakresie objętym kontrolą przed wszczęciem postępowania administracyjnego. W związku z powyższym, w przypadku tego podmiotu Generalny Inspektor Ochrony Danych Osobowych nie skorzystał z prawa określonego w art. 18 ust. 1 ustawy o ochronie danych osobowych.

7) Telekomunikacja

W 2011 r. przeprowadzono **10 kontroli u operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych** w zakresie realizacji obowiązku, o którym mowa w art. 180a ust. 1 pkt 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.)⁴⁴.

Wspomniane kontrole odnosiły się do sposobu niszczenia zatrzymanych i przechowywanych danych, o których mowa w art. 180c Prawa telekomunikacyjnego, dla których upłynął okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi. W toku przedmiotowych kontroli badano również sposób odnotowania zatrzymanych i przechowywanych danych, dla których upłynął okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, które zostały zabezpieczone zgodnie z przepisami odrębnymi.

Zakres zatrzymywanych i przechowywanych danych, o których mowa w art. 180c Prawa telekomunikacyjnego jest uzależniony od rodzaju usług świadczonych przez operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych. Poddane kontroli podmioty świadczyły między innymi następujące rodzaje usług telekomunikacyjnych: połączenia stacjonarne publicznej sieci telekomunikacyjnej, ruchomej publicznej sieci telekomunikacyjnej, dostępu do Internetu, usługi poczty elektronicznej, telefonii internetowej (VOIP) i telefonii nomadycznej.

⁴⁴ np. DIS-K-412/119/11, DIS-K-412/120/11, DIS-K-412/122/11, DIS-K-421/136/11, DIS-K-421/149/11.

Część podmiotów powierzyła w całości lub w części (np. w zakresie usługi poczty elektronicznej) realizację obowiązku, o którym mowa w art. 180a ust. 1 pkt 1 Prawa telekomunikacyjnego, innym podmiotom⁴⁵.

Jak wykazały przeprowadzone kontrole, większość skontrolowanych podmiotów realizowało obowiązek wynikający z art. 180a ust. 1 pkt 1 ustawy Prawo telekomunikacyjne, tj. niszczyło zatrzymane i przechowywane dane, o których mowa w art. 180c wskazanej ustawy⁴⁶. Kontrolowane podmioty nie spotkały się też z praktyką konieczności zatrzymywania i przechowywania danych, dla których upłynął okres 24 miesiące, licząc od dnia połączenia lub nieudanej próby połączenia, które zostały zabezpieczone zgodnie z przepisami odrębnymi.

W pojedynczych przypadkach kontrole wykazały, że dane o których mowa w art. 180c Prawa telekomunikacyjnego, były przechowywane dłużej niż to wynika z art. 180a ust. 1 pkt 1 ustawy Prawo telekomunikacyjne. Wśród przyczyn podawanych przez podmioty, które przechowywały dane dłużej niż to wynika z powołanych przepisów, przeważał argument, iż tak stanowią funkcjonujące w tych podmiotach procedury przechowywania kopii zapasowych i procedury usuwania danych wynikające, m.in. z konstrukcji i wydolności wykorzystywanych przez te podmioty systemów informatycznych.

W jednym z przypadków stwierdzono, iż w treści zawartej między podmiotami umowy nie doprecyzowano kwestii dotyczących powierzenia przetwarzania danych osobowych, w tym danych, o których mowa w art. 180c Prawa telekomunikacyjnego, tj. zakresu i celu powierzenia przetwarzania ww. danych osobowych w szczególności kwestii dotyczących sposobu realizacji obowiązku, o którym mowa w art. 180a ust. 1 pkt 1 ustawy Prawo telekomunikacyjne.

We wszystkich opisanych wyżej przypadkach skierowano do jednostek kontrolowanych pisma informujące o stwierdzonych nieprawidłowościach. Jednocześnie w toku przeprowadzonych czynności pojawiły się kolejne zagadnienia problemowe.

W związku z jedną z kontroli wpłynęło pismo kontrolowanego podmiotu, zawierające stanowisko tego podmiotu związane z odmową udostępnienia upoważnionym do przeprowadzenia kontroli inspektorom, rzeczywistych danych retencyjnych, o których mowa w art. 180c Prawa telekomunikacyjnego. Ustosunkowując się do treści powołanego pisma Generalny Inspektor wskazał, iż podczas kontroli inspektorzy nie żądali udostępnienia im rzeczywistych danych retencyjnych przetwarzanych przez kontrolowany podmiot. Z uwagi na to, iż zakresem kontroli objęto między

⁴⁵ Art. 180a ust. 1 pkt 1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 24 miesiące, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi.

⁴⁶ Art. 180c ust. 1. Obowiązkiem, o którym mowa w art. 180a ust. 1, objęte są dane niezbędne do: 1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego: a) inicjującego połączenie, b) do którego kierowane jest połączenie; 2) określenia: a) daty i godziny połączenia oraz czasu jego trwania, b) rodzaju połączenia, c) lokalizacji telekomunikacyjnego urządzenia końcowego.

innymi zbadanie zgodności zakresu zatrzymywanych i przechowywanych danych z rozporządzeniem Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymania i przechowywania (Dz. U. Nr 226, poz. 1828), niezbędne było określenie zakresu danych przetwarzanych w systemie informatycznym. Podczas kontroli inspektorzy nie żądali udostępnienia rzeczywistych danych retencyjnych przetwarzanych w systemie, a jedynie wydruku z ww. systemu, obrazującego zakres danych przetwarzanych w tym systemie.

Nowelizacja ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.), która weszła w życie 6 lipca 2009 r., stanowiła implementację do krajowego porządku prawnego dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz. Urz. UE L z 2006 r. Nr 105 poz. 54). Stosownie do art. 180a ust. 1 pkt 1 ustawy Prawo telekomunikacyjne, z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt: zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi. Z woli ustawodawcy dane retencyjne objęte są tajemnicą telekomunikacyjną (art. 180a ust.1 pkt 3 ustawy Prawo telekomunikacyjne). Bez uszczerbku dla postanowień przyjętych zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE, każde państwo członkowskie gwarantuje, że dostawcy ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności będą respektować co najmniej zasady dotyczące bezpieczeństwa danych w odniesieniu do danych zatrzymywanych zgodnie z dyrektywą - art. 7 dyrektywy 2006/24/WE.⁴⁷ W przepisie tym wskazano zasady, które należy implementować do krajowego porządku prawnego i z których mają wynikać obowiązki dla przedsiębiorców telekomunikacyjnych. Natomiast zgodnie z art. 9 ust. 1 i 2 ww.

⁴⁷ Art. 7. Ochrona i bezpieczeństwo danych. Bez uszczerbku dla postanowień przyjętych zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE, każde państwo członkowskie gwarantuje, że dostawcy ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności respektują co najmniej następujące zasady dotyczące bezpieczeństwa danych w odniesieniu do danych zatrzymywanych zgodnie z niniejszą dyrektywą: a) zatrzymywane dane mają taką samą jakość i podlegają takim samym zasadom bezpieczeństwa i ochrony, jak dane w sieci; b) w stosunku do danych stosowane będą właściwe środki techniczne i organizacyjne w celu ochrony tych danych przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieupoważnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem; c) w stosunku do danych stosowane będą właściwe środki techniczne i organizacyjne w celu zagwarantowania, że dostęp do danych ma jedynie upoważniony do tego personel; oraz d) wszystkie dane, z wyjątkiem tych, które zostały udostępnione i zachowane, zostaną zniszczone pod koniec okresu zatrzymania.

dyrektywy 2006/24/WE, każde państwo członkowskie wyznacza jeden lub więcej organów publicznych odpowiedzialnych za nadzór nad stosowaniem na ich terytorium przepisów przyjętych przez państwa członkowskie zgodnie z art. 7 w odniesieniu do bezpieczeństwa przechowywanych danych. Organami tymi mogą być te same organy, o których mowa w art. 28 dyrektywy 95/46/WE. Organy, o których mowa w ust. 1 są w pełni niezależne w wykonywaniu nadzoru, o którym wspomina się w tym ustępie. Z brzmienia przedmiotowego przepisu wynika, że organami proponowanymi w dyrektywie do nadzorowania stosowania ww. przepisów, są organy ochrony danych osobowych. Tymczasem, zgodnie z art. 192 ust. 1 pkt 5b ustawy Prawo telekomunikacyjne, do zakresu działania Prezesa UKE należy w szczególności wykonywanie kontroli nad operatorami publicznej sieci telekomunikacyjnej i dostawcami publicznie dostępnych usług telekomunikacyjnych w zakresie realizacji obowiązków, o których mowa w art. 180a ust. 1, z wyjątkiem realizacji obowiązków dotyczących danych osobowych chronionych zgodnie z przepisami o ochronie danych osobowych. Powyższe kompetencje zostały na Prezesa Urzędu Komunikacji Elektronicznej nałożone przepisami ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 716). W uzasadnieniu rządowego projektu tej ustawy (druk sejmowy nr 1448) wskazano: „W art. 192 ust. 5b została dodana kompetencja dotycząca wykonywania kontroli nad operatorami publicznej sieci telekomunikacyjnej i dostawcami publicznie dostępnych usług telekomunikacyjnych w zakresie realizacji obowiązków, o których mowa w art. 180a ust. 1. Przechowywanie danych retencyjnych ma być podporządkowane podstawowym zasadom dotyczącym prawidłowej ochrony i bezpieczeństwa danych. W prawie polskim kontrola przestrzegania owych zasad może być prowadzona przez Generalnego Inspektora Ochrony Danych Osobowych jedynie pośrednio i w zakresie ograniczonym do danych osobowych, według zasad wynikających z ustawy o ochronie danych osobowych. Ww. nadzór będzie wykonywany przez Prezesa UKE z wyłączeniem danych osobowych chronionych zgodnie z przepisami o ochronie danych osobowych.” Z przedmiotowych zapisów wynika wprost, że ustawodawca implementując przepisy dyrektywy 2006/24/WE, uznał, iż organem nadzorczym, o którym mowa w art. 9 ust. 1 i 2 ww. dyrektywy 2006/24/WE, w polskim porządku prawnym będzie Prezes UKE i jedynie pośrednio poprzez powołanie się na przepisy ustawy o ochronie danych osobowych wskazał na uprawnienia Generalnego Inspektora Ochrony Danych Osobowych. Zakres uprawnień Generalnego Inspektora jako organu nadzorczego w procesie zatrzymywania i przechowywania danych, o których mowa w art. 180c ustawy Prawo telekomunikacyjne, będzie zatem zależny od uznania ww. danych retencyjnych za dane osobowe. Na podstawie art. 180c ust. 2 ustawy - Prawo telekomunikacyjne, wydane zostało rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Dz.

U. Nr 226, poz. 1828). W powyższym rozporządzeniu między innymi wprost wskazuje się na dane takie jak imię i nazwisko albo nazwa oraz adres użytkownika końcowego. W świetle obowiązującej definicji danych osobowych, za które uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 6 ust. 1 ustawy o ochronie danych osobowych) należało uznać, że dane, o których mowa w art. 180c ust. 1 ustawy Prawo telekomunikacyjne, o ile dotyczą osób fizycznych, są danymi osobowymi w rozumieniu powołanych przepisów.

Biorąc powyższe pod uwagę stwierdzono, że Generalny Inspektor posiada uprawnienia nadzorcze w odniesieniu do bezpieczeństwa przechowywanych danych osobowych, o których mowa w art. 180c ustawy Prawo telekomunikacyjne.

8) Przedszkola

W 2011 r. poddano kontroli sektor przedszkoli, w ramach którego przeprowadzono **12 kontroli** zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych⁴⁸. Kontrole w tym sektorze są kontynuowane w 2012 r. Zakresem kontroli objęto przetwarzanie danych osobowych przez przedszkola publiczne i niepubliczne zarówno z Warszawy, jak i spoza jej terenu.

W wyniku przeprowadzonych kontroli ustalono, że przedszkola przetwarzają dane osobowe dzieci, ich rodziców lub prawnych opiekunów w związku z rekrutacją do przedszkoli oraz w związku z procesem kształcenia dziecka w przedszkolu. Przetwarzają także dane osób odbierających dzieci z przedszkola.

Uchybień w procesie przetwarzania danych osobowych nie odnotowano w trzech skontrolowanych przedszkolach. W pozostałych zaś stwierdzono nieprawidłowości polegające m.in. na naruszeniu przez dwa przedszkola zasady adekwatności wyrażonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. W toku kontroli ustalono, że rodzice wypełniają kartę przedszkolaka, w której znajduje się pole zawierające informację o miejscach pracy rodziców. Wymaganie od rodziców podania takich danych należało uznać za zbyteczne i nieadekwatne w stosunku do celów, w jakich są one przetwarzane, tj. nawiązania szybkiego kontaktu z rodzicem w nagłych przypadkach. Przedszkole dysponuje bowiem informacjami w wystarczającym zakresie, tj. numerem telefonu do każdego z rodziców. Co więcej, karta ta zawiera pole przeznaczone na wpisanie imion, nazwisk i wieku rodzeństwa. Podawanie tak szczegółowych informacji o rodzeństwie dziecka ubiegającego się o przyjęcie do przedszkola, należy również uznać za nieadekwatne do celu przetwarzania danych, jakim jest poznanie jego sytuacji rodzinnej.

⁴⁸ np. kontrole: DIS-K-421/163/11, DIS-K-421/175/11, DIS-K-421/187/11, DIS-K-421/198/11.

Ustalono ponadto, że dane podlegające szczególnej ochronie, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych⁴⁹, tj. wskazujące, że: u dziecka stwierdzono alergię pokarmową potwierdzoną zaświadczeniem lekarza specjalisty; dziecko jest wychowywane przez samotnego/pracującego rodzica/opiekuna prawnego lub w placówce opiekuńczo – wychowawczej; dziecko jest wychowywane w rodzinie objętej nadzorem kuratorskim; dziecko ma rodzeństwo z orzecznym średnim lub znacznym stopniem niepełnosprawności, były przetwarzane na podstawie art. 27 ust. 2 pkt 1 ustawy, tj. za zgodą rodziców/opiekunów prawnych.

Natomiast dane osobowe pozyskiwane w celu identyfikacji (PESEL, imiona, nazwisko, data i miejsce urodzenia oraz adres zamieszkania dziecka, dane osobowe rodziców/opiekunów prawnych, tj. imię i nazwisko, adres zamieszkania, nr telefonu, informacja o tym czy oboje rodzice/prawni opiekunowie pracują lub studiują w trybie dziennym), a także inne dane decydujące o przyjęciu dziecka do przedszkola (informacja o tym, że jedno z dwojga rodziców/prawnych opiekunów pracuje, że dziecko ma dwoje i więcej rodzeństwa poniżej 14 roku życia, i o tym, czy któreś z rodzeństwa ubiega się jednocześnie po raz pierwszy o przyjęcie do tego samego przedszkola i czy rodzeństwo kontynuuje w roku szkolnym 2011/2012 edukację w przedszkolu pierwszego wyboru) były pozyskiwane na podstawie art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, tj. zgody wyrażonej przez rodziców/prawnych opiekunów dzieci. Adres poczty elektronicznej jest daną, którą rodzice mogą podać, ale nie ma takiego obowiązku.

W jednym niepublicznym przedszkolu nie zapewniono, aby zgoda na przetwarzanie danych osobowych o stanie zdrowia dziecka, wyrażana przez rodziców/opiekunów prawnych, spełniała warunki określone w art. 7 pkt 5 ustawy⁵⁰ (art. 27 ust. 2 pkt 2 ustawy⁵¹). Rodzice (oraz lekarz) wypełniali bowiem kartę zdrowia przedszkolaka, która zawierała, m.in. szczegółowe informacje o przebytych przez dziecko chorobach. Rodzice wypełniając tę kartę przy zapisie dziecka do przedszkola mieli możliwość wyrażenia zgody na objęcie dziecka opieką medyczną. Ale zgoda na objęcie dziecka opieką medyczną nie może być rozumiana jako zgoda na przetwarzanie danych o jego stanie zdrowia, zatem formularz karty zdrowia przedszkolaka powinien być uzupełniony o zapis, z którego wprost wynika oświadczenie o wyrażeniu zgody na przetwarzanie danych o stanie zdrowia dziecka.

⁴⁹ Art. 27. 1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

⁵⁰ Art. 7 pkt 5. Ilekroć w ustawie jest mowa o zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

⁵¹ Art. 27 ust. 2 pkt 2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

Jedno z przedszkoli poddanych kontroli nie zapewniło, aby dane były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt 4 ustawy)⁵². W przedszkolu tym były przechowywane wypełnione w ostatnich 3 latach karty zgłoszenia dzieci, które nie zostały przyjęte do przedszkola. Okres przechowywania tych dokumentów nie został określony w przepisach prawa oraz w regulacjach wewnętrznych obowiązujących w przedszkolu. Należało uznać, że w przypadku nieprzyjęcia dziecka do przedszkola w danym roku szkolnym brak jest uzasadnienia dla przetwarzania (w tym przechowywania) danych osobowych dotyczących takiego dziecka oraz jego rodziców/opiekunów prawnych zawartych na karcie zgłoszenia dziecka w następnych latach. Przetwarzanie tych danych przez okres roku szkolnego, którego rekrutacja dotyczy, można uznać za usprawiedliwione tylko w związku z możliwością przeprowadzenia rekrutacji uzupełniającej bądź możliwością złożenia przez rodzica/opiekuna prawnego odwołania związanego z rekrutacją. Stwierdzono również uchybienia dotyczące przetwarzania danych w systemach informatycznych polegające na niezapewnieniu, aby systemy informatyczne służące do przetwarzania danych osobowych umożliwiały odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego te dane (§ 7 ust. 1 pkt 1 i pkt 2 rozporządzenia)⁵³, jak również niezapewnieniu przez ww. systemy możliwości sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia (oraz § 7 ust. 3 rozporządzenia).

W dwóch przedszkolach kontrola ujawniła brak zabezpieczeń kopii zapasowych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Kopie zapasowe z systemów informatycznych, w których przetwarzane były dane osobowe, przechowywano na dyskach serwera. Niemniej jednak w pomieszczeniu, w którym umieszczony był serwer nie zainstalowano instalacji przeciwpożarowej oraz nie wyposażono tego pomieszczenia w klimatyzację. Brak klimatyzacji w serwerowni skutkuje wysoką temperaturę powietrza, co stwarza ryzyko uszkodzenia dysków serwera, na których przetwarzane są dane osobowe, w tym również kopii zapasowych, co skutkować może bezpowrotną utratą tych danych (część A pkt IV ppkt 4 litera a załącznika do rozporządzenia).

W pojedynczych przypadkach stwierdzono, że w kontrolowanych jednostkach nie zapewniono, aby hasło służące do uwierzytelnienia w systemie informatycznym służącym do przetwarzania danych osobowych składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki

⁵² Art. 26 ust. 1 pkt 4. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

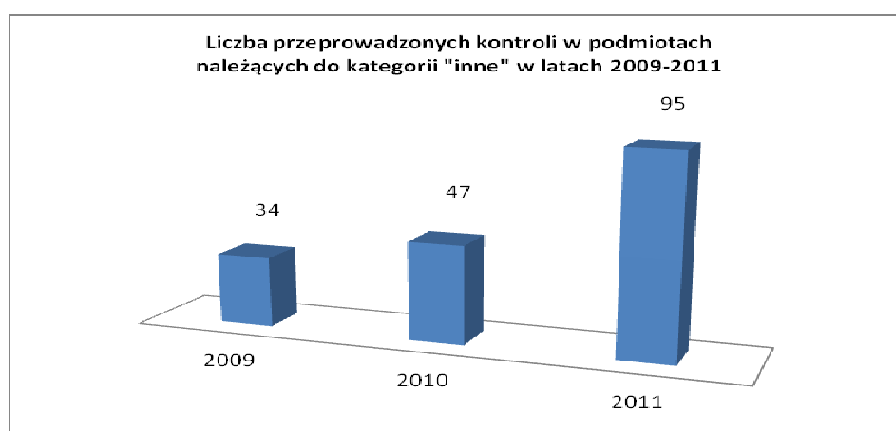
⁵³ § 7 ust. 1 pkt 1 i 2. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

specjalne (część B pkt VIII załącznika do rozporządzenia) i aby było zmieniane nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia) oraz nie zabezpieczono systemu informatycznego służącego do przetwarzania danych osobowych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (część A pkt III ppkt 2 załącznika do rozporządzenia). Inne uchybienia polegały m.in. na: niezawarciu w opracowanym dokumencie stanowiącym instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych elementów, o których mowa w § 4 pkt 2, pkt 5, pkt 6 i pkt 8 rozporządzenia, tj.: procedur nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności, stosowanych metod i środków uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem, sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe w tym kopii zapasowych, sposobu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia, procedur wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Na podstawie wyników kontroli prowadzone są postępowania administracyjne w zakresie stwierdzonych uchybień.

9) Inne

Istotne problemy w procesie przetwarzania danych osobowych stwierdzone były również w toku kontroli przeprowadzonych w podmiotach nienależących do żadnego z przedstawionych wyżej sektorów. W grupie tej przeprowadzono **95 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych, tj. dwa razy więcej niż w poprzednim roku sprawozdawczym.



Wykres 1: Zestawienie porównawcze liczby przeprowadzonych kontroli w podmiotach należących do sektora „Inne” w latach 2009–2011.

Jedną z bardziej interesujących kontroli była kontrola przeprowadzona w spółce prowadzącej klub fitness⁵⁴. W jej toku ustalono, że wśród danych pozyskiwanych od potencjalnych klientów klubu fitness były m.in. informacje o stanie cywilnym oraz informacje na temat posiadania dzieci. Jednocześnie ustalono, że dane osobowe potencjalnych klientów klubu były wykorzystywane przez spółkę w celu prowadzenia marketingu usług własnych spółki, tj. przedstawiania tym osobom oferty klubu. Kontrola wykazała, że informacja na temat posiadanych dzieci była pozyskiwana w celu ustalenia, czy dany klient jest zainteresowany ofertą przygotowaną przez klub dla dzieci, natomiast informacja na temat stanu cywilnego jest pozyskiwana w celu ustalenia, czy klient jest zainteresowany ofertą klubu przygotowaną dla par. Biorąc pod uwagę zasadę adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, Generalny Inspektor wskazał, że pytanie potencjalnych klientów klubu fitness o ich stan cywilny oraz o posiadanie dzieci w sposób nieuzasadniony wkracza w sferę ich prywatności. Pożądane przez spółkę informacje można bowiem uzyskać w sposób mniej ingerujący w prywatność osób, których dane dotyczą.

W związku z powyższym, Generalny Inspektor uznał, iż pozyskiwanie od potencjalnych klientów klubu fitness informacji o stanie cywilnym, jak również informacji na temat posiadania dzieci wykracza poza potrzeby wynikające z celu zbierania tych danych i tym samym narusza zasadę adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych, wobec spółki, jako administratora danych, zostało wszczęte postępowanie administracyjne w zakresie stwierdzonych uchybień.

W analizowanym roku sprawozdawczym dokonano również czynności kontrolnych⁵⁵ wobec jednego z serwisów internetowych świadczącego m.in. usługi polegające na zamieszczaniu w serwisie ofert kandydatów do pracy, ofert pracodawców poszukujących pracowników, umożliwieniu przeszukiwania ofert, a także pośrednictwo w ich przekazywaniu. Korzystając z ww. serwisu pracodawcy mieli możliwość zamieszczania ogłoszeń o wolnych stanowiskach pracy, przy czym mogli oni skorzystać z opcji ogłoszenia mającego charakter ukryty, tj. w ogłoszeniach nie była wskazana nazwa oraz adres pracodawcy. W opinii Generalnego Inspektora, praktyka taka budzi wątpliwości ze względu na wymogi wskazane w art. 24 ust. 1 ustawy o ochronie danych osobowych dotyczące konieczności informowania o okolicznościach wskazanych w tym przepisie⁵⁶.

⁵⁴ DIS-K-421/148/11

⁵⁵ DIS-K-421/14/11, DIS-K-421/55/11

⁵⁶ Art. 24 ust. 1 ustawy o ochronie danych osobowych. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach

W toku kontroli przeprowadzonej w Straży Miejskiej w jednym z miast⁵⁷ stwierdzono, że korzysta ona z prawa do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych. Uprawnienie to przysługuje jej na podstawie art. 11 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o Strażach Gminnych (Dz. U. Nr 123, poz. 779 z późn. zm.)⁵⁸. Osobę naruszającą porządek publiczny będzie można zidentyfikować w momencie dotarcia przez funkcjonariuszy Straży Miejskiej bądź Policji do miejsca wskazanego przez operatora systemu monitoringu, legitymując osobę na miejscu zdarzenia bądź też na podstawie przeprowadzonych czynności służbowych (np. przesłuchania świadków). Celem rejestracji obrazu jest utrwalanie dowodów popełnienia przestępstwa lub wykroczenia, przeciwdziałanie przypadkom naruszania spokoju i porządku w miejscach publicznych oraz ochrona obiektów komunalnych i urządzeń użyteczności publicznej. Osoby rejestrowane posiadały informację, iż na terenie miasta zainstalowany jest system monitoringu wizyjnego. Obowiązek informacyjny zrealizowany był w ten sposób, że na granicach miasta zamontowane zostały tablice informacyjne, na których wskazano „miasto monitorowane”. Wbrew doniesieniom prasowym, jakoby Straż Miejska oprócz obrazu nagrywała również dźwięk (do czego nie jest uprawniona, stosownie do art. 11 ust. 2 ustawy o Strażach Gminnych), stwierdzono, że w ramach systemu monitoringu nie są zainstalowane urządzenia do rejestrowania fonii.

Natomiast w toku kontroli systemu monitoringu przeprowadzonej w jednym z urzędów miast stwierdzono, że dokumentacja opisująca sposób przetwarzania danych nie zawierała informacji dotyczących przetwarzania danych w systemie monitoringu. Przedstawiona przez kontrolowany podmiot ewidencja osób upoważnionych do przetwarzania danych osobowych nie zawierała identyfikatorów użytkowników. Po uruchomieniu stacji roboczej systemu monitoringu automatycznie następowało logowanie na konto operatora, zaś wszyscy operatorzy logowali się na jedno konto użytkownika. Również administratorzy systemu logowali się na jedno konto administratora. Hasła użytkownika oraz administratora systemu monitoringu nie były zmieniane.

W kolejnej analizowanej sprawie, wyniki kontroli dotyczącej przetwarzania danych osobowych przez spółkę świadczącą usługi internetowe dały podstawę do wydania decyzji nakazującej dopełnienie obowiązku wynikającego z art. 36 ust. 3 ustawy o ochronie danych osobowych, polegającego na wyznaczeniu administratora bezpieczeństwa informacji. Od decyzji wniesiono

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.

⁵⁷ DIS-K-421/114/11

⁵⁸ Art. 11 ust. 2. W związku z realizowanymi zadaniami określonymi w ust. 1 i art. 10, straży przysługuje prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych w przypadku, gdy czynności te są niezbędne do wykonywania zadań oraz w celu: 1) utrwalania dowodów popełnienia przestępstwa lub wykroczenia, 2) przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych, 3) ochrony obiektów komunalnych i urządzeń użyteczności publicznej.

wniosek o ponowne rozpatrzenie sprawy, podając jako argument za niesłusznym rozstrzygnięciem decyzji interpretację powołanego przepisu, zgodnie z którą należy przyjąć, iż przewiduje on dwie odrębne sytuacje sprawowania nadzoru nad przestrzeganiem zasad ochrony danych osobowych, tj. poprzez wyznaczenie administratora bezpieczeństwa informacji oraz poprzez samodzielne wykonywanie przez administratora danych czynności nadzorczych. W stosunku do drugiej sytuacji – zdaniem skarżącego - nie istnieją ograniczenia podmiotowe wskazujących, że może ona mieć zastosowanie wyłącznie do określonej kategorii administratorów danych, np. wyłącznie do osób fizycznych prowadzących działalność gospodarczą. Z istoty czynności nadzoru jaką jest pełnienie omawianej funkcji, w żadnym razie nie wynika także, że czynności te mogą być wykonywane wyłącznie przez osobę fizyczną. Generalny Inspektor rozpatrując złożony wniosek wydał decyzję utrzymującą w mocy poprzednie rozstrzygnięcie i podtrzymał stanowisko, iż administrator danych sam może wykonywać zadania administratora bezpieczeństwa informacji jedynie wówczas, gdy jest osobą fizyczną prowadzącą działalność gospodarczą. Administrator danych niebędący osobą fizyczną prowadzącą działalność gospodarczą, jest zobowiązany wyznaczyć na administratora bezpieczeństwa informacji konkretną osobę fizyczną, gdyż tylko taka osoba w świetle art. 37 ustawy o ochronie danych osobowych może zostać upoważniona do przetwarzania danych osobowych, a takie upoważnienie jest niezbędne do prawidłowego wykonywania czynności nadzorczych przez administratora bezpieczeństwa informacji.

Analizując wyniki kontroli przeprowadzonych w 2011 roku należy stwierdzić, że w większości skontrolowanych podmiotów wystąpiły nieprawidłowości w procesie przetwarzania danych osobowych. Uchybienia te dotyczyły zarówno zastosowanych rozwiązań organizacyjnych, jak i aspektów technicznych.

Ponad 15% kontrolowanych jednostek nie opracowało dokumentacji, o której mowa w § 3 rozporządzenia tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zdarzały się również sytuacje, że opracowane dokumenty nie spełniały warunków odnoszących się do wymaganych w tych dokumentach treści określonych w § 4 i § 5 rozporządzenia. Dotyczyło to zarówno polityki bezpieczeństwa, jak i instrukcji zarządzania systemem informatycznym, gdzie ponad 19 % opracowanych dokumentów nie zawierało niezbędnych informacji lub też podane informacje nie miały odzwierciedlenia w rzeczywistości zastosowanych środków organizacyjnych oraz technicznych. Około 12 % podmiotów nie prowadziło ewidencji osób upoważnionych do przetwarzania danych osobowych lub ewidencja ta nie spełniała wymagań określonych w art. 39 ustawy. Natomiast około 5 % odnotowanych uchybień stwierdzonych w sektorze odnoszącym się do organizatorów imprez masowych organizowanych na stadionach oraz

częściowo w podmiotach doradców podatkowych i agencjach pośrednictwa pracy, dotyczyło niewyznaczenia administratora bezpieczeństwa informacji.

W skontrolowanych w 2011 r. podmiotach nadal stwierdzano uchybienia polegające na braku wymaganych funkcjonalności systemów informatycznych służących do przetwarzania danych osobowych (§ 7 rozporządzenia). Uchybienia te dotyczyły najczęściej braku odnotowania daty pierwszego wprowadzenia danych do systemu oraz braku odnotowywania identyfikatora użytkownika wprowadzającego dane do systemu (poniżej 8%). 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 (ponad 12% systemów). Jednakże porównując dostosowanie systemów informatycznych do wymogów funkcjonalnych określonych w § 7 rozporządzenia, w roku 2011 zauważyć należy poprawę w stosunku do roku 2010. Procentowa liczba skontrolowanych w 2011 r. systemów, w których występowały wymagane funkcjonalności była wyższa niż w roku 2010. Jedynie stopień wypełnienia obowiązków w zakresie odnotowywania informacji o odbiorcach danych w systemach informatycznych służących do przetwarzania danych osobowych nie zmienił się. Ponad 98% użytkowanych systemów informatycznych skontrolowanych w 2011 r. umożliwiało odnotowanie ww. informacji w sytuacji gdy udostępnienie takie miało miejsce. Zmniejszenie liczby nieprawidłowości w zakresie funkcjonalności systemów informatycznych w dużym stopniu należy przypisać temu, że w sektorze „Zatrudnienie” nie stwierdzono w tym zakresie uchybień.

W 2011 r. 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 szczególności dotyczyło to sektora „Zatrudnienie”, gdzie dane były przekazywane w większości poprzez sieć publiczną z wykorzystaniem poczty elektronicznej.

W 2011 r. nieznacznie pogorszyło się w porównaniu z rokiem 2010 wdrożenie mechanizmów autoryzacji dostępu do danych, jednakże nadal stało ono na wysokim poziomie, gdyż w 99 % skontrolowanych w 2011 r. systemach informatycznych istniały odpowiednie mechanizmy uwierzytelnienia użytkowników. Jednym z uchybień najczęściej napotkanych w procesie logowania było wykorzystywanie jednego identyfikatora logowania przez więcej niż jedną osobę (szczególnie widoczne w systemach monitoringu). Stwierdzono również wykorzystywanie wspólnego hasła logowania przez kilka osób lub też stosowanie nieodpowiednich parametrów haseł do wymaganego poziomu bezpieczeństwa czy też zmianę haseł rzadziej niż raz na 30 dni.

W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych przez jednostki kontrolowane, wydane zostały decyzje nakazujące ich usunięcie oraz umarzające postępowanie w zakresie nieprawidłowości usuniętych w toku postępowania. 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 2011 r. kontroli, weryfikacji poddano **384 systemy informatyczne**, tj. o 331 mniej niż w roku 2010, w którym skontrolowano 715 systemów informatycznych wykorzystywanych do przetwarzania danych osobowych.

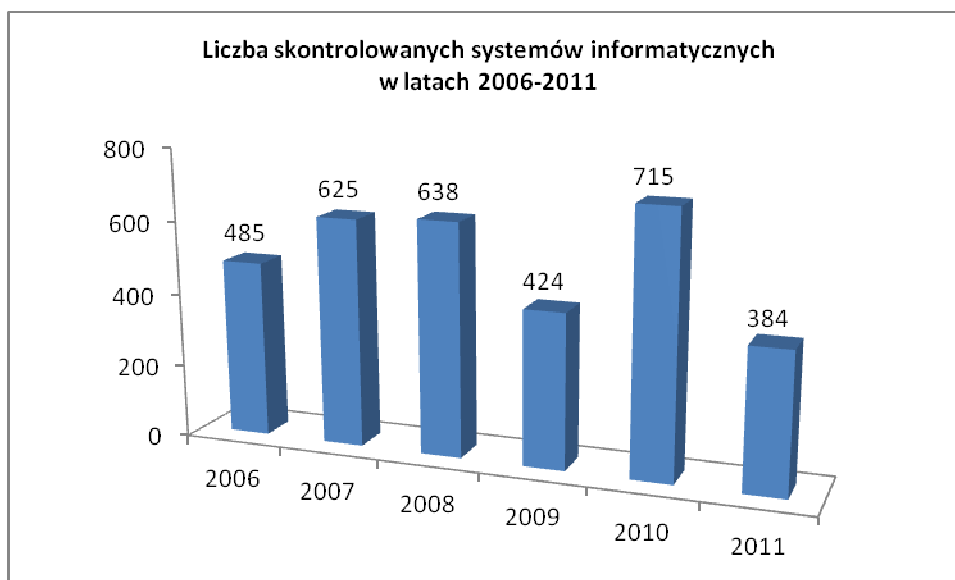
rok 2007 = 161 kontroli, obejmujących 625 systemów informatycznych,

rok 2008 = 201 kontroli, obejmujących 638 systemów informatycznych,

rok 2009 = 220 kontroli, obejmujących 424 systemy informatyczne,

rok 2010 = 196 kontroli, obejmujących 715 systemów informatycznych,

rok 2011 = 199 kontroli, obejmujących 384 systemy informatyczne



Wykres 2: Zestawienie porównawcze liczby skontrolowanych systemów informatycznych w latach 2007-2011.

Jak wynika z przedstawionego Wykresu 2, liczba systemów informatycznych objętych kontrolą w roku 2011 była niższa niż w latach poprzednich. Spowodowane to było tym, że przeprowadzane w 2011 r. kontrole sektorowe dotyczyły m.in. kwestii bezpieczeństwa imprez masowych oraz przetwarzania danych osobowych w przedszkolach, gdzie do przetwarzania danych

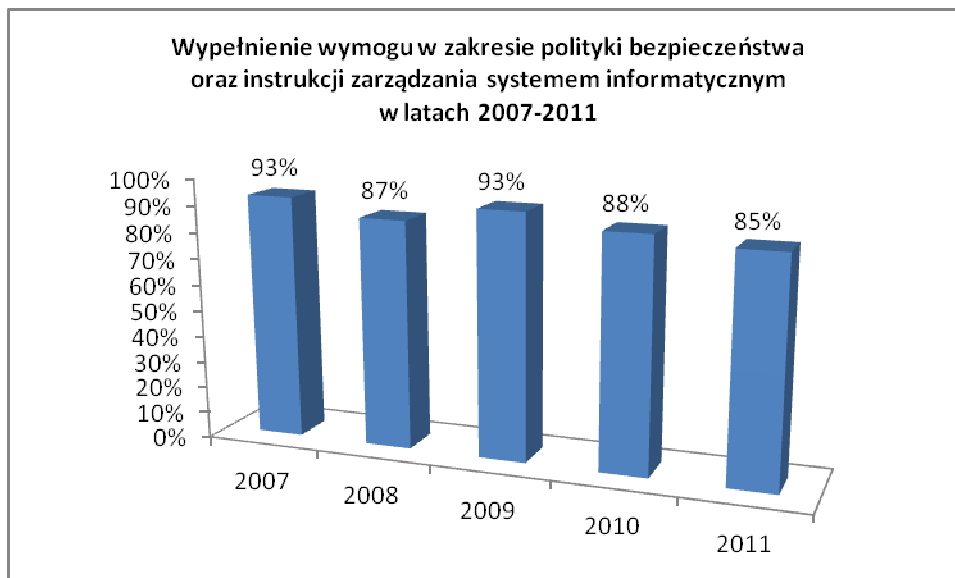
osobowych używane były przeważnie tylko jeden lub dwa systemy informatyczne. Na mniejszą liczbę skontrolowanych systemów informatycznych miał również wpływ charakter dużej grupy przeprowadzonych kontroli częściowych, polegających na sprawdzeniu, czy w przetwarzanych przez kontrolowany podmiot zbiorach danych znajdują się informacje o określonej osobie. Ponadto w 2011 r. przeprowadzane były kontrole sektorowe w podmiotach telekomunikacyjnych dotyczących retencji danych, które swoim zakresem obejmowały jedynie kwestie przetwarzania danych retencyjnych. W większości przypadków dane te były przetwarzane w specjalistycznych systemach informatycznych dostosowanych funkcjonalnie do ich przetwarzania. Zauważyć należy również, że w wielu podmiotach do przetwarzania danych osobowych używano systemów informatycznych, które często służą do przetwarzania kilku różnych zbiorów danych osobowych. Wskazane wyżej czynniki miały istotny wpływ na mniejszą liczbę sprawdzanych systemów informatycznych.

2.4. Wyniki kontroli w zakresie wypełnienia obowiązków formalnych i organizacyjnych

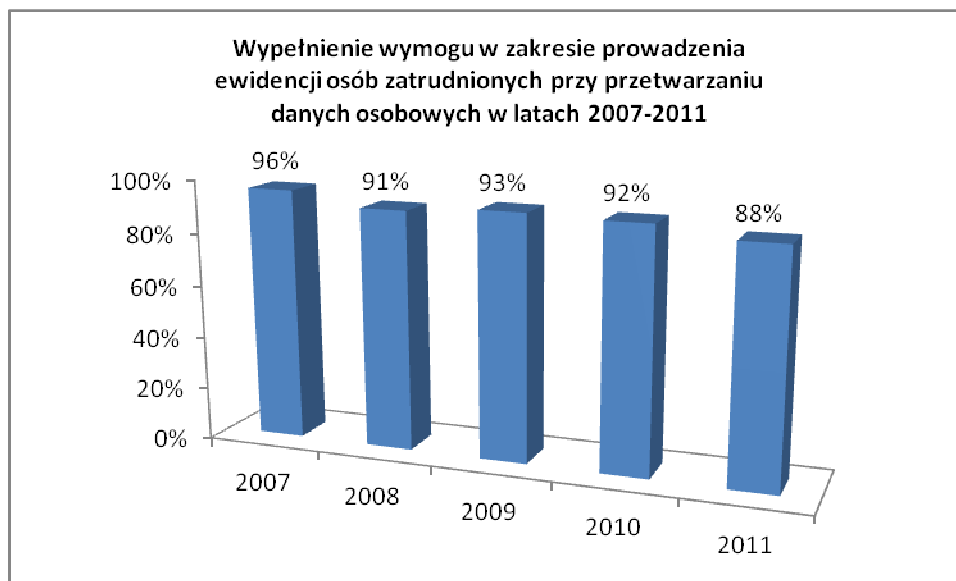
Realizacja w latach 2007-2011 wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie o ochronie danych osobowych i rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zobrażona została poniżej w formie wykresów. Pokazują one procentowe wyniki kontroli w odniesieniu do ogólnej liczby kontroli w danym roku lub ogólnej liczby kontrolowanych w danym roku systemów informatycznych. Zamieszczone informacje odnoszące się do prowadzonej dokumentacji procesu przetwarzania danych, obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, czy też powołania administratora bezpieczeństwa informacji oceniano w skali procentowej w stosunku do liczby kontrolowanych podmiotów. Natomiast warunki odnoszące się do wymagań funkcjonalnych, jakie powinny posiadać systemy informatyczne, oceniane były w skali procentowej do liczby systemów objętych kontrolą.

W przypadku, 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 przetwarzania danych osobowych w zakresie wymogów formalno-organizacyjnych, realizację wymogu prowadzenia dokumentacji uznawano za prawidłową. Sprawdzano również, czy wyznaczony został administrator bezpieczeństwa informacji oraz czy osoby dopuszczone do przetwarzania danych posiadały stosowne upoważnienia nadane przez administratora danych.

Stopień wypełnienia przez kontrolowane podmioty ww. warunków w latach 2007-2011 przedstawiono na poniższych wykresach.

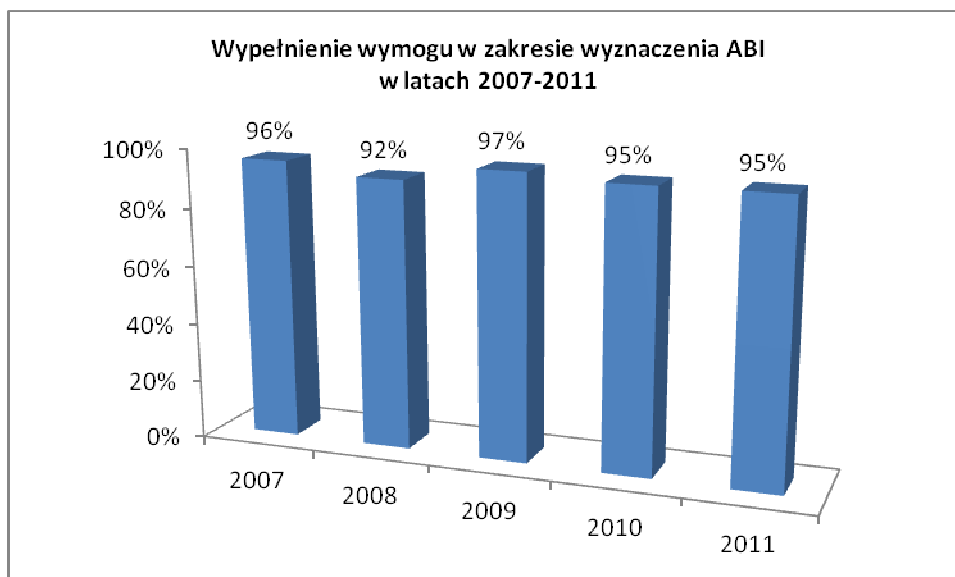


Wykres 3: Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych (polityka bezpieczeństwa i instrukcja zarządzania systemem).

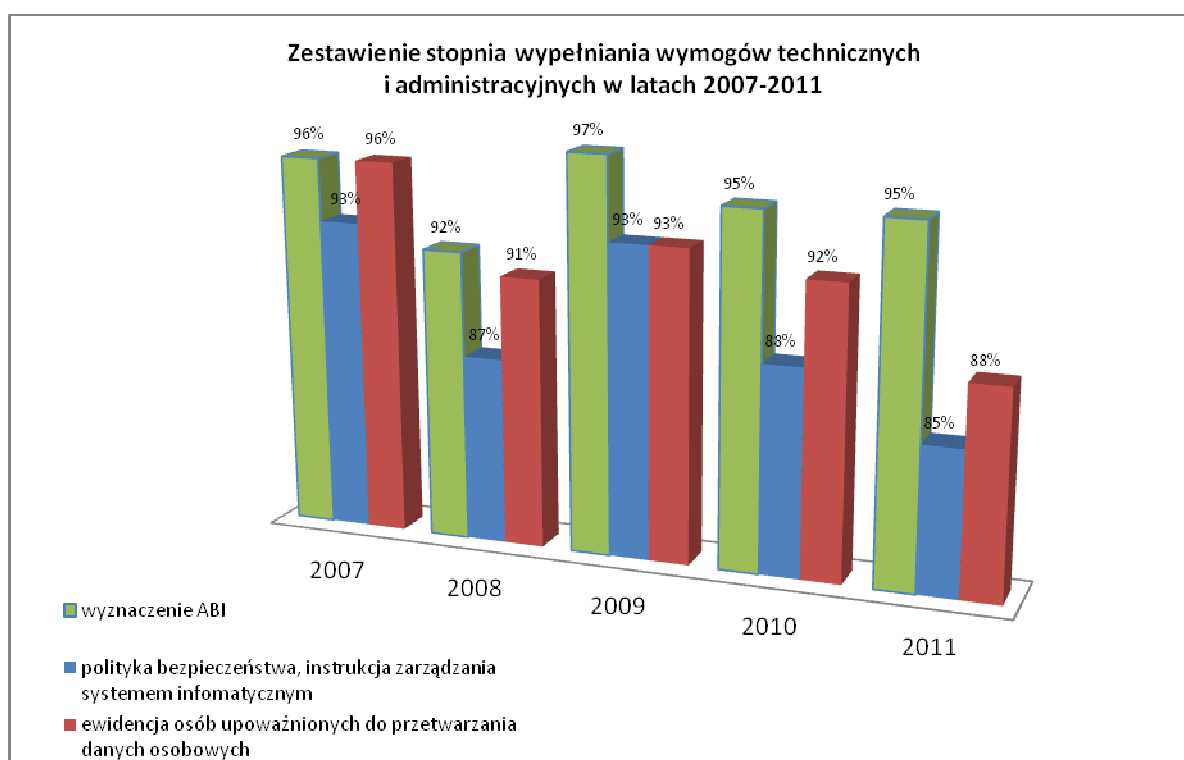


Wykres 4: Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

Zbiorcze zestawienie wypełnienia wymogów formalnych i organizacyjnych w latach 2007-2011 w zakresie dotyczącym prowadzenia dokumentacji przetwarzania danych osobowych oraz wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji, zestawiono na poniższym wykresie.



Wykres 5: Stopień realizacji obowiązku w zakresie wyznaczenia Administratora Bezpieczeństwa Informacji.

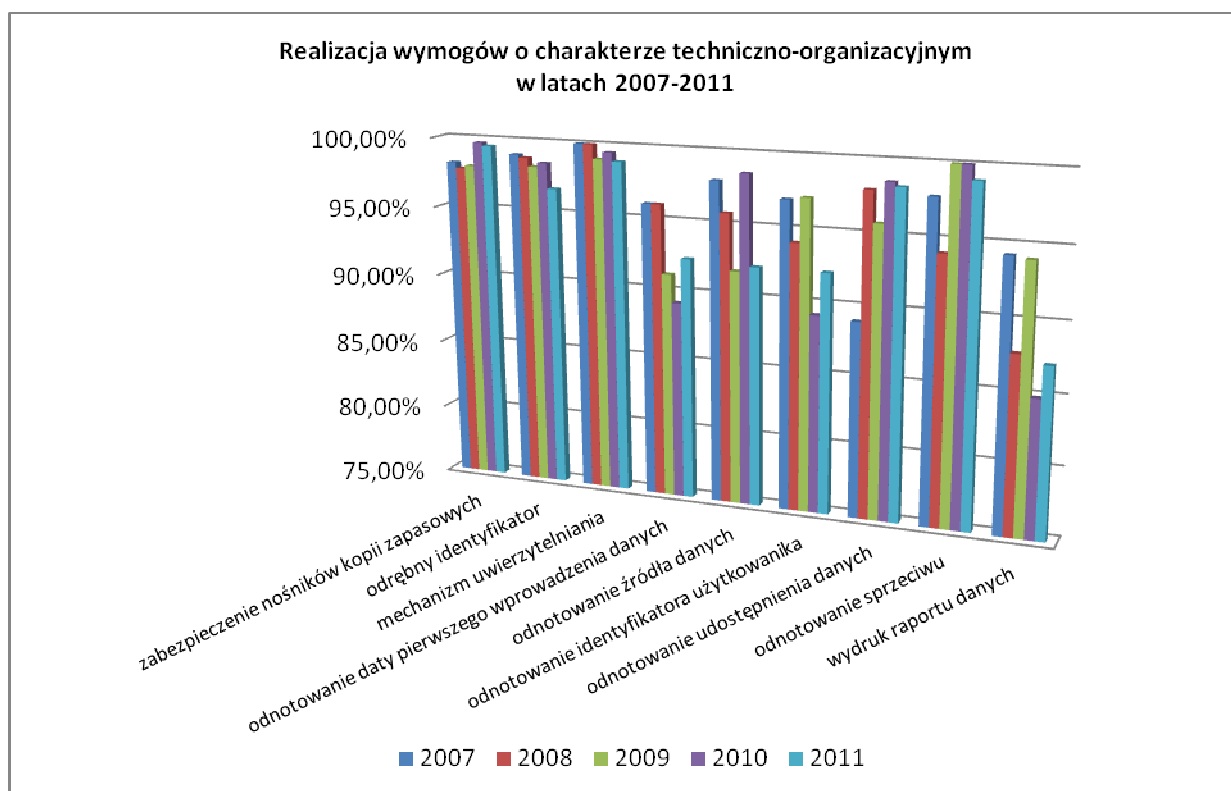


Wykres 6: Stopień realizacji obowiązku prowadzenia dokumentacji stanowiącej politykę bezpieczeństwa, instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wypełnienie obowiązku wyznaczenia osoby pełniącej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

2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych

Podczas wykonywania czynności kontrolnych w 2011 r. skontrolowano 384 systemy informatyczne służące do przetwarzania danych osobowych. Systemy te opierały się o bardzo różnorodne rozwiązania technologiczne: 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.

Jednostkę statystyczną w zestawieniach odnoszących się do stopnia realizacji technicznych warunków przetwarzania danych osobowych stanowił kontrolowany system informatyczny. Jeśli system informatyczny posiadał wymaganą funkcjonalność, lub funkcjonalność ta była realizowana przy użyciu dedykowanych modułów programowych zgodnie z warunkami określonymi w § 7 ust. 4 rozporządzenia, poszczególne warunki uznawano dla systemu objętego kontrolą za spełnione. Stopień realizacji wymogów o charakterze techniczno-organizacyjnym dla systemów informatycznych objętych kontrolą w roku 2011, w porównaniu do lat 2007-2009, przedstawia Wykres 7.

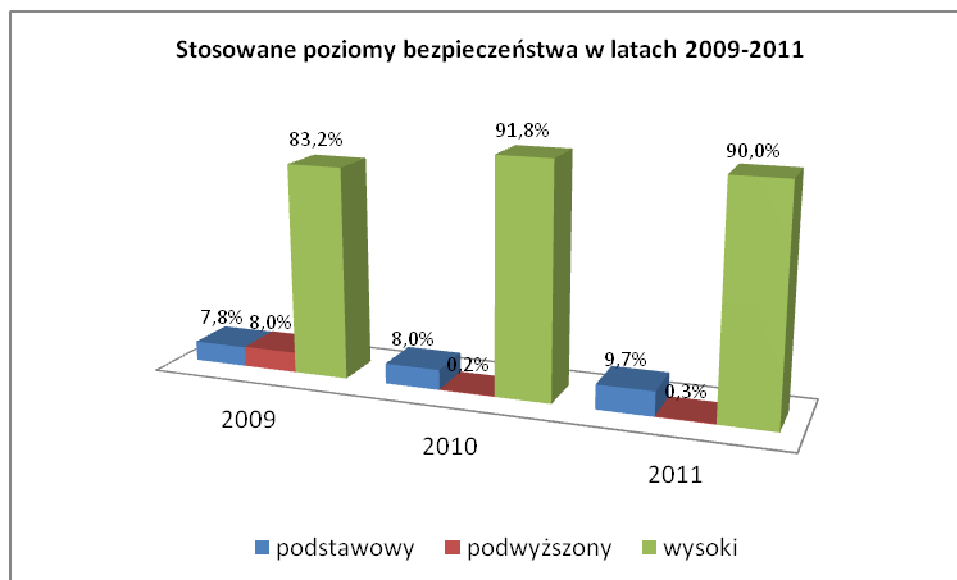


Wykres 7: *Stopień realizacji wymogów technicznych i organizacyjnych w latach 2007-2011.*

Przeprowadzone w 2011 r. kontrole pokazują również, że niemal 100% skontrolowanych jednostek przetwarzało dane osobowe z wykorzystaniem systemów informatycznych. Przypadki

przetwarzania danych osobowych wyłącznie w formie tradycyjnej (papierowej) dotyczyły jedynie kilku skontrolowanych podmiotów.

Podział na poziomy bezpieczeństwa w odniesieniu do skontrolowanych w latach 2009 - 2011 r. systemów informatycznych przedstawiony został poniższym wykresie.



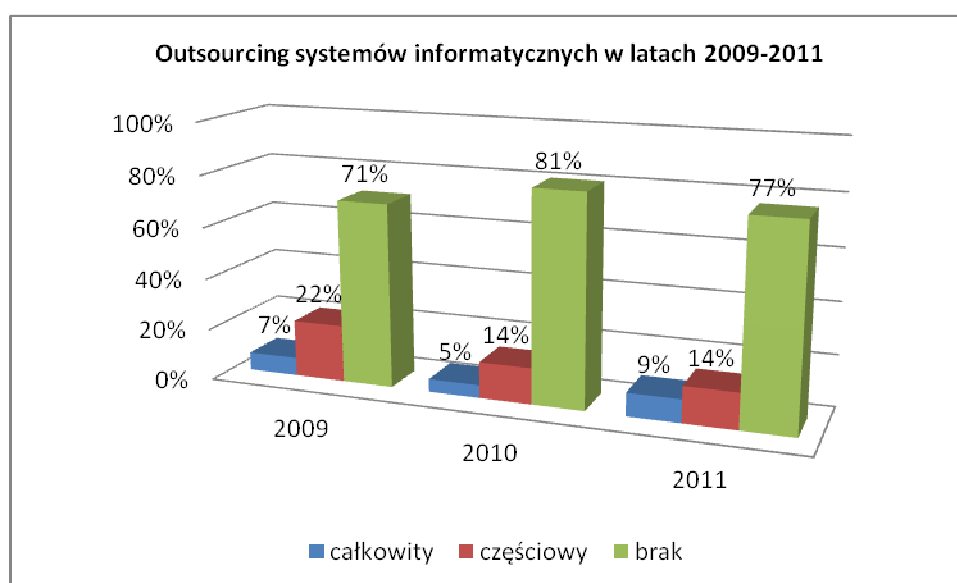
Wykres 8: *Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych skontrolowanych w latach 2009-2011.*

Jak wynika z ww. wykresu, znaczna część podmiotów skontrolowanych w 2011 r. (tj. nieco powyżej 90 %) zastosowała wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Stwierdzono również niewielki wzrost zabezpieczeń na poziomie podstawowym. Wiąże się to z tym, że część kontrolowanych systemów informatycznych były to systemy monitoringu, które w większości przypadków nie są podłączone do sieci publicznej, a co za tym idzie, wystarczającym zabezpieczeniem dla przetwarzanych za pomocą tych systemów danych jest poziom podstawowy.

Jak wynika z przeprowadzonych kontroli większość podmiotów do przetwarzania danych wykorzystuje systemy, nad którymi posiadają w pełni wyłączną kontrolę. Całkowity outsourcing, gdzie proces przetwarzania danych osobowych, jak również oprogramowanie i sprzęt teleinformatyczny administrator danych powierzył w całości do administrowania podmiotom zewnętrznym, w 2011 r. stosowany był tylko w odniesieniu do około 9 % systemów informatycznych. Jest to liczba większa niż w latach ubiegłych. W 2011 r. zauważono natomiast wśród skontrolowanych systemów informatycznych zmniejszenie liczby tych systemów, których obsługą techniczną i administracją zajmowali się pracownicy administratora danych (77 % systemów informatycznych). Bez zmian w porównaniu do roku 2010 pozostaje liczba systemów objętych częściowym outsourcingiem, gdzie podmiotom zewnętrznym powierzano tylko niektóre aspekty związane

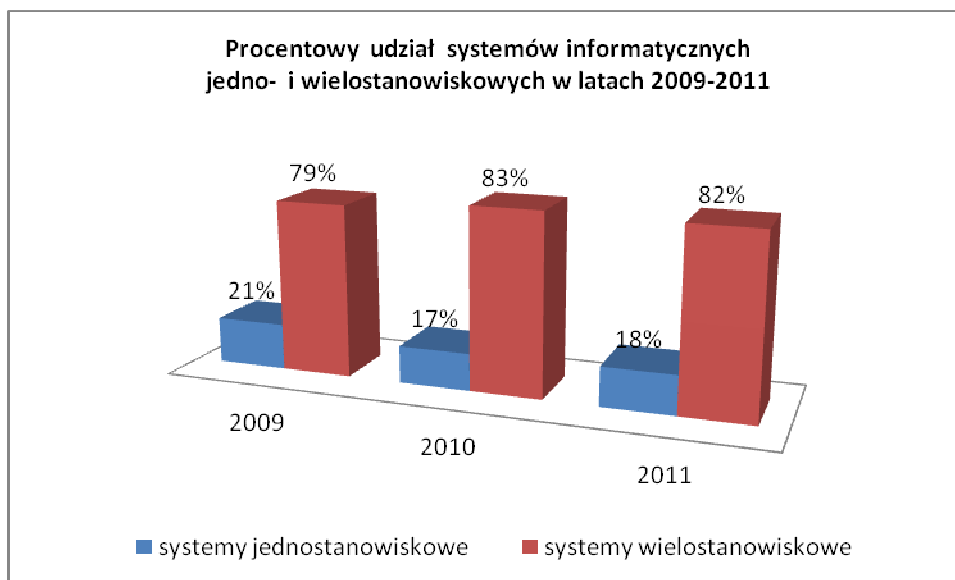
z utrzymywaniem systemu typu kolokacja maszyn stanowiących platformę sprzętową dla użytkowanych systemów informatycznych, czy wykonywanie czynności administracyjnych, typu zarządzanie bazą danych, wykonywanie kopii zapasowych, itp. Outsourcing częściowy stosowany był w 14 % skontrolowanych w 2011 systemach.

Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2009-2011 przedstawiono na poniższym wykresie.



Wykres 9: ***Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2009-2011.***

Jak przedstawiono na poniższym Wykresie 10, w 2011 r. w porównaniu z latami 2009-2010 liczba wykorzystywanych wielostanowiskowych systemów informatycznych znajduje się mniej więcej na stałym poziomie (powyżej 80 %). Rozwiązania oparte o systemy jedno stanowiskowe stanowiły niecałe 20 % 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) lub specyfika ich zastosowania (np. systemy monitoringu).



Wykres 10: *Procentowy udział systemów informatycznych jedno- i wielostanowiskowych wśród systemów objętych kontrolą w latach 2009-2011.*

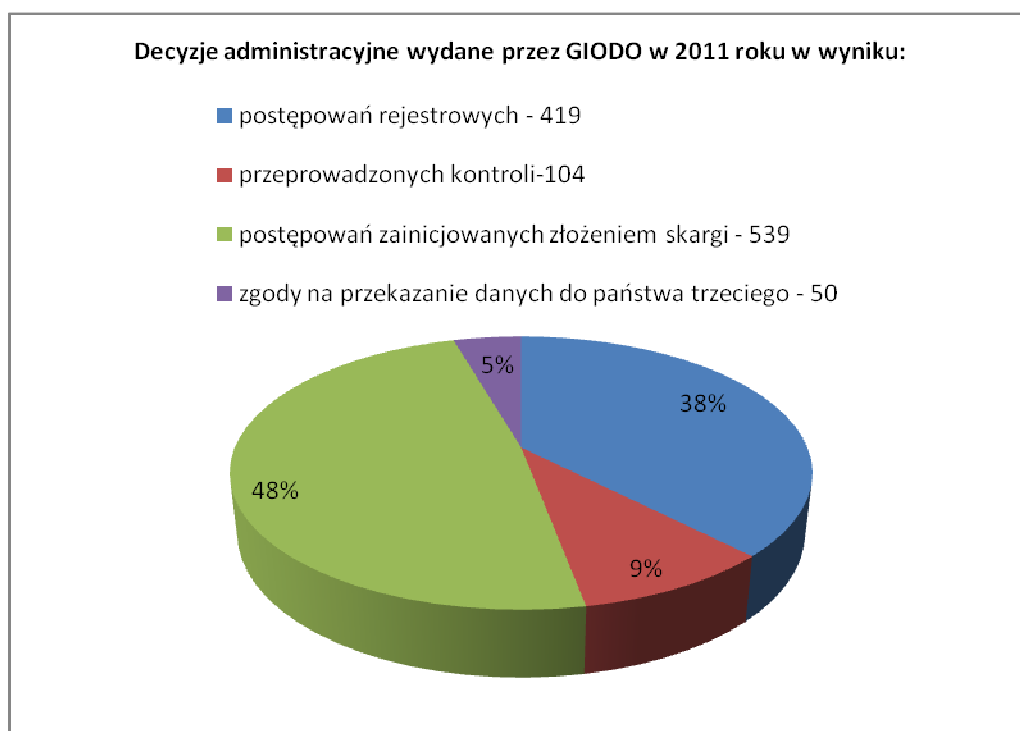
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych

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 2011 r. Generalny Inspektor wydał **1112 decyzji administracyjnych**, tj. o 300 mniej w stosunku do roku 2010, w którym wydanych było 1412 decyzji. Spośród 1112 decyzji wydanych w 2011 r. **419** dotyczyło postępowań rejestrowych, **104** zostało wydanych w związku z przeprowadzonymi kontrolami, **539** wydano na skutek postępowania zainicjowanego skargą, zaś **50** dotyczyło zgody na przekazanie danych do państwa trzeciego. Charakterystyczny jest znaczny wzrost liczby decyzji w postępowaniu zainicjowanym skargą (359 decyzji w 2010 r. i 539 decyzji w 2011 r. – wzrost o 50 %). Sytuacja tak związana jest przede wszystkim ze zwiększeniem liczby samych skarg oraz z faktem, że skarżący częściej wskazują na rzeczywiście istniejące problemy dotyczące

przetwarzania danych i w precyzyjniejszy sposób zwracają uwagę GIODO na zdarzenia, wobec których Generalny Inspektor powinien podjąć działania przewidziane przez Kodeks postępowania administracyjnego i przez ustawę.



Wykres 11: Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2011 r.

3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych skierował do organu powołanego do ścigania przestępstw **10 zawiadomień o podejrzeniu popełnienia przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych**. W porównaniu z rokiem 2010, w którym wystosowano 23 zawiadomienia, stanowi to spadek o ponad połowę.

Niezmiennie najwięcej zawiadomień złożonych zostało w związku z informacjami przekazanymi Generalnemu Inspektorowi Ochrony Danych Osobowych przez podmioty indywidualne - **9 zawiadomień**. Należy w tym miejscu zaznaczyć, że na ogólną liczbę 10 zawiadomień skierowanych do organów ścigania, 4 z nich dotyczyły podejrzenia popełnienia przestępstwa z użyciem Internetu⁵⁹, 7 przypadków dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego w art. 49 ust. 1 ustawy, przetwarzania danych osobowych przez podmioty nieuprawnione⁶⁰, w tym 4 wspomniane przypadki dotyczyły podejrzenia popełnienia

⁵⁹ DOLiS/ZAW-5/11/20161, DOLiS/ZAW-6/11/26906, DOLiS/ZAW-9/11/50497, DOLiS/ZAW-10/11/63170.

⁶⁰ DOLiS/ZAW-1/11/14807, DOLiS/ZAW-2/11/17458, DOLiS/ZAW-4/11/19767, DOLiS/ZAW-5/11/20161, DOLiS/ZAW-6/11/26906, DOLiS/ZAW-9/11/50497, DOLiS/ZAW-10/11/63170.

przestępstwa z użyciem Internetu. W jednym z nich administrator portalu internetowego bezprawnie zamieścił i udostępniał innym osobom na swojej stronie internetowej dane osobowe skarżącego i jego rodziny w zakresie imienia, nazwiska, adresu, daty i miejsca urodzenia, pochodzenia, numerów telefonów (zarówno numeru prywatnego jak i do pracy), adresów e-mail oraz wizerunku. Nadto podkreślić należy, iż dane te zostały przedstawione przez administratora portalu w sposób rasistowski i wulgarny, a także nawołujący do przemocy wobec skarżącego z uwagi na jego kolor skóry i pochodzenie etniczne⁶¹. Kolejny z przypadków naruszenia art. 49 ust. 1 ustawy dotyczył przetwarzania danych osobowych zawartych w zaświadczeniu o zatrudnieniu złożonym w jednym z banków przez osobę prowadzącą oddział tego banku, do których przetwarzania nie była uprawniona, poprzez wykorzystanie ich do celów prywatnych⁶². W pozostałych przypadkach przedmiotem zawiadomień uczyniono podejrzenie popełnienia przestępstwa przez podmioty prowadzące działalność gospodarczą poprzez przetwarzanie danych osobowych bez podstawy prawnej⁶³.

Ponadto w jednym z przypadków zawiadomienie dotyczyło przestępstwa wskazanego w art. 51 ustawy, tj. udostępnienia danych osobowych podmiotom nieuprawnionym przez osoby odpowiedzialne w Urzędzie Miejskim za przetwarzanie danych osobowych w związku z postępowaniami administracyjnymi prowadzonymi przez Burmistrza Miasta⁶⁴.

W jednym z zawiadomień Generalny Inspektor stwierdził wypełnienie znamion czynu zabronionego wskazanego w art. 52 ustawy o ochronie danych osobowych przez osoby odpowiedzialne za przetwarzanie danych osobowych w Szpitalu Wojewódzkim poprzez zagubienie dokumentacji medycznej jednego z pacjentów⁶⁵.

Natomiast tylko 1 zawiadomienie miało związek z przeprowadzonymi kontrolami⁶⁶. Na podstawie materiału dowodowego dotyczącego szpitala, przesłanego przez marszałka jednego z województw, skierowano zawiadomienie o popełnieniu przestępstw wskazanych w art. 51 i art. 52 ustawy o ochronie danych osobowych⁶⁷, polegających odpowiednio na: umożliwieniu dostępu do danych osobowych pacjentów tego szpitala zawartych w zaświadczeniach lekarskich oraz niezabezpieczeniu tych danych przed zabraniami przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Na skutek zawiadomienia Generalnego Inspektora zostało wszczęte dochodzenie, które następnie umorzono ze względu na brak znamion czynu zabronionego (w odniesieniu do znamion z art.

⁶¹ DOLiS/ZAW-10/11/63170

⁶² DOLiS/ZAW-2/11/17458

⁶³ DOLiS/ZAW-1/11/14807, DOLiS/ZAW-4/11/19767.

⁶⁴ DOLiS/ZAW-3/11/18565

⁶⁵ DOLiS/ZAW-8/11/43946

⁶⁶ DIS/ZAW/-7/39615/11

⁶⁷ Art. 51 ust. 1 ustawy o ochronie danych osobowych. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniami przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

51) oraz niewykrycie sprawcy przestępstwa określonego w art. 52 ustawy o ochronie danych osobowych.

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

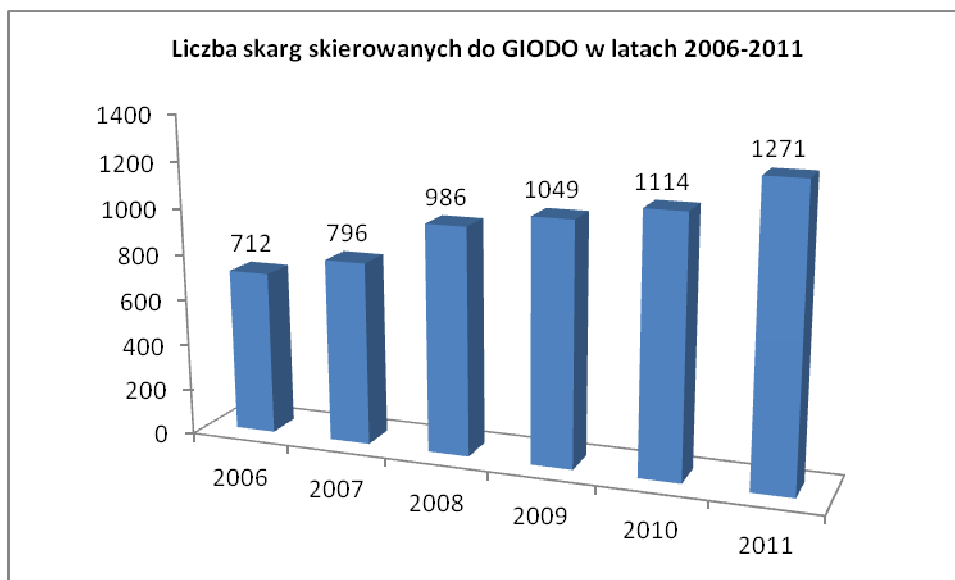
Liczbę zawiadomień o podejrzeniu popełnienia przestępstwa składanych przez Generalnego Inspektora w latach 2009-2011 przedstawia Wykres 12.



Wykres 12: Porównanie liczby zawiadomień o podejrzeniu popełnienia przestępstwa kierowanych przez GIODO w latach 2009-2011.

3.3. Rozpatrywanie skarg

W 2011 r. do Departamentu Orzecznictwa, Legislacji i Skarg wpłynęło **1271 skarg** dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2010, w którym wpłynęło 1114 skarg, liczba ta uległa zwiększeniu o 157, co przedstawia Wykres 13.



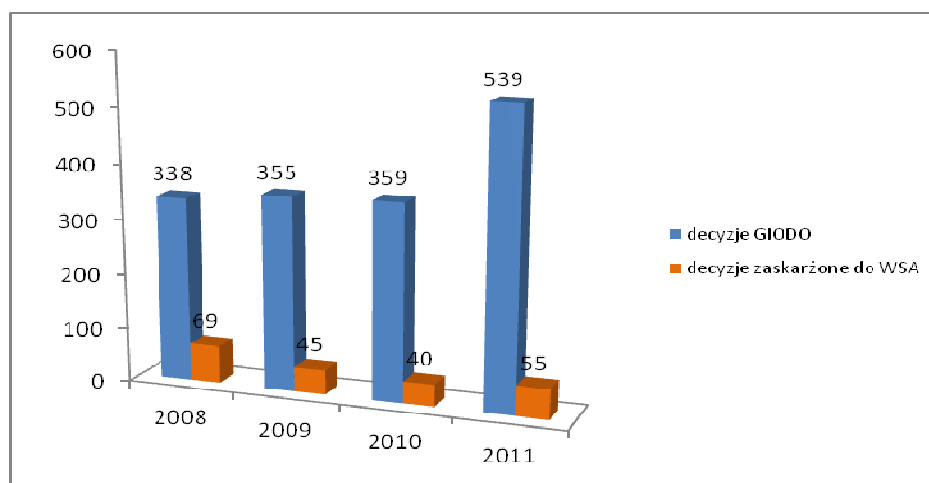
Wykres 13: Zestawienie porównawcze liczby skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009–2011 r.

Każda ze skarg analizowana była na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego. W przypadku tych, które je spełniały, Generalny Inspektor Ochrony Danych Osobowych inicjował postępowania administracyjne. Jeżeli w ich toku stwierdzał naruszenie przepisów ustawy o ochronie danych osobowych, wydawał decyzje administracyjne i zgodnie z art. 18 ustawy o ochronie danych osobowych 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 skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych z urzędu, wydanych zostało **539 decyzji administracyjnych**, z których **55** zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie (WSA). Charakterystyczny jest znaczny wzrost liczby decyzji w postępowaniu zainicjowanym skargą (359 decyzji w 2010 r. i 539 decyzji w 2011 r. – wzrost o 50 %). Sytuacja tak związana jest przede wszystkim ze zwiększeniem liczby samych skarg oraz z faktem, że skarżący częściej wskazują na rzeczywiście istniejące problemy dotyczące przetwarzania danych i w precyzyjniejszy sposób zwracają uwagę GODO na zdarzenia, wobec których Generalny Inspektor powinien podjąć działania przewidziane przez Kodeks postępowania administracyjnego i przez ustawę.

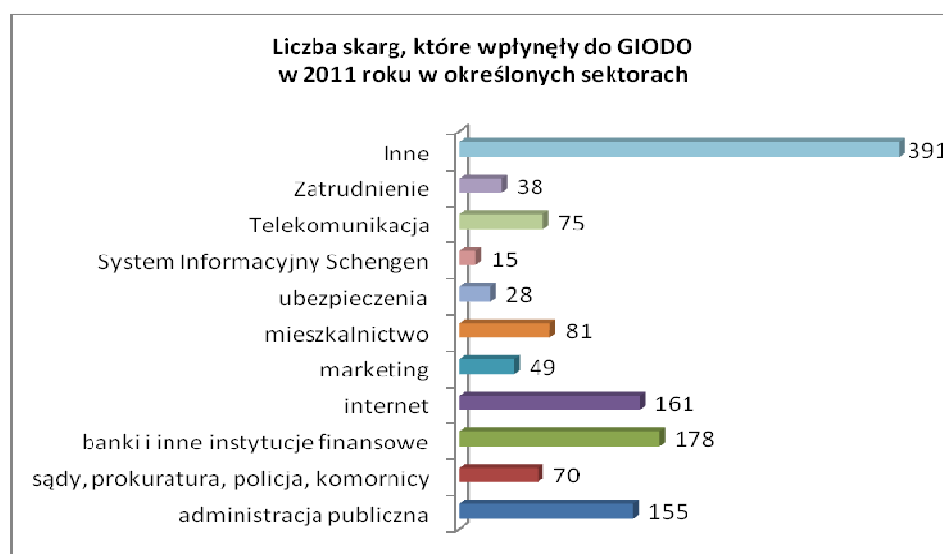
W porównaniu z rokiem 2010, w którym 40 decyzji zostało zaskarżonych, zaobserwowano wzrost o liczby zaskarżonych decyzji o 15 (wzrost o 22 %). Należy jednak pamiętać, że sama liczba

decyzji wzrosła w tym samym okresie o 50 %. Oznacza to, że o ile w 2010 r. zaskarżono do WSA 11 % decyzji GIODO wydanych w postępowaniu zainicjowanym skargami o tyle w 2011 r. zaskarżono 10 % takich decyzji.



Wykres 14: *Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011 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.

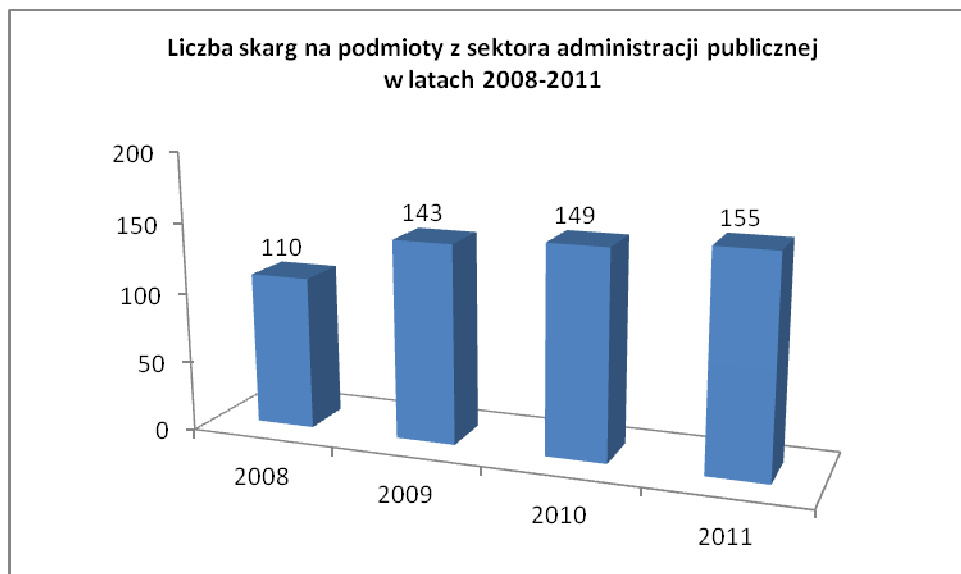


Wykres 15: *Zestawienie porównawcze liczby skarg, które wpłynęły do Biura GIODO w 2011 r. w określonych sektorach.*

Poniżej zostaną przedstawione przykłady skarg, które wpłynęły w 2011 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych na podmioty działające w wybranych obszarach.

1) Administracja publiczna

W omawianym roku 2011, Generalny Inspektor Ochrony Danych Osobowych - podobnie jak w latach poprzednich - najwięcej wystąpień kierował do podmiotów z sektora **administracji publicznej**. W analizowanym okresie sprawozdawczym do GIODO wpłynęło **155** skarg dotyczących tego sektora. Zbliżona liczba skarg z tego zakresu wpłynęła także w 2010 r.- 149.



Wykres 16: *Zestawienie porównawcze liczby skarg na podmioty z sektora administracji publicznej, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

W omawianym okresie GIODO wydał decyzję nakazującą Straży Miejskiej wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego poprzez usunięcie jego danych osobowych w zakresie informacji o jego stanie zdrowia⁶⁸. W uzasadnieniu tego rozstrzygnięcia organ ds. ochrony danych osobowych - mając na uwadze, że skarżący zakwestionował legalność przetwarzania przez Straż Miejską jedynie danych w zakresie jego stanu zdrowia - powołał art. 10a ustawy o Strażach Gminnych. Stosownie do treści tego przepisu, Straż w celu realizacji ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane: 1) w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia, 2) z rejestrów, ewidencji

⁶⁸ Decyzja GIODO z dnia 11 lutego 2011 r., znak: DOLiS/DEC-95/11/6055,6057.

i zbiorów, do których Straż posiada dostęp na podstawie odrębnych przepisów. Zatem w ocenie Generalnego Inspektora Ochrony Danych Osobowych nie budziło wątpliwości, że Straż Miejska nie mogła przetwarzać danych osobowych w zakresie informacji o stanie zdrowia, gdyż żaden przepis prawa nie zezwalał na takie działanie.

W omawianym okresie sprawozdawczym GODO wydawał decyzje nakazujące organom administracji wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżących poprzez usunięcie ze strony internetowej Biuletynu Informacji Publicznej tych organów danych osobowych skarżących w określonym zakresie⁶⁹. Generalny Inspektor Ochrony Danych Osobowych wskazywał w przedmiotowych rozstrzygnięciach, iż na organie administracji - jako administratorze danych osobowych - spoczywają konkretne obowiązki określone w ustawie o ochronie danych osobowych. Z punktu widzenia tych spraw istotny był obowiązek ustanowiony w art. 26 ust. 1 pkt 3 ustawy, zgodnie z którym 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 merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Wyrażona w przytoczonym przepisie zasada adekwatności oznaczała, że cyt.: „(...) swym rodzajem i swą treścią dane nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania (...)”⁷⁰. W ocenie Generalnego Inspektora Ochrony Danych Osobowych w przedmiotowych sprawach przy realizacji obowiązku ogłoszenia na stronie internetowej Biuletynu Informacji Publicznej informacji publicznej, w treści której udostępniono dane osobowe skarżących, nie uwzględniono ich prawa do prywatności. Jednocześnie została naruszona wspomniana wyżej zasada adekwatności. Zdaniem organu ochrony danych osobowych przy upublicznieniu dokumentów jedynie w celu informacyjnym zbędne było (nieadekwatne do celu) ujawnianie danych osobowych skarżących w zbyt szerokim zakresie. Publikacja dokumentu zawierającego dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna nastąpić po odpowiednim przetworzeniu danych osobowych w nim zawartych. W niniejszych sprawach oznaczało to, że przedmiotowe dokumenty powinny zostać upublicznione po uprzednim usunięciu danych osobowych skarżących.

Powyższe potwierdził Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 18 listopada 2008 r.⁷¹ uznając, iż „usunięcie personaliów osób prywatnych, czy też ich zanonimizowanie w ogłoszonej w BIP uchwale organu gminnego, nie wpływa na czytelność dokonanego w ten sposób przekazu. W tym przypadku treść aktu administracyjnego nie traci waloru informacyjnego, albowiem wynika z niej kto, kiedy i w jakiej sprawie publicznej zajął określone stanowisko. Podstawowym celem

⁶⁹ zob. DOLiS/DEC-96/11/6059,6062 dot. DOLiS-440-421/10; DOLiS/DEC-102/11/6445,6447 dot. DOLiS-440-628/10; DOLiS/DEC-105/11/6590,6592 dot. DOLiS-440-440/10; DOLiS/DEC-224/11/12639,12644 dot. DOLiS-440-45/11.

⁷⁰ J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych, Komentarz, Zakamycze 2004, s. 556.

⁷¹ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 18 listopada 2008 r. sygn. akt II SA/Wa 1177/08.

BIP jest powszechne informowanie o sprawach publicznych i w tym przypadku cel ten został zrealizowany. Prezentowanie odmiennego poglądu pozostaje w sprzeczności z konstytucyjnymi gwarancjami wolności i praw obywatela. W świetle art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia nie mogą naruszać istoty wolności i praw”.

W rozpatrywanym czasie GODO wystąpił o uwzględnienie przy podejmowanych przez prezydenta miasta działaniach odnoszących się do publikacji oświadczeń majątkowych w Biuletynie Informacji Publicznej, zasad wynikających z przepisów ustawy o ochronie danych osobowych⁷². W wystąpieniu tym Generalny Inspektor Ochrony Danych Osobowych wskazał, iż pomimo tego, że skarżący pełnił funkcję publiczną i upubliczniona wraz z oświadczeniem majątkowym skarżącego korespondencja pomiędzy nim a prezydentem (zawierająca jego dane osobowe) wiązała się z tym oświadczeniem, to nie wszystkie informacje dotyczące osób publicznych powinny podlegać ujawnieniu. W ocenie Generalnego Inspektora Ochrony Danych Osobowych upublicznienie danych skarżącego w zakresie obejmującym korespondencję prowadzoną z prezydentem miasta, naruszyło zasadę adekwatności przetwarzania danych, o której mowa w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Zgodnie z powołanym przepisem 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 merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Kwestionowane przez skarżącego upublicznienie jego danych nie było adekwatne do celu, w jakim dane te powinny być przetwarzane. Powód, dla którego ww. korespondencja była prowadzona, wynikał z konieczności przeprowadzenia przez prezydenta postępowania mającego na celu wyjaśnienie źródeł dochodów skarżącego, nie zaś informowania opinii publicznej o trwającym postępowaniu wyjaśniającym. Ponadto ze zgromadzonego w sprawie materiału dowodowego nie wynikało, aby ktokolwiek był zainteresowany ww. postępowaniem i wnosił o udostępnienie tych informacji w trybie ustawy o dostępie do informacji publicznej.

W omawianym 2011 roku GODO wydał także decyzję nakazującą Narodowemu Funduszowi Zdrowia udostępnienie oddziałowi kardiologii uniwersytetu medycznego, danych osobowych w zakresie daty i przyczyny hospitalizacji po wypisie z tego oddziału (zwłaszcza wszystkich postaci choroby wieńcowej, udaru mózgu, migotania przedsionków, cukrzycy) oraz wykonania procedur rewaskularyzacji przezskórnej (z lub bez implantacji stentu) oraz pomostowania aortalno-wieńcowego dotyczących powtórnych hospitalizacji chorych, osób uprzednio leczonych w ww. oddziale⁷³.

⁷² Pismo GODO z dnia 18 marca 2011 r. znak: DOLiS-440-734/10/12158/11.

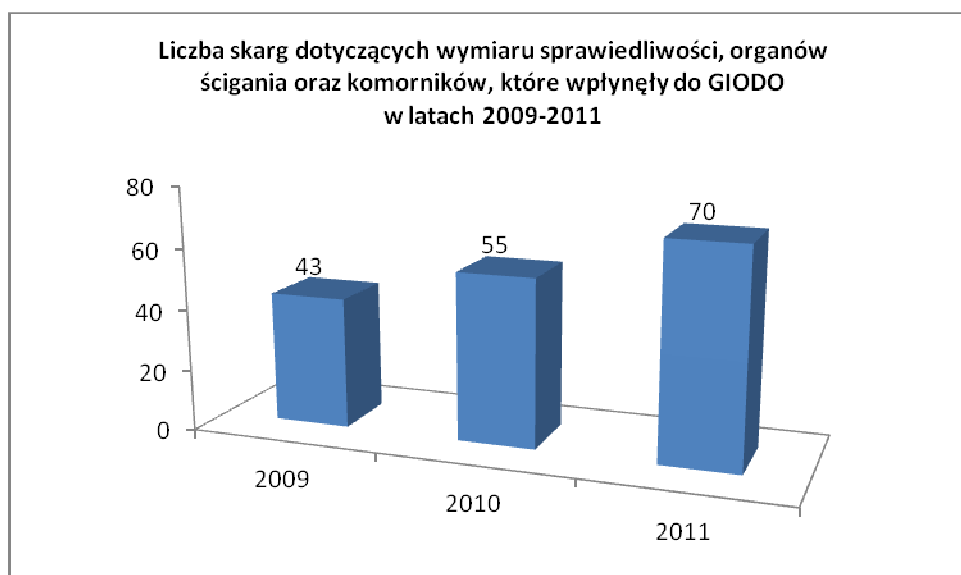
⁷³ DOLiS/DEC-288/11/15718,15719 dot. DOLiS-440-571/10.

W uzasadnieniu tego rozstrzygnięcia organ stwierdził, iż okoliczność, że art. 188 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych wskazywał cele, w jakich NFZ mógł przetwarzać dane osobowe ubezpieczonych, nie wykluczała legalności udostępnienia danych w celu prowadzenia badań naukowych w sytuacji, gdy publikowanie wyników badań naukowych nastąpi w sposób uniemożliwiający identyfikację osób, których dane zostaną udostępnione, bowiem przesłanką legalizującą takie udostępnienie będzie art. 27 ust. 2 pkt 9 ustawy o ochronie danych osobowych.

Za nieuzasadnione natomiast uznawane były skargi, w których skarżący, jako podmioty nieuprawnione, wskazywali osoby uczynione stroną postępowań przez odrębne organy administracji publicznej. Jako przykład można wskazać sprawy, w których skarżący kwestionowali legalność udostępnienia ich danych osobowych innym podmiotom, które zostały uznane przez organy administracji za strony postępowań, wszczętych na wniosek skarżących⁷⁴.

2) Sądy, prokuratura, Policja, komornicy

W analizowanym okresie do GODO wpłynęło **70** skarg dotyczących sektora **sądów, prokuratury, Policji i komorników**. Stanowi to nieznaczny wzrost w stosunku do 2010 r., w którym wpłynęło 55 skarg z tego sektora.



Wykres 17: *Zestawienie porównawcze liczby skarg dotyczących sektora sądów, prokuratury, Policji i komorników, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

⁷⁴ Zob. DOLiS/DEC-600/11/35334,35337,35340,35342 dot. DOLiS-440-977/09, DOLiS/DEC-909/11/52236,52238 dot. DOLiS-440-560/10.

W jednej ze spraw GODO wydał decyzję nakazującą Komendantowi Wojewódzkiemu Policji spełnienie wobec skarżącego obowiązku informacyjnego, o którym mowa w art. 33 ustawy o ochronie danych osobowych, poprzez poinformowanie go o pełnej nazwie i adresie swojej siedziby, jako administratora danych osobowych, o celu, zakresie i sposobie przetwarzania jego danych w zbiorach oraz sposobie udostępniania jego danych, a także w jakim zakresie i komu jego dane zostały udostępnione⁷⁵. W uzasadnieniu tego rozstrzygnięcia Generalny Inspektor Ochrony Danych Osobowych jednoznacznie wskazał, że komendant nie dopełnił wobec skarżącego obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych, w zakresie wnioskowanym przez skarżącego i we wskazanym ustawowo terminie.

Część skarg wpływających do Biura Generalnego Inspektora Ochrony Danych Osobowych dotyczyła przetwarzania danych osobowych skarżących w Krajowym Systemie Informacji Policji⁷⁶. W swoich decyzjach wydanych w 2011 roku z tego zakresu⁷⁷, Generalny Inspektor nakazywał Komendantowi Policji usunięcie danych osobowych skarżących z Krajowego Systemu Informacji Policji. GODO wskazywał, że przy ocenie zasadności odmowy usunięcia danych osobowych skarżących ze zbioru KSIP zastosowanie znajduje § 11 ust. 3 rozporządzenia w sprawie przetwarzania przez Policję informacji o osobach⁷⁸, przewidujący możliwość usunięcia danych po dokonaniu oceny przetwarzanych informacji o osobach pod kątem ich przydatności w prowadzonych postępowaniach oraz niezbędności w realizacji zadań ustawowych Policji. Niemniej jednak, jak podkreślił Generalny Inspektor, powyższa regulacja nie zawiera jednoznacznych zapisów o terminie przechowywania danych, co stało się przedmiotem wystąpienia w 2010 r. Generalnego Inspektora Ochrony Danych Osobowych do Ministra Spraw Wewnętrznych i Administracji o rozważenie zasadności podjęcia działań legislacyjnych mających na celu nowelizację przepisów regulujących przetwarzanie danych osobowych w Krajowym Systemie Informacyjnym Policji, poprzez wprowadzenie do nich regulacji precyzyjnie określających okresy, w których Policja może przetwarzać pozyskane dane osobowe⁷⁹. Niemniej jednak w obecnym stanie prawnym, w ocenie organu do spraw ochrony danych osobowych, zastosowanie w kwestii przetwarzania danych osobowych w KSIP będą miały przepisy ustawy o ochronie danych osobowych.

Ponadto GODO podkreślił, że każdy przypadek przetwarzania w KSIP danych osobowych musi odbywać się także z poszanowaniem zasad wyznaczonych przepisami ustawy o ochronie danych osobowych. Zdaniem organu dalsze przetwarzanie w KSIP danych osób skarżących należy uznać za

⁷⁵ DOLiS/DEC-242/11/13660,13661,13663 dot. DOLiS-440-571/10.

⁷⁶ np. DOLiS-440-698/11, DOLiS-440-699/11, DOLiS-440-963/11, DOLiS-440-1213/11.

⁷⁷ zob. DOLiS/DEC-188/11/10381,10385 dot. DOLiS-440-712/10.

⁷⁸ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 5 września 2007 r. w sprawie przetwarzania przez Policję informacji o osobach, Dz. U. z 2007 r. Nr 170, poz. 1203.

⁷⁹ 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.

zbędne dla realizacji celu, jakim jest realizacja zadań ustawowych Policji oraz możliwość wykorzystania gromadzonych informacji w innych postępowaniach skoro nie są prowadzone jakiejkolwiek czynności przeciwko skarżącym przez Policję. Zatem opisane powyżej działanie naraża Komendanta Policji, jako administratora przedmiotowych danych, na zarzut naruszenia wskazanego powyżej art. 26 ust. 1 ustawy o ochronie danych osobowych.

3) Banki i inne instytucje finansowe

W analizowanym 2011 r. do GIODO wpłynęło **178** skarg dotyczących sektora **banków i innych instytucji finansowych**, tj. o 59 więcej niż w roku 2010, w którym skarg tych było 119.



Wykres 18: *Zestawienie porównawcze liczby skarg dotyczących sektora banków i innych instytucji finansowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

W omawianym okresie GIODO zwrócił się do banków, aby uwzględniały w ramach prowadzonej działalności zasady wynikające z ustawy o ochronie danych osobowych, zwłaszcza jej art. 26 ust. 1, stanowiącego o obowiązku administratora danych dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą⁸⁰. Dane przetwarzane były bowiem często nieaktualne, co rzutowało na sytuację prawną osób np. ubiegających się o kredyt.

Jako przykład można wskazać wystąpienie Generalnego Inspektora Ochrony Danych Osobowych z dnia 18 kwietnia 2011 r. w którym wskazał, iż poprzez działanie jednego z banków informacje zawarte w bazie Biura Informacji Kredytowej S.A. przez okres około 4 lat nie

⁸⁰ Pismo GIODO z dnia 18 kwietnia 2011 r. znak: DOLiS-440-641/10/18898/11, pismo GIODO z dnia 30 grudnia 2011 r. znak: DOLiS-440-773/09/64491/11.

odzwierciedlały faktycznej sytuacji prawnej skarżącego, a tym samym narażały go na powstanie negatywnych dla niego skutków. Opisane postępowanie banku znacząco wpływało na pogorszenie sytuacji życiowej osób, których nieaktualne lub nieprawdziwe dane osobowe były przetwarzane w bazie Biura Informacji Kredytowej S.A., gdyż z tego powodu ich zdolność kredytowa oceniana była negatywnie. Generalny Inspektor Ochrony Danych Osobowych zaznaczył, iż nie kwestionuje udostępnienia danych osobowych przez bank innemu podmiotowi (w tej sytuacji Biura Informacji Kredytowej S.A.), gdyż w przedstawionym stanie faktycznym było to uzasadnione na podstawie obowiązujących przepisów prawa, jednakże bank – jako administrator danych osobowych skarżącego – zobowiązany był, zgodnie z art. 26 ust. 1 ustawy, dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. „Szczególna staranność administratora danych zbliżona jest do kategorii tzw. staranności zawodowej. Oznacza to, że administrator danych jest obowiązany dochować staranności nie tyle o podwyższonym poziomie, ile staranności szczególnej w tym sensie, że związanej z jego działalnością, tj. decydowaniem o celach i środkach przetwarzania, a także przetwarzaniem danych osobowych. Celem tej staranności jest ochrona interesów osób, których dane dotyczą. Przejawem szczególnej staranności administratora danych jest w szczególności zabezpieczenie przed zagrożeniami dóbr osobistych osób, których dane dotyczą, przede wszystkim czci, sfery życia prywatnego, a także wolności”.⁸¹ W sytuacji, gdy administrator nie wywiązywał się z powyższego obowiązku, osoba, której dane były przetwarzane, miała prawo domagać się sprostowania (także usunięcia) danych nieprawdziwych. W szczególności bank, jako instytucja zaufania publicznego, powinien zapewnić przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa.

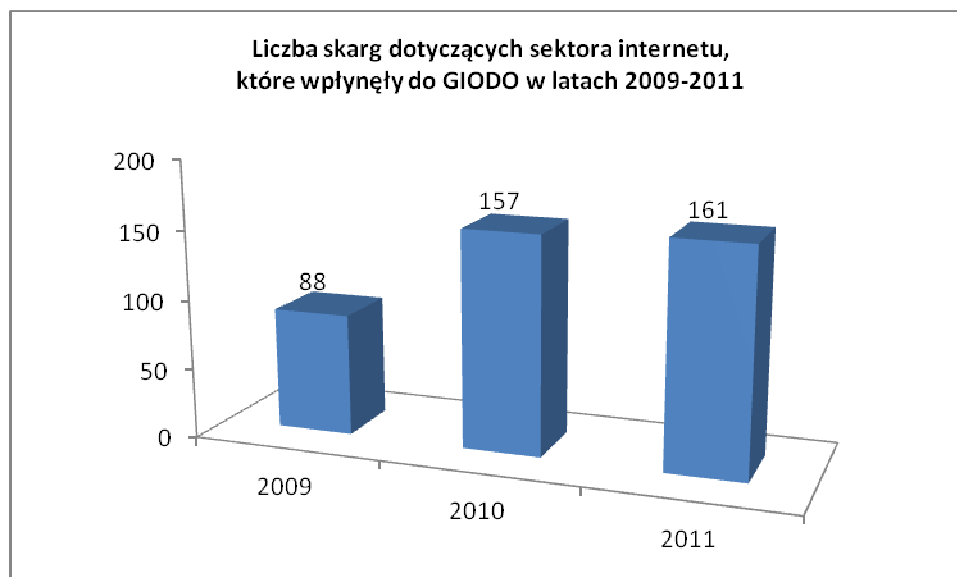
W omawianym roku sprawozdawczym GODO wystąpił także do Związku Banków Polskich o podjęcie działań zwracających uwagę bankom na konieczność dostosowania procesu przetwarzania danych osobowych do wymogów ustawy o ochronie danych osobowych poprzez informowanie Biura Informacji Kredytowej S.A. o dokonanych uaktualnieniach lub sprostowaniach przekazanych jemu danych osobowych bez zbędnej zwłoki⁸². Zdarzało się bowiem, że na skutek pomyłki pracownika lub błędu w systemie wymiany informacji, czas powiadamiania Biura Informacji Kredytowej S.A. przez banki o zaistniałych zmianach był nie tylko dłuższy niż niezbędny z obiektywnych przyczyn, ale znacznie przekraczał ten okres.

4) Internet

W 2011 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **161** skarg dotyczących **Internetu**, to jest o 4 więcej w stosunku do roku 2010, w którym skarg tych było 157.

⁸¹ zob. Andrzej Drozd, Komentarz do ustawy o ochronie danych osobowych, LexPolonica.

⁸² Pismo GODO z dnia 22 czerwca 2011 r. znak: DOLiS-440-578/11/29917.



Wykres 19: *Zestawienie porównawcze liczby skarg dotyczących sektora Internetu, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

Na wstępie należy przytoczyć, przełomowe z punktu widzenia przetwarzania danych osobowych w omawianym sektorze, stwierdzenie Naczelnego Sądu Administracyjnego zawarte w uzasadnieniu do wyroku z dnia 19 maja 2011 r.⁸³, że cyt.: „(...) Internet często pozornie, a czasami faktycznie zapewnia anonimowość jego użytkownikom. Stanowi medialne forum, na którym prezentowane są treści naruszające ludzką godność, cześć i dobre imię. Dlatego też wszędzie tam gdzie numer IP pozwala pośrednio na identyfikację konkretnej osoby fizycznej powinien on być uznany za dane osobowe w rozumieniu art. 6 ust. 1 i 2 ustawy o ochronie danych osobowych. Odmienna interpretacja byłaby sprzeczna z normami konstytucyjnymi zawartymi w art. 30 i 47 Konstytucji RP (...)”. Skład sędziowski w ww. wyroku jako pierwszy jednoznacznie stwierdził, że adres IP (Internet Protocol Address) jest daną osobową.

W omawianym okresie 2011 r. GIODO wydał decyzję nakazującą spółce udostępnienie skarżącemu numeru IP komputera użytkownika forum internetowego⁸⁴. Generalny Inspektor Ochrony Danych Osobowych w rozstrzygnięciu tym wskazał, iż skoro w ocenie wnioskodawcy doszło do naruszenia jego dóbr osobistych, to uzasadnionym było dochodzenie przez niego ochrony tych dóbr poprzez wystąpienie do sądu z powództwem wobec autora wpisu na forum internetowym prowadzonym przez spółkę. Niewątpliwie był to prawnie usprawiedliwiony cel wnioskodawcy, o którym mowa w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych. Ponadto w ocenie organu, przyjęcie, że przetwarzanie (udostępnienie) - w celu zainicjowania postępowania sądowego - danych osoby, wobec której zachodziło domniemanie, że to ona dokonała wpisu (mającego godzić w dobra osobiste wnioskodawcy) miałoby naruszać jej prawa i wolności, prowadziłoby do nieuzasadnionej

⁸³ Wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011 r. sygn. akt I OSK 1079/10.

⁸⁴ DOLiS/DEC-28/11/2185,2193 dot. DOLiS-440-352/10.

ochrony takiej osoby przed ewentualną odpowiedzialnością za swoje działania, zwłaszcza, że mogła ona w trakcie postępowania sądowego w pełni korzystać ze swoich praw zagwarantowanych przepisami Kodeksu postępowania cywilnego. Działanie spółki polegające na nieudostępnieniu wnioskodawcy danych osobowych, mogło natomiast doprowadzić do ograniczenia jego prawa do wystąpienia do sądu z powództwem w sprawie naruszenia dóbr osobistych oraz skutecznie chronić sprawcę przed odpowiedzialnością cywilnoprawną za jego działania.

W innej z kolei sprawie GODO wydał decyzję nakazującą spółce udostępnienie skarżącemu danych osobowych w zakresie imienia, nazwiska oraz adresu zamieszkania użytkowników portalu aukcyjnego⁸⁵. W ocenie Generalnego Inspektora Ochrony Danych Osobowych wniosek pełnomocnika skarżącego skierowany do spółki odpowiadał wymogom określonym w powołanym wyżej art. 29 ust. 2 i 3 ustawy o ochronie danych osobowych⁸⁶. Podano w nim informacje umożliwiające wyszukanie interesujących skarżącego danych (poprzez wskazanie loginu zarejestrowanych użytkowników serwisu), określono zakres wnioskowanych danych (tj. imię, nazwisko i adres zamieszkania jako elementy niezbędne pozwu w celu określenia strony postępowania) oraz ich przeznaczenie (w celu skierowania przeciwko ww. osobom powództwa w związku z dokonaniem przez nich czynu nieuczciwej konkurencji). Ponadto skarżący wiarygodnie uzasadnił potrzebę uzyskania tych danych wskazując, że zamierza wykorzystać ww. informacje dla ustalenia danych osób, które – w jego ocenie – dopuściły się czynu nieuczciwej konkurencji, podając się za producenta mebli, których wyłącznym twórcą i producentem był skarżący, oferując możliwość zakupu narożnika, który był identyczny z oferowanym przez skarżącego oraz wykorzystując zdjęcia z katalogu skarżącego znajdującego się na stronie internetowej prowadzonego przez niego przedsiębiorstwa i użycie ich w swoich ogłoszeniach, zamieniając nazwę oferowanego produktu. Zgodnie bowiem z art. 13 ust. 1 ustawy o zwalczaniu nieuczciwej konkurencji, czynem nieuczciwej konkurencji jest naśladowanie gotowego produktu polegające na tym, że za pomocą technicznych środków reprodukcji kopiowana jest zewnętrzna postać produktu, jeżeli może wprowadzić klientów w błąd co do tożsamości producenta lub produktu. Dochodzenie roszczeń w sprawach o zwalczanie nieuczciwej konkurencji następuje na podstawie art. 18-22 ustawy o zwalczaniu nieuczciwej konkurencji oraz przepisów Kodeksu postępowania cywilnego. Zgodnie natomiast z art. 126 § 1 pkt 1 Kodeksu postępowania cywilnego, każde pismo procesowe powinno zawierać oznaczenie sądu, do którego jest skierowane, imię i nazwisko lub nazwę stron, ich przedstawicieli ustawowych i pełnomocników. Gdy pismo procesowe jest pierwszym pismem w sprawie, powinno ponadto zawierać oznaczenie miejsca zamieszkania lub siedziby stron, ich

⁸⁵ DOLiS/DEC-259/11/14558,14560 dot. DOLiS-440-697/10.

⁸⁶ Przepis ten obowiązywał do 7 marca 2011 r., tj. do dnia wprowadzenia 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), uchylającej art. 29.

przedstawicieli ustawowych i pełnomocników oraz przedmiotu sporu, pisma zaś dalsze - sygnaturę akt (§ 2 ww. przepisu).

W związku z uzyskaniem informacji, z której wynika, iż przedsiębiorca udostępnił osobom trzecim, za pośrednictwem przesłanej do zindywidualizowanej grupy adresatów wiadomości elektronicznej, dane osobowe skarżącego osobom nieupoważnionym, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do niego o podjęcie stosownych działań mających na celu wyeliminowanie podobnych nieprawidłowości w przyszłości⁸⁷. W wystąpieniu tym organ wskazał, iż niewątpliwie wśród informacji zawartych w wiadomości przesłanej skarżącemu drogą elektroniczną przez przedsiębiorcę były dane osobowe. Wskazany fakt upoważnia również do stwierdzenia, iż przedsiębiorca, jako administrator danych, nie dopełnił spoczywającego na nim – wynikającego z treści art. 36 ust. 1 ustawy – obowiązku zabezpieczenia danych.

Generalny Inspektor wydał również decyzję nakazującą spółce udostępnienie na rzecz skarżącej informacji o osobie, która korzystała z urządzenia określonym o adresie IP w określonym dniu i godzinie, tj. w czasie, gdy w serwisie internetowym zamieszczono anonimowy wpis na temat skarżącej – w zakresie obejmującym imię, nazwisko i adres tej osoby⁸⁸. W ocenie Generalnego Inspektora Ochrony Danych Osobowych w skierowanym do spółki wniosku skarżąca w sposób wiarygodny uzasadniła potrzebę pozyskania żądanych od tego podmiotu danych osobowych. Omawiany wniosek skarżącej odpowiadał ponadto wymogom formalnym wynikającym z brzmienia art. 29 ust. 3 ustawy o ochronie danych osobowych - miał bowiem formę pisemną, został umotywowany (zamiarem wykorzystania żądanych danych dla celu zainicjowania przeciwko autorowi kwestionowanego wpisu postępowania sądowego o ochronę dóbr osobistych skarżącej), zawierał informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych (wskazano w nim precyzyjnie datę i godzinę dokonania kwestionowanego wpisu na portalu oraz adres IP urządzenia, z którego dokonano tego wpisu), wskazywał ich zakres (imię, nazwisko i adres) i przeznaczenie. Jednocześnie, mając na uwadze prawne gwarancje ochrony przed roszczeniami zgłaszanymi w postępowaniu sądowym (w tym także w sprawach z zakresu ochrony dóbr osobistych), brak było podstaw by uznać, że udostępnienie skarżącej żądanych informacji wiązałoby się z naruszeniem praw czy wolności osoby, której one dotyczą. Przyjęcie przeciwnego stanowiska - skutkujące pozbawieniem osoby, w ocenie której bezprawnie naruszono jej prawnie chronione dobra osobiste, możliwości dochodzenia roszczeń stąd wynikających w stosunku do sprawcy tego naruszenia – oznaczałoby w istocie bezzasadną ochronę tego ostatniego przed odpowiedzialnością związaną z zarzucanym mu naruszeniem prawa. Z tych samych powodów nie można było uznać, że udostępnienie skarżącej żądanych danych osobowych pracownika spółki stanowiłoby istotne naruszenie jego dóbr osobistych,

⁸⁷ Pismo GODO z dnia 23 lutego 2011 r. znak: DOLiS-440-49/11/7791.

⁸⁸ DOLiS/DEC-392/11/24002,24005,24007,24009,24013,24016, 24018 dot. DOLiS-440-727/10.

lub dóbr osobistych innych osób (art. 30 pkt 4 ustawy o ochronie danych osobowych). Oczywistym było zarazem, że zadośćuczynieniu wnioskowi skarżącej w omawianym jego zakresie nie stoi na przeszkodzie żadna z pozostałych okoliczności wymienionych w cytowanym już wcześniej art. 30 ustawy o ochronie danych osobowych (pkt 1 – 3).

W omawianym roku sprawozdawczym GIODO zwrócił się do instytutu oferującego uczniom pomoc w nauce o dostosowanie procesu przetwarzania danych osobowych za pomocą zamieszczonego na stronie internetowej formularza zgłoszeniowego do zasad określonych w ustawie o ochronie danych osobowych⁸⁹. Z udzielonych przez instytut wyjaśnień wynikało, że w jednym oświadczeniu sformułowana została klauzula zgody osoby zainteresowanej lekcją pokazową na przetwarzanie jej danych osobowych przez instytut oraz obowiązek informacyjny wynikający z art. 24 ust. 1 ustawy o ochronie danych osobowych. W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wskazał, że na gruncie przepisów ustawy czym innym jest klauzula zgody na przetwarzanie danych osobowych, a czym innym obowiązek informacyjny. Ww. klauzula zgody nie mogła być z tym obowiązkiem łączona (utożsamiana). O ile zatem przetwarzanie danych następowało na podstawie pisemnie wyrażonej zgody, to treść klauzuli zgody powinna być wyodrębniona z treści innych oświadczeń i informacji zawartych w ww. formularzu, tak aby osoba zainteresowana miała możliwość swobodnego podjęcia decyzji co do uczestnictwa w lekcji pokazowej. Dopełnienie ww. obowiązku informacyjnego było istotne z punktu widzenia realizacji praw osób, których dane dotyczą, bowiem pozwalało na świadome podjęcie decyzji o wyrażeniu zgody na przetwarzanie danych, a także na wykonywanie uprawnień kontrolnych określonych w art. 32 ustawy o ochronie danych osobowych. Realizacja ww. obowiązku powinna nastąpić przed rozpoczęciem zbierania danych osobowych, gdyż warunkuje legalność ich przetwarzania. Zatem w sytuacji gdy dane osobowe przetwarzane były na podstawie zgody udzielonej przez osobę, której dane dotyczą, administrator danych musiał spełnić obowiązek powiadomienia jeszcze przed jej wyrażeniem⁹⁰ „i to najlepiej przed przystąpieniem do zbierania poszczególnych informacji”⁹¹. Powzięcie przez osobę, której dane dotyczą, wiadomości o okolicznościach wskazanych w art. 24 ustawy o ochronie danych osobowych, było warunkiem skuteczności zgody na przetwarzanie danych osobowych. Tylko wtedy można bowiem mówić, że zgoda nie miała charakteru abstrakcyjnego, tj. odnosiła się do skonkretyzowanego stanu faktycznego, obejmowała określone dane osobowe oraz sprecyzowany sposób i cel przetwarzania.

Natomiast jedno z postępowań wszczętych z urzędu przez Generalnego Inspektora dotyczyło praktyki polegającej na żądaniu przez administratora danych osobowych od użytkowników jednego z tzw. „randkowych” serwisów internetowych, którzy zdecydowali się na usunięcie swojego konta,

⁸⁹ Pismo GIODO z dnia 1 kwietnia 2011 r. znak: DOLiS-440-900/09/14903/11.

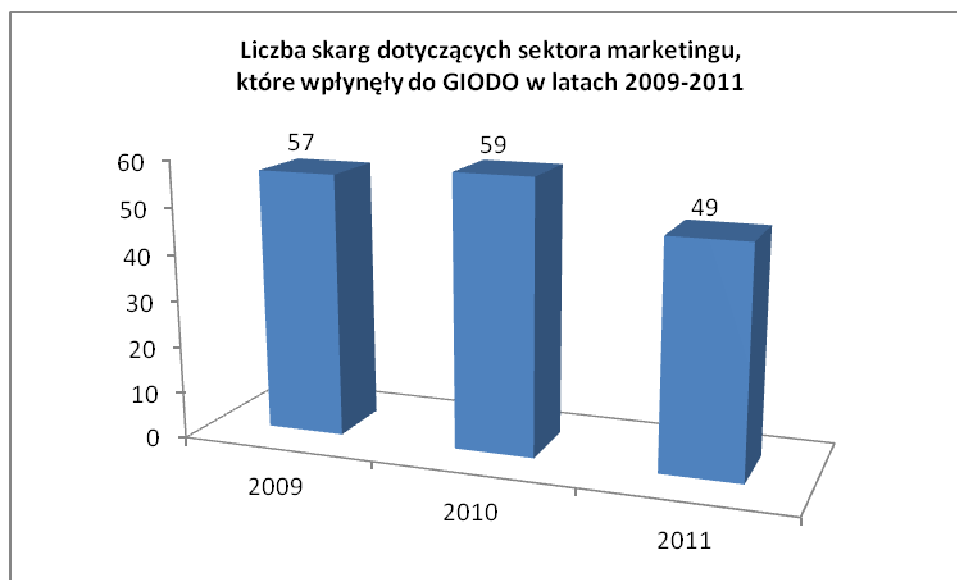
⁹⁰ por. A. Drozd, op. cit.

⁹¹ Zob. A. Medniś, „Ustawa o ochronie danych osobowych. Komentarz”, Warszawa 1999, Wydawnictwo Prawnicze, wydanie I.

dostarczenia skanu dowodu tożsamości.⁹² Z uwagi na fakt, że w trakcie trwania postępowania wyjaśniającego w ww. zakresie administrator zaniechał tej praktyki, Generalny Inspektor wydał w tej sprawie decyzję umarzającą postępowanie.⁹³

5) Marketing

W analizowanym okresie do GODO wpłynęło **49** skarg dotyczących sektora **marketingu**. Dla porównania w 2010 r. wpłynęło 59 skarg dotyczących tego obszaru.



Wykres 20: *Zestawienie porównawcze liczby skarg dotyczących sektora marketingu, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

Najczęściej Generalny Inspektor Ochrony Danych Osobowych wydawał decyzje nakazujące spółkom przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych osobowych skarżących poprzez zaprzestanie przetwarzania ich danych osobowych w celach marketingowych⁹⁴. Z materiałów dowodowych zgromadzonych w tych sprawach wynikało, że skarżący składali sprzeciw wobec przetwarzania ich danych w celach marketingowych, czemu administratorzy danych nie zaprzeczali i co odnotowali w swoich systemach informatycznych. Wątpliwości budził fakt, że pomimo złożonego sprzeciwu do skarżących skierowane zostały drogą telefoniczną oraz poprzez wiadomości tekstowe sms informacje marketingowe w zakresie możliwości przedłużenia przez nich umowy ze spółką, skorzystania z nowej oferty spółki czy informacje o możliwości wymiany przez nich telefonu na nowy model.

⁹² DOLiS-440-706/11

⁹³ DOLiS/DEC-1070/11 dot. DOLiS-440-706/11.

⁹⁴ DOLiS/DEC-567/11/32971,33004 dot. DOLiS-440-547/10, DOLiS/DEC-418/11/25089,25093 dot. DOLiS-440-1095/10.

Natomiast w innej sprawie⁹⁵, która wpłynęła w 2011 r. do Biura GODO skarżący otrzymał ofertę marketingową podmiotu trzeciego, dołączoną do faktury VAT przesłanej przez dostawcę usług internetowych, pomimo sprzeciwu wobec przetwarzania jego danych osobowych w celach marketingowych. I w tej sprawie Generalny Inspektor wydał decyzję⁹⁶ nakazującą dostawcy usług internetowych przywrócić stanu zgodnego z prawem w procesie przetwarzania danych osobowych skarżącego poprzez zaprzestanie przetwarzania jego danych osobowych w celach marketingowych.

6) Mieszkalnictwo

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**. Należy wskazać, że w 2010 r. wpłynęły do Biura GODO 52 skargi na podmioty działające w tym obszarze, natomiast w 2011 r. liczba ta wzrosła do **81**.



Wykres 21: *Zestawienie porównawcze liczby skarg dotyczących sektora mieszkalnictwa, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

Pomimo sygnalizowania tym podmiotom przez Generalnego Inspektora w poprzednich latach konieczności respektowania w ich działalności przepisów ustawy o ochronie danych osobowych, nadal udostępniają one dane osobowe mieszkańców osobom nieupoważnionym⁹⁷, w tym także dane wrażliwe dotyczące np. wyroków czy decyzji administracyjnych zapadłych w toczących się przeciwko

⁹⁵ DOLiS-440-164/11

⁹⁶ DOLiS/DEC-646/11/36797,36798 dot. DOLiS-440-164/11.

⁹⁷ Pismo GODO z dnia 18 kwietnia 2011 r., znak: DOLiS-440-907/10/17953/11, pismo GODO z dnia 16 września 2011 r. znak: DOLiS-440-1039/09/44242/11.

mieszkańcom postępowaniach sądowych czy administracyjnych⁹⁸, jak również udostępniają dane osobowe swych członków w celach sprawozdawczych w zbyt szerokim zakresie⁹⁹.

W przedmiotowym okresie sprawozdawczym 2011 r. GIODO wydał decyzję nakazującą spółdzielni mieszkaniowej udostępnienie skarżącemu danych osobowych w zakresie informacji, czy określone osoby są lub były właścicielami lokalu mieszkalnego, czy, a jeżeli tak, to w jakiej formie i na jakiej podstawie wyzbyły się one powyższego prawa¹⁰⁰. Analiza materiału dowodowego zgromadzonego w niniejszej sprawie prowadziła do wniosku, iż żądanie skarżącego o udostępnienie danych osobowych było w pełni uzasadnione i wypełniało dyspozycję art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych. Wniosek skarżącego o udostępnienie danych spełniał przesłanki udostępnienia danych wskazane w art. 29 ustawy o ochronie danych osobowych, ponieważ został złożony do administratora danych przez osobę uprawnioną, był umotywowany, wskazywał zakres i przeznaczenie oraz w sposób wiarygodny uzasadniał potrzebę ich udostępnienia. Ponadto w ocenie Generalnego Inspektora Ochrony Danych Osobowych wykorzystanie danych w celu realizacji konstytucyjnie przysługującego uprawnienia do dochodzenia swoich praw w drodze procesu sądowego nie mogło być uznane za naruszenie praw i wolności osób, których dane dotyczą. Prawo do prywatności nie ma bowiem charakteru absolutnego, a jego ochrona nie może odbywać się kosztem braku poszanowania praw innych osób. Z kolei odmowa udostępnienia danych, o które wnioskował skarżący mogła służyć ochronie dłużnika, który dokonał czynności prawnej z pokrzywdzeniem wierzyciela. Takie stanowisko znajduje potwierdzenie w orzecznictwie administracyjnym. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 30 listopada 2004 r.¹⁰¹ stwierdził, iż „(...) zasadą powszechnie akceptowaną, wynikającą nie tylko z przepisów prawa cywilnego, lecz także z norm moralnych, zasad współżycia społecznego oraz dobrych obyczajów jest regulowanie zaciągniętych zobowiązań (zapłata długów). (...) Dłużnik, który nie wywiązuje się ze swoich zobowiązań, musi liczyć się z konsekwencjami, wynikającymi z przepisów regulujących obrót gospodarczy. Postawa dłużnika nie może bowiem prowadzić do uprzywilejowania jego sytuacji prawnej. Gdyby generalnie uznać każdy wypadek przetwarzania danych osobowych dłużnika za godzący w jego prawa i wolności, doszłoby z jednej strony do niczym nieuzasadnionej ochrony osób niewywiązujących się ze swoich zobowiązań, z drugiej natomiast do naruszenia zasady swobody działalności gospodarczej, co z pewnością nie było zamiarem ustawodawcy przy uchwalaniu ustawy o ochronie danych osobowych”.

⁹⁸ Pismo GIODO z dnia 13 października 2011 r. znak: DOLiS-440-423/11/48906, pismo GIODO z dnia 7 grudnia 2011 r. znak: DOLiS-440-193/11/59403.

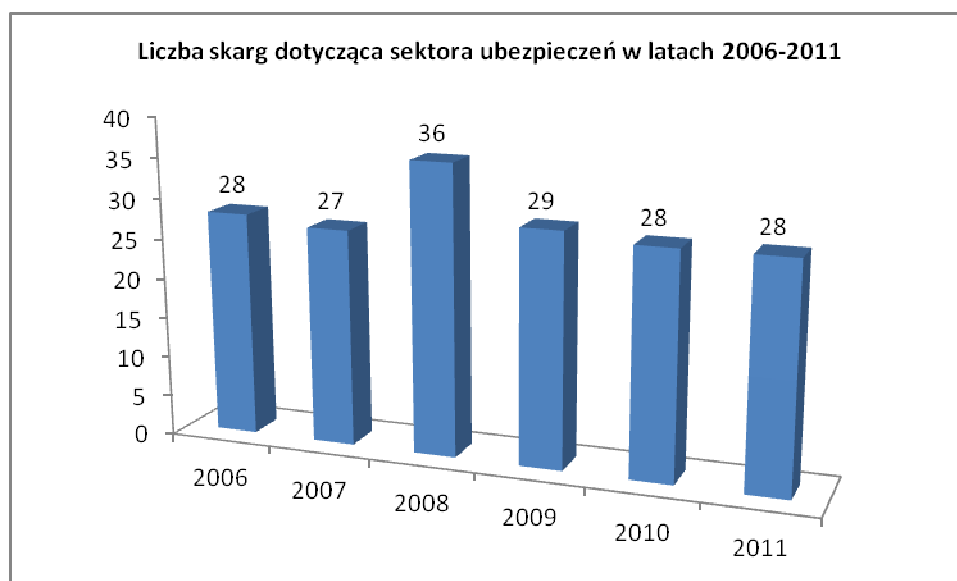
⁹⁹ Pismo GIODO z dnia 3 sierpnia 2011 r. znak: DOLiS-440-314/11/37249.

¹⁰⁰ DOLiS/DEC-443/11/25778,25782 dot. DOLiS-440-744/10.

¹⁰¹ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 30 listopada 2004 r. sygn. akt: II SA/Wa 1057/04.

7) Ubezpieczenia społeczne, majątkowe i osobowe

W 2011 r. do GIODO wpłynęło **28** skarg dotyczących sektora **ubezpieczeń społecznych, majątkowych i osobowych**. W porównaniu z poprzednim rokiem sprawozdawczym liczba ta utrzymuje się na niezmienionym poziomie.



Wykres 22: *Zestawienie porównawcze liczby skarg na podmioty działające w sektorze ubezpieczeń społecznych, majątkowych i osobowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

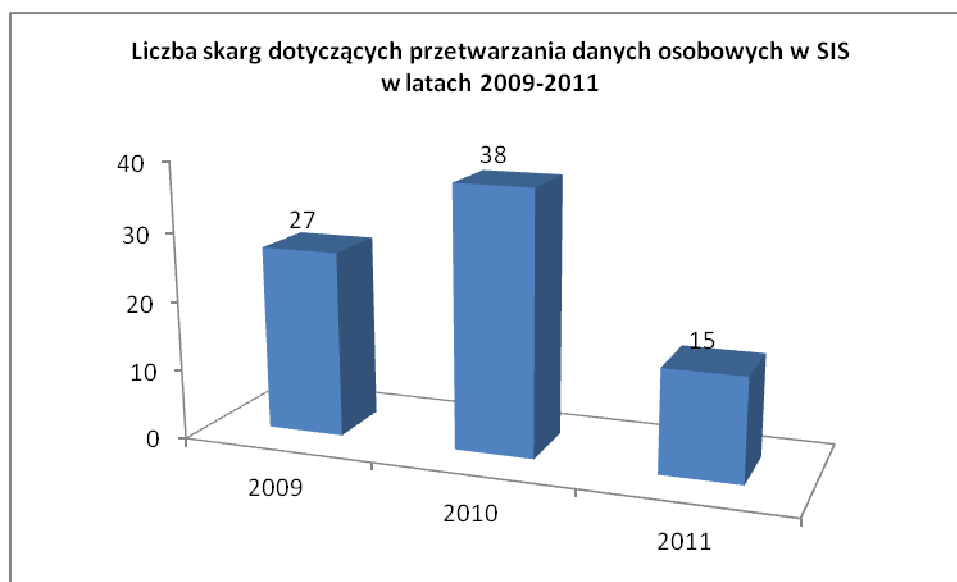
W rozpatrywanym okresie 2011 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję nakazującą Zakładowi Ubezpieczeń Społecznych udostępnienie miejskiemu ośrodkowi pomocy społecznej danych określonej osoby w zakresie informacji o wysokości przyznanego jej w miesiącu kwietniu 2010 r. zasiłku chorobowego¹⁰². W uzasadnieniu tego rozstrzygnięcia Generalny Inspektor Ochrony Danych Osobowych wskazał art. 50 ust. 3 ustawy o systemie ubezpieczeń społecznych jako podstawę wystąpienia miejskiego ośrodka pomocy społecznej o udostępnienie przez ZUS danych określonej osoby w celu ustalenia możliwości ponoszenia przez ww. odpłatności za pobyt krewnej, która korzysta z pomocy społecznej w formie pobytu w domu pomocy społecznej. Przedmiotowy przepis w ocenie organu wskazywał na uprawnienia ośrodka pomocy społecznej do zapoznania się z danymi osobowymi przetwarzanymi przez Zakład Ubezpieczeń Społecznych, a tym samym udostępnienie żądanych przez miejski ośrodek pomocy społecznej danych znajdowało oparcie w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych – zgodnie z którym przetwarzanie danych jest dopuszczalne, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

¹⁰² DOLiS/DEC-231/11/12733,12739 dot. DOLiS-440-941/10.

8) System Informacyjny Schengen

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.¹⁰³ 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.

W 2011 r. do Biura GODO wpłynęło **15** skarg dotyczących przetwarzania danych osobowych w **Systemie Informacyjnym Schengen**, tj. o ponad połowę mniej w stosunku do roku 2010, gdzie skarg tych było 38.

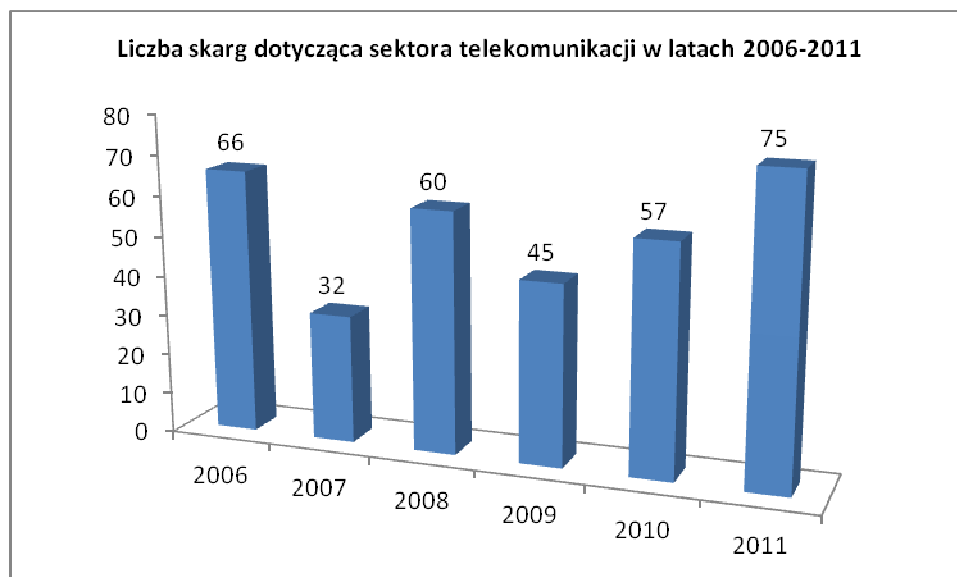


Wykres 23: *Zestawienie porównawcze liczby skarg dotyczących przetwarzania danych osobowych w Systemie Informacyjnym Schengen, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

9) Telekomunikacja

W omawianym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **75** skarg dotyczących działalności **telekomunikacyjnej**. Stanowi to wzrost w porównaniu z rokiem 2010 r., w którym wpłynęło 57 skarg na podmioty tego sektora.

¹⁰³ 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.



Wykres 24: *Zestawienie porównawcze liczby skarg na podmioty działające w sektorze telekomunikacji, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

GIODO zwrócił się do operatora telekomunikacyjnego o uwzględnienie w jego działalności przepisów ustawy o ochronie danych osobowych¹⁰⁴. W wystąpieniu tym organ wskazał, iż celem przetwarzania przez operatora telekomunikacyjnego niepodlegającego udostępnieniu w spisie abonentów („zastrzeżonego”) numeru telefonu skarżącego było wykonanie umowy o świadczenie usługi telekomunikacyjnej, zaś powodem „zastrzeżenia” przez skarżącego ww. numeru było nieupublicznianie go przez operatora telekomunikacyjnego w ogólnie dostępnym wykazie abonentów. Istotą usługi zastrzeżenia numeru telefonu przed jego nieupublicznieniem w spisie (o którym mowa w art. 169 Prawa telekomunikacyjnego) było chronienie m.in. tej informacji przed dostępem do niej przez osoby trzecie. Zatem skoro skarżący nie wyraził operatorowi telekomunikacyjnemu zgody na upublicznienie dotyczącego go numeru telefonu w spisie abonentów, należało uznać, iż nie zgodził się on również na jego przekazywanie podmiotom trzecim (choćby świadczącym usługi na rzecz operatora telekomunikacyjnego) - tym bardziej, że upoważnił on operatora telekomunikacyjnego do przetwarzania dotyczącego go numeru telefonu do kontaktu. W sytuacji, gdy operator telekomunikacyjny dysponował numerem do kontaktu ze skarżącym, to ten właśnie numer powinien przekazać podmiotowi świadczącemu usługi na jego rzecz - firmie kurierskiej.

W 2011 r. do GIODO wpłynęła skarga Komendanta Straży Miejskiej na jednego z operatorów telekomunikacyjnych. Komendant wskazał, że Straż Miejska prowadzi postępowanie wyjaśniające w sprawie o wykroczenie przeciwko domniemanemu sprawcy, który zamieścił ogłoszenie w miejscu

¹⁰⁴ Pismo GIODO z dnia 20 maja 2011 r. znak: DOLiS-440-851/10/23576/11.

publicznym do tego nieprzeznaczonym. Komendant wyjaśnił, że dane osobowe są mu niezbędne dla zrealizowania obowiązków nałożonych na Straż Miejską przez przepisy ustawy o strażach gminnych oraz Kodeksu postępowania w sprawach o wykroczenia. Operator telekomunikacyjny odmówił udostępnienia danych osobowych Komendantowi powołując się na obowiązek zachowania tajemnicy telekomunikacyjnej wynikającej z art. 159 Prawa telekomunikacyjnego (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.). Generalny Inspektor w swojej decyzji¹⁰⁵ nakazał operatorowi telekomunikacyjnemu udostępnienie Komendantowi Straży Miejskiej danych osobowych abonenta telefonu komórkowego o wskazanym numerze telefonu w zakresie jego imienia, nazwiska oraz adresu zamieszkania. GIODO wskazał, że realizacja przez Straż Miejską zadań nałożonych na nią ustawowo (ustawa o strażach gminnych¹⁰⁶, Kodeks postępowania w sprawach o wykroczenia¹⁰⁷) wymaga wykorzystywania informacji o osobach, których działania te dotyczą. Przepisy ustawy o strażach gminnych wprost stanowią o prawie Straży Miejskiej do przetwarzania danych w związku z realizacją określonych prawem zadań, bez konieczności uzyskania na to zgody osoby, której dane dotyczą. Jednocześnie należy wskazać, że Straż Miejska jest jednym z oskarżycieli publicznych w myśl art. 17 Kodeksu postępowania w sprawach o wykroczenia, któremu przysługuje prawo do przeprowadzenia czynności wyjaśniających w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie oraz zebrania danych niezbędnych do sporządzenia wniosku o ukaranie (art. 54 – 56 ustawy Kodeks postępowania w sprawach o wykroczenia). Oznacza to, iż Straż Miejska, na mocy stosownych przepisów rangi ustawowej, ma prawo zwrócić się do operatora telekomunikacyjnego o udostępnienie niezbędnych jej danych osobowych, zaś operator ten winien – mając na względzie fakt realizacji obowiązku czuwania przez Straż Miejską nad przestrzeganiem prawa przez obywateli – udostępnić informacje w zakresie wnioskowanym przez Straż Miejską. W tym zakresie stanowisko Generalnego Inspektora oparte zostało na licznych podobnych rozstrzygnięciach sądów.¹⁰⁸

10) Zatrudnienie

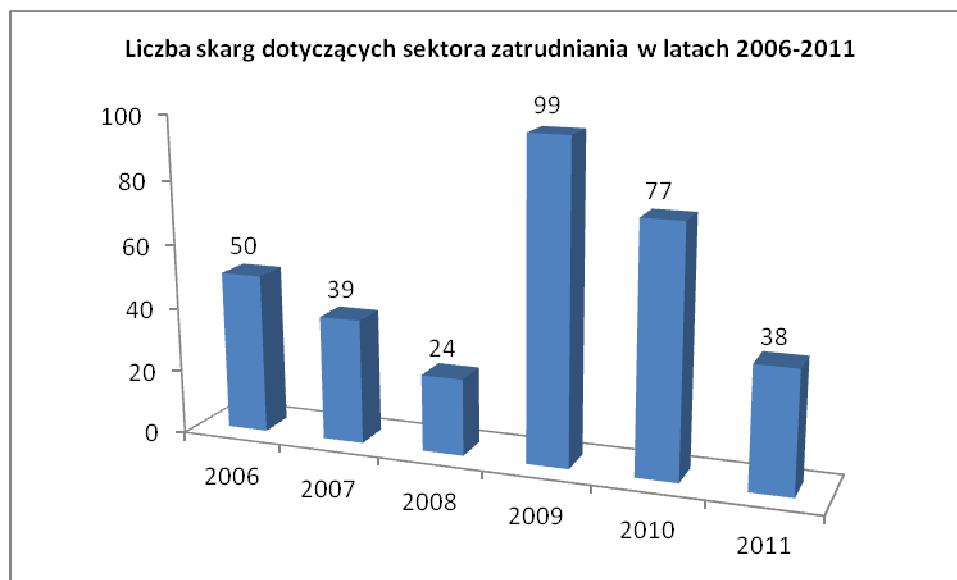
W 2011 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **38** skarg dotyczących podmiotów sektora **zatrudnienia**. W porównaniu z poprzednim rokiem sprawozdawczym, w którym wpłynęło aż 77 skarg, stanowi to znaczny spadek skarg na podmioty działające w tym obszarze.

¹⁰⁵ DOLiS/DEC-1088/11/63446,63448 dot. DOLiS-440-559/11.

¹⁰⁶ Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych, Dz. U. 1997 r. Nr 123, poz. 779 z późn. zm.

¹⁰⁷ Ustawa z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia, Dz. U. 2008 r. Nr 133, poz. 848 z późn. zm.

¹⁰⁸ Zob. wyrok Naczelnego Sądu Administracyjnego z dnia 5 lutego 2008 r. sygn. akt I OSK 37/07, wyrok Naczelnego Sądu Administracyjnego z dnia 3 lipca 2009 r. sygn. akt I OSK 1007/08.



Wykres 25: *Zestawienie porównawcze liczby skarg dotyczących sektora zatrudniania, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

W omawianym okresie GODO wydał decyzje nakazujące pracodawcom usunięcie uchybień przy przetwarzaniu danych osobowych pracowników poprzez pozyskiwanie informacji o osobach korzystających z obrony związku zawodowego jedynie w sytuacji, gdy przepisy prawa pracy przewidują w stosunku do tych osób współdziałanie pracodawcy z zakładową organizacją związkową w indywidualnych sprawach ze stosunku pracy, zgodnie z art. 23² Kodeksu pracy¹⁰⁹. W ocenie Generalnego Inspektora Ochrony Danych Osobowych przepisy art. 30 ust. 2¹ ustawy o związkach zawodowych oraz art. 23² Kodeksu pracy nie mogły stanowić podstawy do pozyskiwania przez pracodawców od związku danych osobowych wszystkich pracowników korzystających z ochrony związku. Artykuł 30 ust. 2¹ ustawy o związkach zawodowych stanowił o indywidualnych sprawach ze stosunku pracy. Odnosił się on zatem do ochrony stosunku pracy indywidualnego pracownika, którą zapewniają w szczególności przepisy art. 38 § 1 Kodeksu pracy (wypowiedzenie umowy o pracę na czas nieokreślony), art. 52 § 3 Kodeksu pracy (rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika) i art. 177 § 1 Kodeksu pracy (rozwiązanie umowy o pracę w okresie ciąży lub urlopu macierzyńskiego bez wypowiedzenia z winy pracownicy). Powyższe oznaczało, że pozyskiwanie informacji o przynależności związkowej pracownika w toku konsultacji ze związkami zawodowymi było uzasadnione w razie zamiaru rozwiązania umowy o pracę z konkretnym pracownikiem. Dlatego brak było podstaw do pozyskiwania przez pracodawców od związku danych osobowych we wskazanym zakresie w odniesieniu do wszystkich pracowników korzystających z ochrony związków w sytuacji, gdy nie są oni objęci zamiarem pracodawców rozwiązania z nimi umów o pracę.

¹⁰⁹ DOLiS/DEC-2/11/205,208 dot. DOLiS-440-500/10; DOLiS/DEC-41/11/2819,2820 dot. DOLiS-440-755/10.

Ponadto pozyskiwanie danych osobowych wszystkich pracowników korzystających z obrony związku, gdy nie byli oni objęci zamiarem pracodawców wymagającym współdziałania z organizacją związkową, naruszało określoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych zasadę adekwatności. Powołany przepis stanowił, iż 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 merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swoimi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych realizacja przez związek wniosku pracodawców skutkowałaby pozyskaniem danych osobowych osób korzystających z obrony związku również na zapas (ewentualna realizacja trybu z Kodeksu pracy mogła, ale nie musiała się rozpocząć), co w świetle przepisów ustawy było niedopuszczalne¹¹⁰.

Generalny Inspektor wydał także decyzję nakazującą spółce wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącej poprzez zaprzestanie przetwarzania jej danych osobowych w zakresie imienia i nazwiska zawartych w adresie poczty elektronicznej, którym posługiwała się będąc pracownikiem spółki.¹¹¹ W przedmiotowej sprawie spółka wskazała, iż zawierający w swej nazwie dane osobowe skarżącej adres poczty e-mail wykorzystywany był jedynie biernie – jako skrzynka odbiorcza, za pomocą której klienci spółki mogli składać zamówienia lub kontaktować się ze spółką. Prawdą było, że spółka miała prawo dbać o swoje interesy i na tej podstawie przetwarzać dane osobowe, jednakże w niniejszej sprawie ciągła aktywność przedmiotowego adresu e-mail naruszała w ocenie organu prawa i wolności skarżącej. Skarżąca nie była już pracownikiem spółki, natomiast podjęła pracę w innej firmie, z którą chciała być utożsamiana. Z uwagi na fakt, że skarżąca nie wykonywała zadań wynikających z łączącego ją ze spółką stosunku pracy, GODO uznał, iż ustał cel przetwarzania jej danych zawartych w adresie e-mail, a ponadto ich przetwarzanie stanowiło przetwarzanie niezgodne z celem, dla którego dane te były zbierane. W ocenie GODO ciągła aktywność przedmiotowego adresu poczty elektronicznej, a zarazem możliwość przesyłania wiadomości na ten adres, pośrednio jednak nadal wpływało na utożsamianie osoby skarżącej ze spółką, co w obecnej sytuacji dawało fałszywy obraz jej aktywności zawodowej. Ponadto osoba, do której, zgodnie z jej identyfikatorem zawartym w adresie, kierowana była korespondencja nie

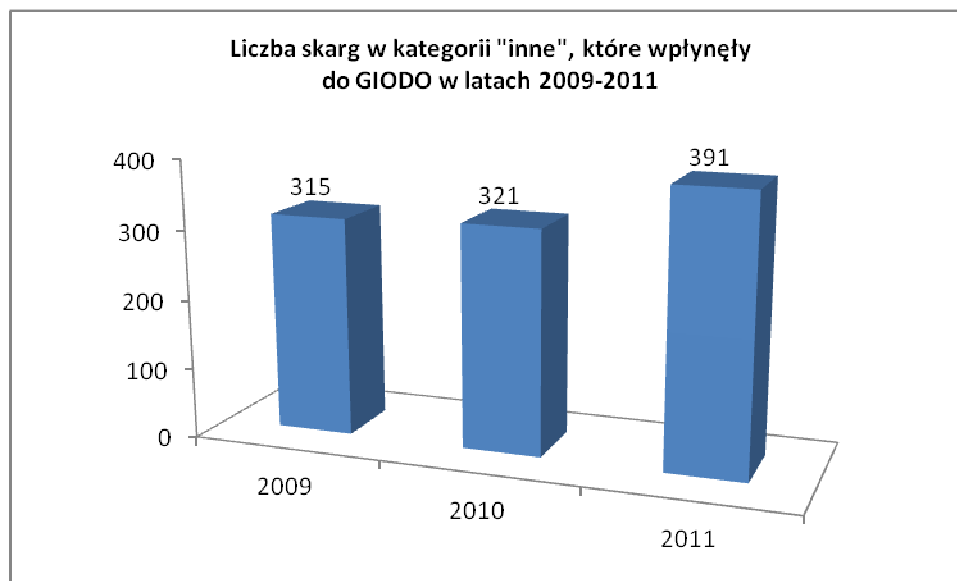
¹¹⁰ Podobne stanowisko zajął Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 26 sierpnia 2010 r. sygn. akt II SA/Wa 923/10.

¹¹¹ DOLiS/DEC-498/11/29141,29142 dot. DOLiS-440-82/11.

miała możliwość zapoznania się nią, co z kolei stanowiło przejaw naruszenia wolności tej osoby do prawa komunikowania się oraz ochrony jej korespondencji.

11) Inne

Wśród skarg, które Generalny Inspektor Ochrony Danych Osobowych badał w 2011 r. wyodrębnić należy te, które z racji swojego przedmiotu nie mogły być zakwalifikowane do wcześniej przedstawionych kategorii spraw. Ich liczba wyniosła **391**, co w porównaniu z rokiem 2010, gdzie spraw tych było 323, wskazuje na systematyczny wzrost.



Wykres 26: *Zestawienie porównawcze liczby skarg z sektora „Inne”, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009–2011.*

Wśród nich odnotować należy wzrost liczby skarg zawierających zarzut przetwarzania danych osobowych przez proboszczów parafii Kościoła Katolickiego¹¹². 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. Z wyjaśnień uzyskanych przez Generalnego Inspektora wynikało, że osoby skarżące są wciąż członkami Kościoła Katolickiego, ponieważ nie przeszły formalnej procedury apostazji. Powyższa procedura postępowania zagwarantowana jest przez konkordat pomiędzy Kościołem Katolickim w Polsce a Państwem. W związku z powyższym organ ochrony danych osobowych umarzał postępowania administracyjne w takich sprawach wskazując na brak swojej kognicji do wydania merytorycznej decyzji

¹¹² np.: DOLiS-440-615/11, DOLiS-440-842/11, DOLiS-440-879/11, DOLiS-440-927/11, DOLiS-440-1005/11, DOLiS-440-1119/11.

administracyjnej w tym względzie, wskazany w art. 43 ust. 2 ustawy o ochronie danych osobowych.¹¹³ Wiele z tych rozstrzygnięć zostało poddanych kontroli sądowej wskutek ich zaskarżenia do WSA¹¹⁴.

Spełnienie obowiązku informacyjnego wobec osoby skarżącej było przedmiotem kolejnej skargi rozpatrywanej przez GODO w 2011 r. W sprawie tej Generalny Inspektor wydał decyzję nakazującą osobie prowadzącej działalność gospodarczą spełnienie wobec skarżącego obowiązku informacyjnego określonego w art. 33 ust. 1 ustawy o ochronie danych osobowych¹¹⁵. W przedmiotowej sprawie skarżący zwrócił się do przedsiębiorcy o udzielenie informacji we wskazanym w art. 33 ust. 1 ustawy o ochronie danych osobowych zakresie, żądając udzielenia mu odpowiedzi na piśmie. Przedsiębiorca do dnia wydania decyzji nie udzielił mu odpowiedzi, natomiast wskazał, iż pismo skierowane przez niego do Generalnego Inspektora Ochrony Danych Osobowych zawiera informacje na temat przetwarzania przez niego danych skarżącego i dlatego traktuje je jako dopełnienie ciążącego na nim obowiązku określonego w art. 33 ust. 1 ustawy. W związku z powyższym wniósł o przesłanie przez organ ds. ochrony danych osobowych odpisu tego pisma skarżącemu w celu uczynienia mu zadość. Odpowiedź taka w ocenie Generalnego Inspektora Ochrony Danych Osobowych pozostawała w sprzeczności z regulacją art. 33 ustawy o ochronie danych osobowych, albowiem nie została skierowana bezpośrednio do osoby, której dane dotyczą. Wypełniając ciążący na nim obowiązek, przedsiębiorca zobowiązany był do udzielenia odpowiedzi bezpośrednio skierowanej do skarżącego i dokładnego ustosunkowania się do treści jego żądań, a zatem wymienienie: jakimi konkretnie danymi skarżącego dysponuje, a także, nawet jeżeli zgodnie z wiedzą przedsiębiorcy skarżący posiadał te informacje, do wskazania źródła pozyskania danych i sposobu ich pozyskania, pouczenie skarżącego co do przysługujących mu w kontekście ustawy o ochronie danych osobowych praw, wskazania dokładnie celu i zakresu przetwarzania jego danych oraz zbioru, w którym były przetwarzane i wymienienie podmiotów i zakresu w jakich jego dane zostały im udostępnione.

W analizowanym 2011 roku GODO wydał decyzję nakazującą związkowi działkowców udostępnienie na rzecz skarżącego danych osobowych użytkowników działek o określonych numerach w zakresie imion, nazwisk i adresów zamieszkania¹¹⁶. W niniejszej sprawie wniosek skarżącego skierowany do związku działkowców w ocenie Generalnego Inspektora Ochrony Danych Osobowych odpowiadał wymogom określonym w art. 29 ust. 2 i 3 ustawy o ochronie danych osobowych. Podano w nim informacje umożliwiające wyszukanie interesujących skarżącego danych (poprzez wskazanie

¹¹³ zob. DOLiS/DEC-21/11/1560,1570 dot. DOLiS-440-845/10, DOLiS/DEC- 33/11/2429,2430 dot. DOLiS-440-588/10, DOLiS/DEC- 44/11/3079,3082 dot. DOLiS-440-771/10, DOLiS/DEC- 45/11/3167,3170 dot. DOLiS-440-810/10, DOLiS/DEC- 91/11/5808,5812 dot. DOLiS-440- 954/10, DOLiS/DEC- 413/11/24660,24662 dot. DOLiS-440- 313/11.

¹¹⁴ zob. wyroki Wojewódzkiego Sądu Administracyjnego w Warszawie o sygn. akt: II SA/Wa 1560/11 (nieprawomocny), II SA/Wa 2558/11, II SA/Wa 1320/11, II SA/Wa 1671/11, II SA/Wa 2026/11.

¹¹⁵ Decyzja GODO z dnia 24 stycznia 2011 r. znak: DOLiS/DEC-42/11/2823,2824.

¹¹⁶ Decyzja GODO z dnia 25 stycznia 2011 r. znak: DOLiS/DEC-46/11/3182,3184.

o użytkowników której działki chodzi), określono zakres wnioskowanych danych (imię, nazwisko, adres) oraz ich przeznaczenie (w celu skierowania przeciwko ww. osobom powództwa cywilnego). W ocenie organu skarżący wiarygodnie uzasadnił potrzebę pozyskania wnioskowanych danych, wskazując, że są mu niezbędne do prawidłowego dopoznania ww. osób do postępowania cywilnego mającego na celu doprowadzenie do wydania mu ww. nieruchomości.

W podobnej sprawie zwróciła się do GIODO skarżąca, która nie uzyskała od spółki żądanych danych osobowych w zakresie adresów zamieszkania redaktora naczelnego oraz autora materiału prasowego, niezbędnych jej do prawidłowego pozwania tych osób w postępowaniu cywilnym. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję nakazującą spółce udostępnienie na rzecz skarżącej danych osobowych we ww. zakresie¹¹⁷. Analiza materiału dowodowego zgromadzonego w niniejszej sprawie prowadziła bowiem do wniosku, iż żądanie skarżącej o udostępnienie wspomnianych danych osobowych wypełnia dyspozycję cytowanego art. 23 ust. 1 pkt 2 i 5 ustawy o ochronie danych osobowych. W ocenie organu skarżąca wiarygodnie uzasadniła potrzebę pozyskania wnioskowanych danych wskazując, że są jej niezbędne do prawidłowego wszczęcia postępowania cywilnego z zakresu ochrony jej dóbr osobistych w związku z opublikowaniem materiału prasowego. Dochodzenie przez skarżącą swych praw przed sądem z tytułu naruszenia jej dóbr osobistych niewątpliwie stanowi realizację prawnie usprawiedliwionego celu skarżącej i jednocześnie pozyskanie ww. danych było niezbędne do realizacji uprawnienia wynikającego z przepisu prawa, tj. z art. 43 w związku z art. 24 § 1 Kodeksu cywilnego.

W kolejnej sprawie GIODO wydał decyzję nakazującą spółce przywrócenie stanu zgodnego z prawem, poprzez spełnienie wobec skarżącej obowiązku informacyjnego określonego w art. 25 ust. 1 ustawy o ochronie danych osobowych¹¹⁸. W uzasadnieniu tego rozstrzygnięcia Generalny Inspektor Ochrony Danych Osobowych wskazał, iż spółka z chwilą pozyskania informacji o skarżącej stała się ich administratorem, a w konsekwencji także adresatem obowiązków nałożonych na administratorów danych przepisami ustawy o ochronie danych osobowych. Jednym z ww. obowiązków było udzielenie informacji określonych w art. 25 ust. 1 ustawy. Zgodnie z tym przepisem, 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. Zatem wobec

¹¹⁷ Decyzja GIODO z dnia 26 stycznia 2011 r. znak: DOLiS/DEC-48/11/3346,3353.

¹¹⁸ Decyzja GIODO z dnia 29 marca 2011 r. znak: DOLiS/DEC-246/11/13928,13930,13931.

faktu, iż spółka nie udzieliła skarżącej informacji określonych w przedmiotowej normie, organ stwierdził, że podmiot ten uchybił spoczywającemu na nim obowiązкови.

W omawianym 2011 r. GODO wystąpił o uwzględnienie w działalności spółki przepisów ustawy o ochronie danych osobowych, w szczególności o nieudostępnianie danych osobowych prasie bez podstawy prawnej¹¹⁹. Z okoliczności sprawy wynikało, że spółka była odrębnym administratorem danych w rozumieniu przepisów ustawy, więc przetwarzanie (w tym udostępnianie) danych osobowych osób, których dotyczyły działania spółki, powinno znajdować uzasadnienie w co najmniej jednej z przesłanek określonych w art. 23 ust. 1 pkt 1-5 ustawy (dane tzw. zwykłe) albo art. 27 ust. 2 pkt 1-10 ustawy (dane tzw. wrażliwe). Zatem udostępniając informacje burmistrzowi miasta czy prasie spółka powinna była dokonać oceny, czy wystąpiła przesłanka dopuszczająca przetwarzanie danych osobowych. W ocenie Generalnego Inspektora w stanie faktycznym niniejszej sprawy nie zaistniała żadna ze wskazanych w powyższych przepisach przesłanek dopuszczających udostępnienie danych osobowych skarżących prasie. W szczególności zaś, dopuszczalność udostępnienia danych osobowych skarżących w żaden sposób nie wynikał ze wskazanego w piśmie spółki art. 4 Prawa prasowego. Ustęp pierwszy tego przepisu ograniczał bowiem możliwość udostępnienia prasie informacji przez przedsiębiorców, jeżeli naruszało to prawo do prywatności osób, których informacje dotyczą. Informacje o stosunkach łączących spółkę ze skarżącymi niewątpliwie należały do sfery ich życia prywatnego. Wobec powyższego, w ocenie Generalnego Inspektora Ochrony Danych Osobowych, brak było podstaw do udostępnienia prasie danych osobowych skarżących.

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

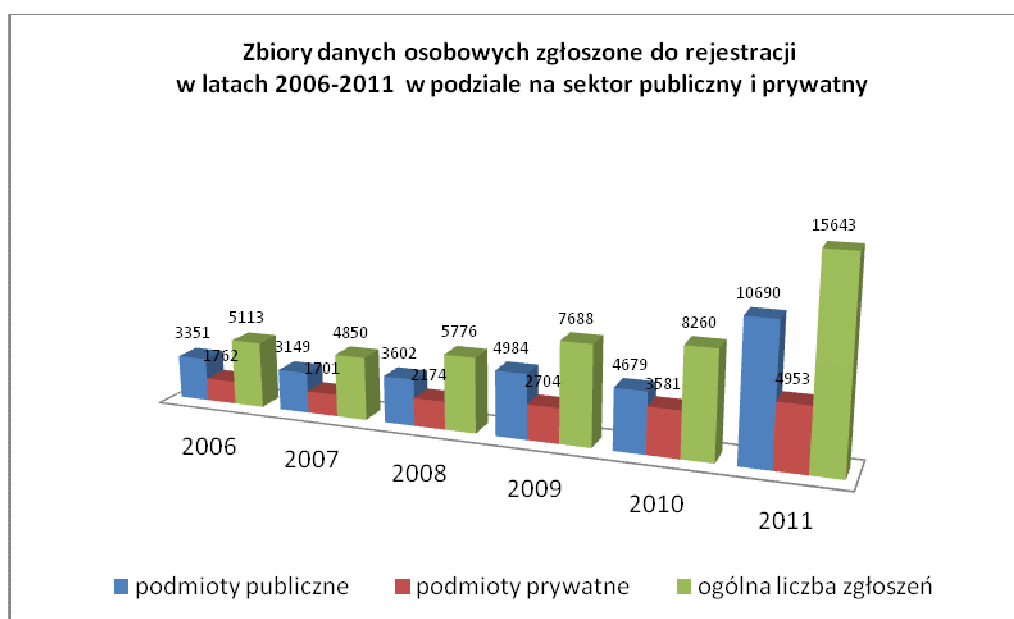
Jednym z podstawowych zadań Generalnego Inspektora Ochrony Danych Osobowych jest prowadzenie ogólnokrajowego jawnego rejestru zbiorów danych osobowych. Z zadaniem tym skorelowany jest obowiązek zgłaszania zbiorów danych osobowych przez administratorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.¹²⁰ 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 ds. ochrony danych osobowych podstawowe

¹¹⁹ Pismo GODO z dnia 11 lutego 2011 r., znak: DOLiS-440-726/10/5986/11.

¹²⁰ 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.

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. Ponadto 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 o ochronie danych osobowych.

W roku 2011 administratorzy danych wypełniając nałożony przepisami ustawy o ochronie danych osobowych obowiązek, zgłosili do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych **15643** zbiory, z czego podmioty z sektora administracji publicznej zgłosiły **10690** zbiorów, co stanowi 68 % ogólnej liczby zgłoszeń dokonanych w tym okresie, zaś podmioty z sektora prywatnego **4953** zbiory, co stanowi 32 % ogólniej liczby zgłoszonych zbiorów.



Wykres 27: **Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2009 -2011.**

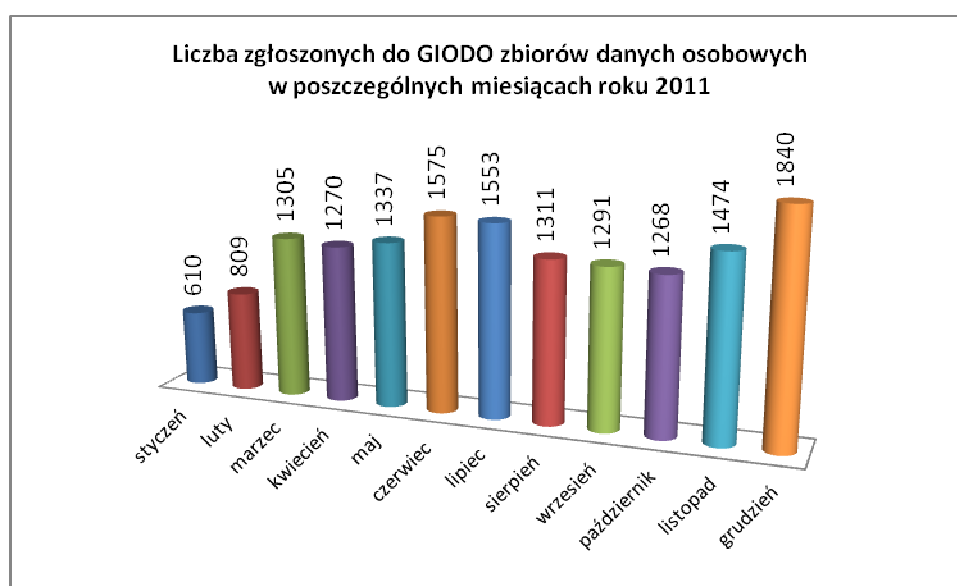
Analizując powyższy wykres należy wskazać, że w 2011 r. nastąpił wzrost o 7383 ogólnej liczby zgłoszeń nadesłanych do rejestracji (o 89 % więcej w stosunku do roku 2010). Ten sam trend można zaobserwować w odniesieniu do zgłoszeń nadesłanych przez podmioty prywatne – w 2011 r. było ich o 1372 więcej w stosunku do roku poprzedniego (tj. o ok. 38 %), zaś podmioty sektora publicznego nadesłały w 2011 r. aż o 6011 zgłoszeń więcej niż w 2010 r. (tj. o 128 %).

Znaczący wzrost liczby zgłoszeń wynikał przede wszystkim z rozwoju świadomości prawnej społeczeństwa w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych –

w tym obowiązku rejestracji zbiorów danych osobowych - i miało związek z prowadzoną na szeroką skalę działalnością edukacyjną Generalnego Inspektora. Na taki stan rzeczy niewątpliwie wpływ miała także możliwość zgłaszania zbiorów drogą elektroniczną.

Wśród podmiotów z sektora publicznego najwięcej zbiorów zgłosiły do rejestracji, podobnie jak w latach ubiegłych, jednostki samorządu terytorialnego (gminy, powiaty), a także straże gminne oraz ośrodki pomocy społecznej. Natomiast wśród podmiotów prywatnych, tak jak w latach ubiegłych, najwięcej zbiorów zgłosiły podmioty, które do przetwarzania danych osobowych wykorzystują sieć Internet (portale społecznościowe, sklepy internetowe).

Poniższy wykres przedstawia zestawienie liczby zbiorów danych osobowych zgłoszonych do rejestracji w poszczególnych miesiącach 2011 roku.



Wykres 28: *Liczbowe zestawienie zbiorów danych osobowych zgłoszonych do rejestracji w 2011 r. z podziałem na poszczególne miesiące.*

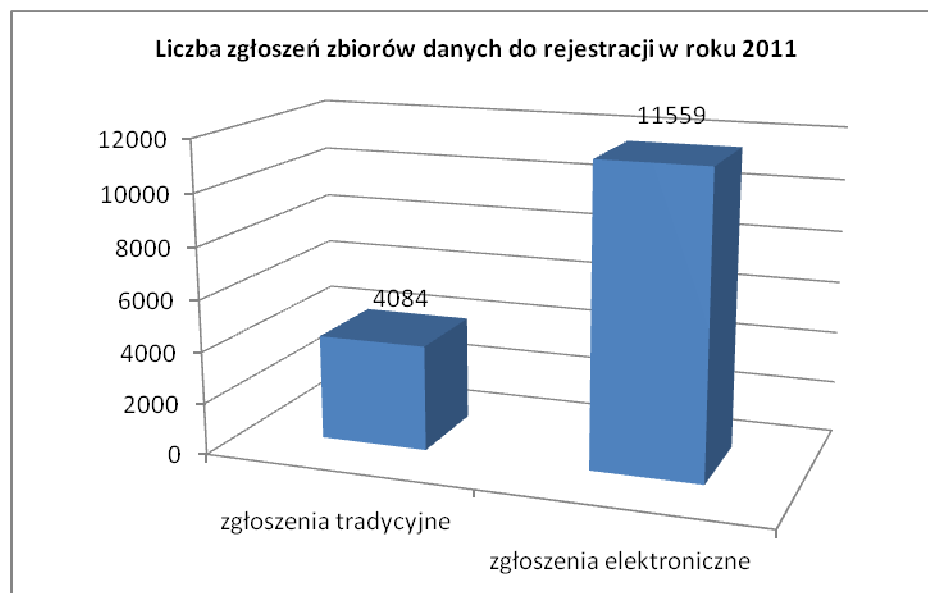
Analizując powyższe zestawienie najwięcej zgłoszeń wpłynęło w grudniu – **1840**, tj. 12 % wszystkich zgłoszeń dokonanych w 2011 r. Należy również zwrócić uwagę, na znaczny wzrost (w stosunku do poprzednich miesięcy) liczby zgłoszeń nadesłanych do rejestracji w marcu 2011 r. i kolejnych miesiącach roku sprawozdawczego. Na taką liczbę zgłoszeń miały niewątpliwie wpływ liczne publikacje w środkach masowego przekazu dotyczące wejścia w życie w dniu 7 marca 2011 r. nowelizacji ustawy o ochronie danych osobowych oraz możliwość zgłaszania zbiorów do rejestracji drogą elektroniczną.

W realizowaniu tego obowiązku niewątpliwie pomocny był 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

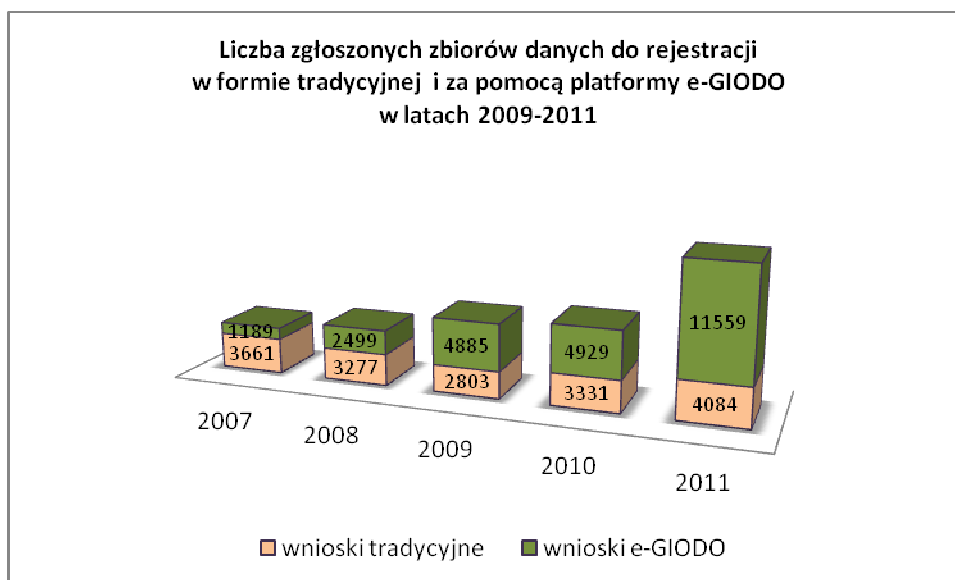
komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych” (w skrócie e-GIODO). Program ten został opracowany na podstawie dotychczasowych doświadczeń Departamentu Rejestracji Zbiorów Danych Osobowych Biura GIODO, z uwzględnieniem najczęstszych błędów popełnianych przez wnioskodawców przy wypełnianiu zgłoszenia. 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. Liczba zgłoszeń wypełnianych za pomocą ww. programu z roku na rok systematycznie rośnie.

W okresie sprawozdawczym do ww. programu komputerowego została wprowadzona kolejna modyfikacja ułatwiająca zgłoszenie zbioru danych do rejestracji. Modyfikacja polegała na umożliwieniu administratorowi danych wyboru nazw ustaw, wraz z aktualnymi publikatorami, których przepisy mogą stanowić podstawę prawną przetwarzania danych osobowych w zgłoszonych do rejestracji zbiorach (punkty 4 i 10 zgłoszenia). Listę aktów prawnych administrator może również uzupełnić poprzez samodzielne wpisanie dodatkowych pozycji. Dzięki wprowadzeniu tej zmiany, administratorzy prowadzący zbiory danych w oparciu o przepisy prawa, mogą w sposób wygodny i szybki wskazać w zgłoszeniu podstawy prawne przetwarzania danych w zbiorze. Omawiana modyfikacja, wraz z systemem podpowiedzi i komunikatów, ogranicza możliwość popełnienia błędów przy wypełnianiu formularza zgłoszenia, skutkujących koniecznością prowadzenia postępowania wyjaśniającego.

W omawianym okresie sprawozdawczym **11 559 zgłoszeń dokonano drogą elektroniczną** przy użyciu ww. programu, w tym 2289 zgłoszeń opatrzonych było podpisem elektronicznym, co stanowi 20 % wszystkich zgłoszeń przesłanych elektronicznie i 15 % ogólnej liczby zgłoszeń nadesłanych do rejestracji w 2011 r. Zgłoszenia dokonane drogą elektroniczną stanowiły 74 % wszystkich zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2011 r., co oznacza, że w stosunku do roku poprzedniego, gdzie zgłoszeń tych było 4929, nastąpił wzrost o 14 %.

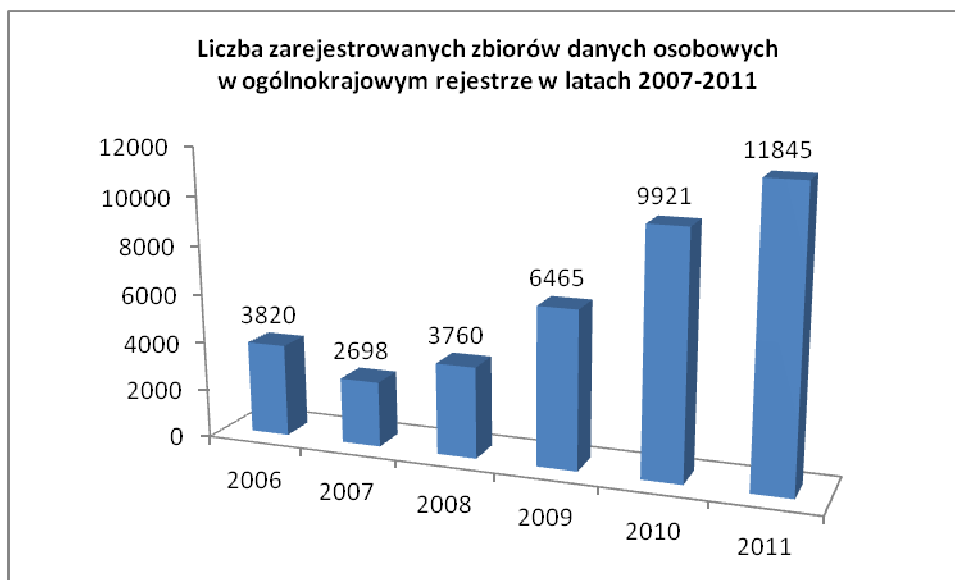


Wykres 29: *Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonywanych w 2011 r. w formie tradycyjnej i elektronicznej.*



Wykres 30: *Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2009-2011 w formie tradycyjnej i przy użyciu programu wspomagającego, udostępnionego na stronie www.giodo.gov.pl*

W okresie sprawozdawczym do **ogólnokrajowego publicznego rejestru zbiorów danych osobowych** prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych zostało wpisanych **11845** zbiorów danych, tj. o 19 % więcej niż w roku 2010 r. i aż o 83 % więcej niż w roku 2009.



Wykres 31: Zestawienie porównawcze zarejestrowanych zbiorów danych osobowych w ogólnokrajowym rejestrze w latach 2009 - 2011.

Chociaż liczba zarejestrowanych zbiorów danych osobowych stale rośnie, nie zawsze informacje zawarte w zgłoszeniu pozwalały na zakończenie sprawy bez przeprowadzenia postępowania wyjaśniającego. Dzięki systemowi podpowiedzi w programie komputerowym służącym do wypełnienia zgłoszenia zbioru danych do rejestracji, znacznie zmniejszyła się liczba zgłoszeń, które nie zawierają informacji, o których mowa w art. 41 ust. 1 ustawy, toteż wyjaśnienia w prowadzonych postępowaniach dotyczą głównie przestrzegania przez administratorów danych zasad przetwarzania danych osobowych.

W ramach postępowania prowadzonego w związku ze zgłoszeniem zbioru do rejestracji dokonywana jest szczegółowa analiza i ocena treści zgłoszenia. W trakcie postępowania 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 ustawy¹²¹. W tym miejscu należy zwrócić uwagę, że z dniem 2 stycznia 2011 r. nowe brzmienie

¹²¹ Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych: 1) zawierających informacje niejawne, 1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności, 2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym, 2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej, 2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, 2c) przetwarzanych przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, 3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego, 4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się, 5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego

otrzymał pkt 1 w art. 43 ust. 1 ustawy, który stanowił dotychczas, że z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego. Po nowelizacji dokonanej ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz.1228) przepis w nowym brzmieniu zwalnia z obowiązku rejestracji zbioru danych administratorów danych zawierających informacje niejawne. Z kolei, ustawą z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz. U. Nr 230, poz. 1371), w art. 43 ust. 1 dodany został pkt 2c przewidujący zwolnienie z obowiązku zgłoszenia zbioru do rejestracji administratorów danych przetwarzanych przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej. Przepis ten wszedł w życie w dniu 1 stycznia 2012 r.

Jeśli ma miejsce sytuacja uniemożliwiająca zarejestrowanie zbioru danych, wówczas Generalny Inspektor Ochrony Danych Osobowych kierował do wnioskodawcy pismo informujące o braku podstaw do dokonania, na podstawie złożonego zgłoszenia, wpisów w rejestrze.

W roku 2011 zostały wysłane **603** takie pisma, w tym **327** pism informujących administratorów danych o braku obowiązku rejestracji zbioru, wynikającym z przesłanek określonych w art. 43 ust. 1 ustawy oraz **276** pism informujących o braku podstaw do dokonania wpisów w rejestrze z innych przyczyn niż wynikające z powołanego powyżej przepisu (dotyczyły one 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).

W podsumowaniu stwierdzić należy, że 2011 roku w toku postępowań rejestracyjnych do wnioskodawców skierowano ogółem **1598 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 na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego skierowano do wnioskodawców **1164 wezwań** do uzupełnienia w zgłoszeniu braku podpisu lub braku potwierdzenia umocowania wnioskodawcy do reprezentowania administratora danych.

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. 23-28

rewidenta, 6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego, 7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności, 8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, 9) powszechnie dostępnych, 10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, 11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

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. Zatem w postępowaniu rejestracyjnym ocenie poddawany jest 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 dokonywana jest analiza przepisów prawa regulujących zadania lub działalność, w związku z realizacją których administrator przetwarza dane osobowe w zbiorze.

W kontekście przesłanek wydania przez Generalnego Inspektora Ochrony Danych Osobowych decyzji o odmowie rejestracji nadmienić należy, że w dniu 7 marca 2011 r. weszła w życie ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. Nr 229, poz.1497). W wyniku tej nowelizacji zmianie uległo brzmienie art. 41 ust. 1 pkt 2 ustawy, dotyczącego informacji, jakie powinno zawierać zgłoszenie zbioru danych do rejestracji. Do tej pory przepis ten wskazywał, że zgłoszenie powinno zawierać m.in. oznaczenie podmiotu prowadzącego zbiór. W wyniku nowelizacji zwrot „podmiot prowadzący zbiór” został zastąpiony zdefiniowanym w ustawie pojęciem administratora danych. Przepis w nowym brzmieniu wskazuje również, że w przypadku powierzenia przetwarzania danych podmiotowi, o którym mowa w art. 31 ustawy, elementem zgłoszenia powinno być oznaczenie tego podmiotu i adresu jego siedziby lub miejsca zamieszkania. Podkreślić należy, że omawiana zmiana miała przede wszystkim znaczenie porządkowe, bowiem wzór zgłoszenia stanowiący załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536), w pkt 1 części B, posługiwał się pojęciem administratora danych, a pkt 3 tej części zgłoszenia wymagał podania informacji o powierzeniu przez administratora przetwarzania danych oraz o podmiocie, na rzecz którego takie powierzenie nastąpiło. Brak oznaczenia w zgłoszeniu podmiotu, któremu administrator powierzył przetwarzanie danych i adresu jego siedziby lub miejsca zamieszkania, stanowi przesłankę wydania przez Generalnego Inspektora Ochrony Danych Osobowych decyzji o odmowie rejestracji zbioru na podst. art. 44 ust. 1 pkt 1 ustawy.

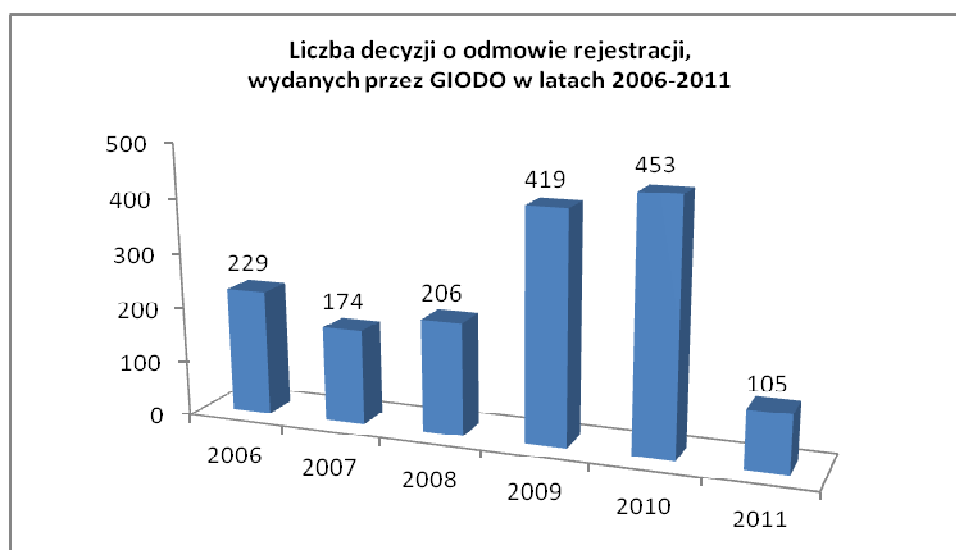
Ww. nowelizacja dotyczyła również art. 44 ust. 1 pkt 2 ustawy, który stanowił, że Generalny Inspektor Ochrony Danych Osobowych wydaje decyzję o odmowie rejestracji zbioru danych osobowych, jeżeli przetwarzanie danych naruszałoby zasady określone w art. 23 – 30 ustawy. Po nowelizacji odmowa rejestracji zbioru na podstawie art. 44 ust. 1 pkt 2 ustawy jest następstwem naruszenia zasad określonych w art. 23 – 28 ustawy, a konieczność zmiany przepisu wiązała się z uchynieniem art. 29 i 30 ustawy, które określały zasady udostępniania przez administratorów danych osobowych w celach innych niż włączenie do zbioru.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **105 decyzji o odmowie rejestracji zbioru danych, 45 decyzji o umorzeniu postępowania, 268 decyzje o wykreśleniu zbioru danych z ogólnokrajowego jawnego rejestru zbiorów danych osobowych oraz 1 decyzję po ponownym rozpatrzeniu sprawy** dotyczącej odmowy rejestracji zbioru.



Wykres 32: Liczbowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2011 r.

Działania legislacyjne, edukacyjne, organizacyjne i techniczne podjęte w roku 2011 i w latach ubiegłych miały znaczny wpływ na zmniejszenie się liczby decyzji o odmowie rejestracji zbioru danych, przy jednoczesnym wzroście liczby zbiorów zarejestrowanych.



Wykres 33: Zestawienie porównawcze decyzji o odmowie rejestracji zbioru wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2009 - 2011.



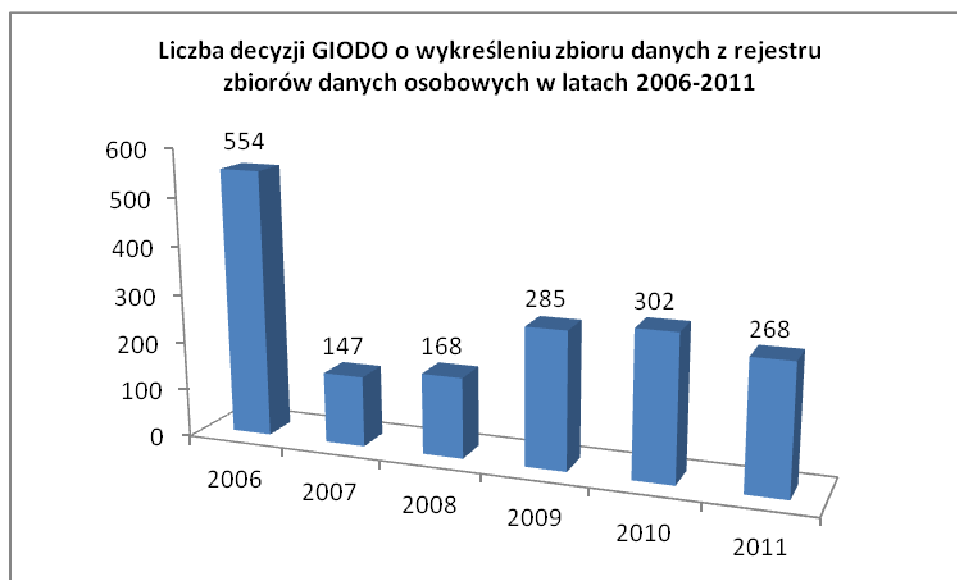
Wykres 34: Zestawienie porównawcze decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2009 - 2011.

Należy zwrócić uwagę, że 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. Świadomość negatywnych konsekwencji związanych z odmową rejestracji zbioru danych niewątpliwie mobilizuje administratorów danych do tego, aby przed zgłoszeniem dokonali oceny, czy spełnione są wszystkie wymogi przewidziane w ustawie o ochronie danych osobowych. Zgodnie z art. 41 ust. 2 ustawy, co do zasady, administrator danych obowiązany jest zgłaszać każdą zmianę informacji zawartych w zgłoszeniu do rejestracji w terminie 30 dni od dnia dokonania zmiany w zbiorze danych, a w przypadku zaprzestania przetwarzania danych, na podstawie art. 44a ustawy wydawana jest decyzja o wykreśleniu zbioru z rejestru. Działania te służą aktualności rejestru i umożliwiają jego porządkowanie, zgodnie ze zmieniającymi się okolicznościami przetwarzania danych.

Odnosnie obowiązku zgłaszania przez administratora danych każdej zmiany informacji zawartych w zgłoszeniu rejestracyjnym zauważyć warto, że w wyniku wejścia w życie w dniu 7 marca 2011 r. nowelizacji ustawy nastąpiło sprecyzowanie terminu, w jakim administrator powinien zgłosić Generalnemu Inspektorowi Ochrony Danych Osobowych zmianę informacji o zakresie przetwarzanych danych, dotyczącą rozszerzenia tego zakresu o tzw. dane szczególnie chronione, o których mowa w art.

27 ust. 1 ustawy¹²². Zgodnie z dodanym przepisem ust. 3 w art. 41 ustawy o ochronie danych osobowych, administrator zobowiązany jest dokonać ww. zgłoszenia przed dokonaniem zmiany w zbiorze.

Ponadto Generalny Inspektor Ochrony Danych Osobowych wydał **268 decyzji o wykreśleniu** zbioru danych z ogólnokrajowego publicznego rejestru zbiorów danych osobowych z powodu zaprzestania przetwarzania danych w zbiorze.



Wykres 35: *Zestawienie porównawcze decyzji o wykreśleniu zbioru danych z rejestru zbiorów danych osobowych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2009 - 2011.*

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 ustawy¹²³, jak również instytucja wykreślenia. Obie te instytucje stwarzają możliwość porządkowania rejestru, zgodnie ze zmieniającymi się okolicznościami przetwarzania danych.

W 2011 roku zostało rozpatrzonych **3050 zgłoszeń aktualizacyjnych** dokonanych przez administratorów danych. 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 przetwarzanych danych osobowych.

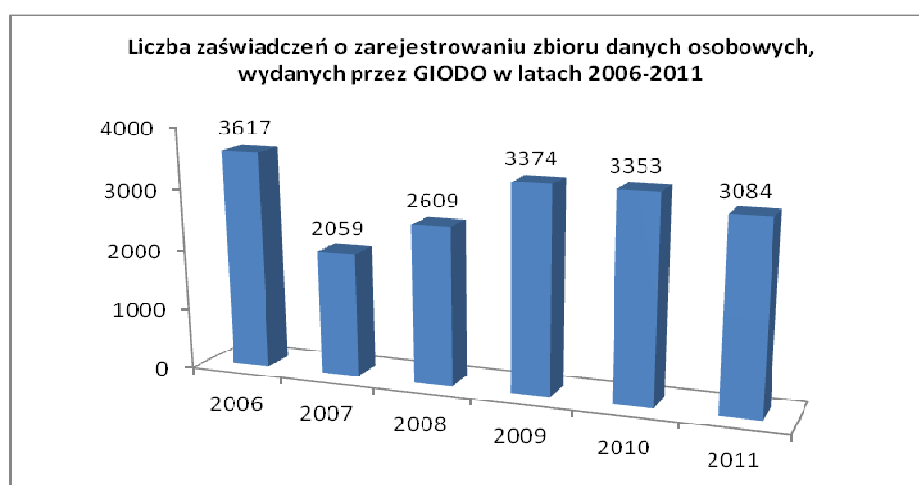
¹²² Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

¹²³ 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.



Wykres 36: Zestawienie porównawcze zgłoszeń aktualizacyjnych rozpatrzonych w latach 2009 - 2011.

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 **3084 zaświadczenia o zarejestrowaniu zbioru**. Generalny Inspektor wydaje zaświadczenia o zarejestrowaniu zgłoszonego zbioru danych na wniosek administratora¹²⁴. 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 zbioru¹²⁵.



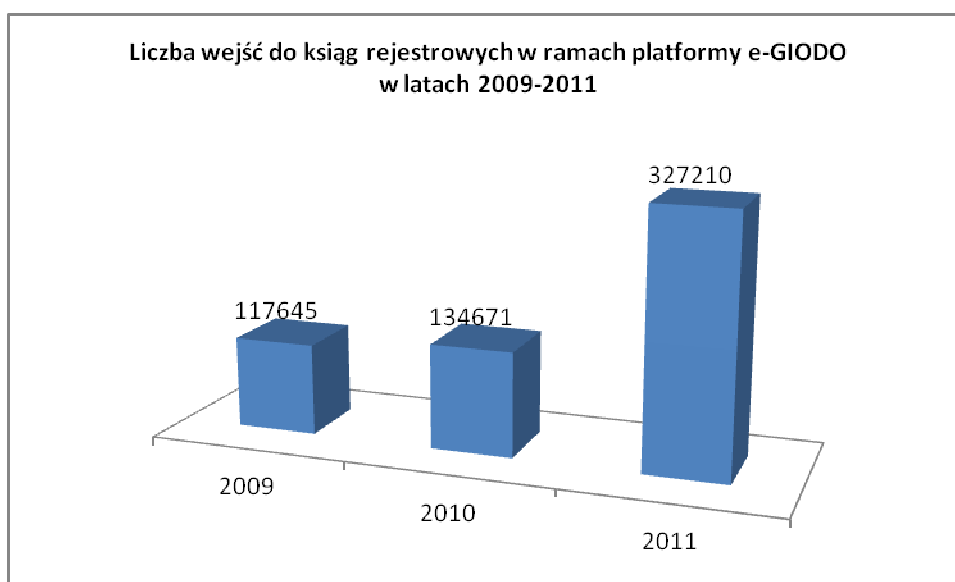
Wykres 37: Zestawienie liczby zaświadczeń o zarejestrowaniu zbioru danych osobowych wydanych w latach 2009 - 2011.

¹²⁴ Art. 42 ust. 3 ustawy

¹²⁵ Art. 42 ust. 4 ustawy o ochronie 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) 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 2011 w elektronicznej wersji rejestru odnotowano **327 210** wejść do poszczególnych ksiąg rejestrowych, tj. o prawie dwa i pół razy więcej niż w roku 2010, w którym wejść tych było 134 671.



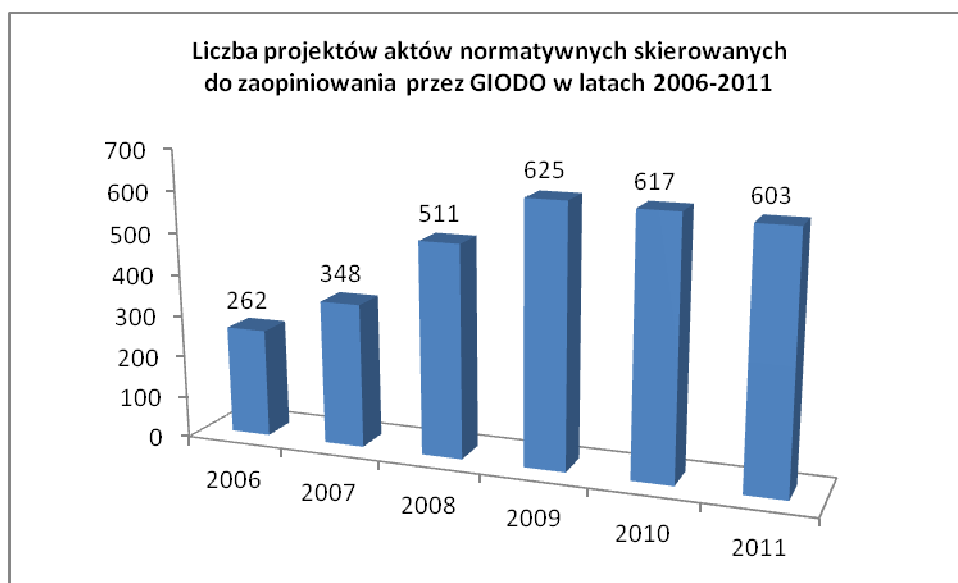
Wykres 38: *Liczbowe zestawienie wejść do poszczególnych ksiąg rejestrowych w rejestrze zbiorów danych osobowych w ramach platformy e-GIODO w latach 2009 - 2011.*

W okresie od stycznia do grudnia 2011 roku, poza korespondencją prowadzoną w związku z postępowaniami rejestracyjnymi, wysłano **44 odpowiedzi na pytania** dotyczące problematyki rejestracji zbiorów danych osobowych, tj. interpretacji przepisów zawierających zwolnienia z obowiązku rejestracji, czy określenia podmiotów zobowiązanych do zgłoszenia zbioru do rejestracji na podstawie obowiązujących przepisów.

5. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych

Na wyeliminowanie licznych – jak wykazuje praktyka - nieprawidłowości dotyczących przetwarzania danych osobowych już na etapie procesu tworzenia prawa, pozwala uprawnienie przyznane Generalnemu Inspektorowi w art. 12 pkt 5 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 2011 do Biura GIODO wpłynęły do zaopiniowania **603 projekty aktów prawnych**, a zatem odnotować należy nieznaczny spadek w tej kategorii względem roku poprzedniego, w którym wpłynęło 617 takich projektów.



Wykres 39: *Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2011.*

Ze względu aktualną problematykę organizacji turnieju finałowego UEFA EURO 2012, znaczną uwagę Generalny Inspektor poświęcił projektowi *ustawy o zmianie ustawy o bezpieczeństwie imprez masowych oraz o zmianie niektórych innych ustaw* (na początkowym etapie prac legislacyjnych projekt ten nosił nazwę projektu ustawy o zmianie ustawy o bezpieczeństwie imprez masowych oraz o zmianie niektórych innych ustaw, a także o zapewnieniu bezpieczeństwa w związku z organizacją Turnieju Finałowego UEFA EURO 2012), w pracach nad którym brał aktywny udział prezentując obszerne stanowisko.

Uwagę Generalnego Inspektora Ochrony Danych Osobowych absorbowwała również kontynuacja procesu legislacyjnego nad projektem *ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej*, który finalnie wprowadził zmiany do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

W okresie objętym sprawozdaniem opiniowany był projekt *założeń projektu ustawy o redukcji obowiązków informacyjnych oraz o ograniczeniu barier administracyjnych dla obywateli i przedsiębiorców*¹²⁶. Generalny Inspektor zaoponował przeciwko propozycji¹²⁷ wprowadzenia czternastodniowego terminu na rejestrację zbioru danych zawierającego dane szczególnie chronione w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych¹²⁸ oraz na zarejestrowanie zbioru danych po jego ponownym zgłoszeniu po usunięciu wad, które były powodem odmowy rejestracji zbioru¹²⁹. Co więcej, GODO uznał wprowadzenie „szybnego” czternastodniowego terminu za niemożliwy zarówno z przyczyn faktycznych, jak i z uwagi na uwarunkowania wynikające z innych przepisów ustawy o ochronie danych osobowych. O ile bowiem sam wpis zbioru danych do ogólnokrajowego, jawnego rejestru zbiorów danych osobowych stanowi czynność materialno-techniczną, to poprzedzony on zostaje analizą i oceną treści zgłoszenia. Przed dokonaniem wpisu Generalny Inspektor Ochrony Danych Osobowych musi przede wszystkim ustalić, czy nie zachodzi któraś ze wskazanych enumeratywnie w art. 44 ust. 1 ustawy o ochronie danych osobowych, przesłanek odmowy rejestracji zgłoszonego zbioru danych¹³⁰.

Generalny Inspektor podniósł, że powyższa ocena ma szczególnie istotne znaczenie z punktu widzenia ochrony praw osób, których dane dotyczą, w sytuacji gdy przedmiotem przetwarzania w zbiorze danych mają być dane sensytywne¹³¹, a dokonanie rzetelnej analizy w proponowanym w projekcie założeniu terminie nie jest realne. Zbyt pochopna ocena w tym zakresie byłaby niezgodna z prawem i prowadziła do daleko idących i niekorzystnych dla zgłaszającego skutków¹³². Generalny Inspektor ocenił, że wzgląd na konieczność dokonywania prawidłowych rozstrzygnięć przez organ do spraw ochrony danych osobowych musi w tej sytuacji mieć prymat przed szybkością postępowania¹³³.

¹²⁶ DOLiS-033-60/11

¹²⁷ Zamieszczonej na s. 62 projektu założeń.

¹²⁸ zob. zmiana art. 42 ustawy o ochronie danych osobowych.

¹²⁹ zob. zmiana art. 44 ustawy o ochronie danych osobowych.

¹³⁰ tzn. czy zgłoszenie zawiera wszystkie wymagane informacje, o których mowa w art. 41 ust. 1 ustawy o ochronie danych osobowych, czy przetwarzanie danych osobowych w zgłoszonym do rejestracji zbiorze danych nie naruszałoby zasad określonych w art. 23-28 ustawy o ochronie danych osobowych (w szczególności – czy dane przetwarzane są zgodnie z prawem, czy dane są adekwatne w stosunku do celów, w jakich są przetwarzane), czy urządzenia i systemy informatyczne służące do przetwarzania danych spełniają podstawowe warunki techniczne i organizacyjne określone w przepisach wydanych na podstawie art. 39a ustawy o ochronie danych osobowych.

¹³¹ W przypadku danych sensytywnych przedmiotem wyjątkowej troski ze strony organu do spraw ochrony danych osobowych musi być dokonanie prawidłowych ustaleń w przedmiocie: prawnej dopuszczalności zbierania takich danych, ich adekwatności w stosunku do deklarowanego celu zbierania, zastosowanego przez administratora danych poziomu bezpieczeństwa zebranych danych.

¹³² Stwierdzenie naruszenia którejkolwiek z zasad przetwarzania danych osobowych implikuje bowiem po stronie Generalnego Inspektora Ochrony Danych Osobowych obowiązek wydania decyzji o odmowie rejestracji zbioru danych (art. 44 ust. 1 ustawy o ochronie danych osobowych). Decyzja ta zaś skutkować może nałożeniem na administratora danych obowiązku usunięcia zebranych danych. Tak więc skutki odmowy rejestracji zbioru danych mogą mieć negatywny wpływ na całą działalność wnioskodawcy, często wręcz uniemożliwiając jej kontynuowanie.

¹³³ W 2010 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło 8260 zgłoszeń zbiorów danych do rejestracji i liczba tych zgłoszeń systematycznie rośnie (w 2008 roku administratorzy danych zgłosili do rejestracji 5776 zbiorów, w roku 2009 – 7688 zbiorów). W tym samym roku (2010) Generalny Inspektor Ochrony Danych Osobowych zwracał się do wnioskodawców w 1828 pismach o złożenie niezbędnych wyjaśnień lub dowodów w procedurze rejestracji

Oprócz – wskazanej wyżej – propozycji *zmiany ustawy o ochronie danych osobowych*, wątpliwości Generalnego Inspektora wzbudził, zawarty w projekcie założeń¹³⁴, postulat zmiany art. 22 ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (t. j. Dz. U. z 2010 r. Nr 11, poz. 66 z późn. zm.). Wbrew bowiem twierdzeniu projektodawcy zaproponowana zmiana tego przepisu nie miała charakteru technicznego (dopuszczenie formy elektronicznej), lecz merytoryczny. GIODO podniósł, iż wprowadzony w art. 22 ust. 3 w zw. z ust. 1 ustawy o działalności ubezpieczeniowej wymóg uzyskania przez zakład ubezpieczeń pisemnej zgody ubezpieczonego (osoby, na rzecz której ma zostać zawarta umowa ubezpieczenia albo jej przedstawiciela ustawowego) na pozyskanie przez zakład ubezpieczeń od podmiotów, o których mowa w art. 4 ustawy o zakładach opieki zdrowotnej (t. j. Dz. U. z 2007 r. Nr 14, poz. 89 z późn. zm.), które udzielały świadczeń zdrowotnych ubezpieczonemu lub osobie, na rzecz której ma zostać zawarta umowa ubezpieczenia, informacji o okolicznościach związanych z oceną ryzyka ubezpieczeniowego i weryfikacją podanych przez tę osobę danych o jej stanie zdrowia, ustaleniem prawa tej osoby do świadczenia z zawartej umowy ubezpieczenia i wysokością tego świadczenia, a także informacji o przyczynie śmierci ubezpieczonego (z wyłączeniem wyników badań genetycznych), stanowi bezpośrednie przeniesienie na grunt prawa ubezpieczeń dyspozycji art. 27 ust. 2 pkt 1 w zw. z ust. 1 tego przepisu ustawy o ochronie danych osobowych¹³⁵. Generalny Inspektor podniósł, że zamieszczona w projekcie założeń propozycja nowego brzmienia art. 22 ustawy o działalności ubezpieczeniowej¹³⁶, stanowi w istocie próbę ominięcia przepisów dotyczących formy czynności prawnej¹³⁷. Zaakcentowania wymagało, że propozycja taka pozostaje w sprzeczności z dyspozycją art. 58 §1 oraz art. 73 §1 ustawy – Kodeks cywilny.

Generalny Inspektor wyraził stanowisko, że rozwiązanie przedstawione w projekcie założeń wydaje się zbędne w świetle brzmienia art. 78 §2 ustawy – Kodeks cywilny¹³⁸. W obowiązującym stanie prawnym nie ma przeszkód, by zakład ubezpieczeń występował za pomocą środków komunikacji elektronicznej do podmiotu, o którym mowa w art. 4 ustawy o zakładach opieki

(nie może zaś umknąć uwadze, że dopiero po analizie nadesłanych wyjaśnień możliwa jest rejestracja zbioru danych lub wydanie decyzji o odmowie rejestracji).

¹³⁴ zob. s. 43 – 44.

¹³⁵ Powołane przepisy ustawy o ochronie danych osobowych nakładają bowiem konieczność zachowania formy pisemnej dla zgody osoby, której dane dotyczą, na przetwarzanie (w tym udostępnienie – art. 7 pkt 2 ustawy o ochronie danych osobowych) dotyczących jej danych szczególnie chronionych (w niniejszym przypadku – danych o stanie zdrowia), przy czym – w świetle jednoznacznego brzmienia art. 27 ust. 2 pkt 1 w zw. z ust. 1 ustawy o ochronie danych osobowych – forma ta zastrzeżona jest pod rygorem nieważności.

¹³⁶ Zgodnie z tą propozycją zakład ubezpieczeń mógłby wystąpić do podmiotu, o którym mowa w art. 4 ustawy o zakładach opieki zdrowotnej, z wnioskiem o udostępnienie wskazanych informacji, legitymując się zgodą ubezpieczonego (osoby, na rzecz której ma zostać zawarta umowa ubezpieczenia albo jej przedstawiciela ustawowego) wyrażoną za pomocą środków komunikacji elektronicznej w przypadku, gdy ubezpieczony (osoba na rzecz której ma zostać zawarta umowa ubezpieczenia albo jej przedstawiciel ustawowy) złoży zakładowi ubezpieczeń pisemny wniosek o zastosowanie do takiego udostępnienia środków komunikacji elektronicznej.

¹³⁷ Zob. dział III tytułu IV książki pierwszej ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz. U. Nr 16, poz. 93 z późn. zm.

¹³⁸ Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne z oświadczeniem woli złożonym w formie pisemnej.

zdrowotnej, z wnioskiem o udostępnienie informacji wskazanych w art. 22 ust. 1 ustawy o działalności ubezpieczeniowej, jeżeli wniosek taki będzie zawierał zgodę ubezpieczonego (osoby na rzecz której ma zostać zawarta umowa ubezpieczenia albo jej przedstawiciela ustawowego) na udostępnienie takich informacji wyrażoną w formie, którą art. 78 §2 ustawy – Kodeks cywilny uznaje za równoważną z formą pisemną.

Kontynuując opiniowanie projektu dokumentu pt. *„Założenia do projektu ustawy o zmianie ustawy o zasadach ewidencji i identyfikacji podatników i płatników oraz o zmianie niektórych innych ustaw”*¹³⁹, Generalny Inspektor Ochrony Danych Osobowych podniósł, iż przedstawiona przez Ministerstwo Finansów propozycja wykorzystania administracyjnego numeru identyfikacyjnego jako identyfikatora w kontaktach z administracją podatkową nie jest rozwiązaniem powszechnie przyjętym w ustawodawstwach państw europejskich. W kilku krajach unijnych (np. RFN, Czechy) uznano nawet, iż wykorzystywanie we wszystkich kontaktach z administracją publiczną jednego numeru identyfikacyjnego obywatela stanowiłoby nadmierną ingerencję w jego prywatność¹⁴⁰. Nie negując prawa projektodawcy do zmiany istniejącego stanu prawnego¹⁴¹, Generalny Inspektor Ochrony Danych Osobowych zobligowany był do wskazania, że zaproponowane przez Ministerstwo Finansów wykorzystanie numeru PESEL jako identyfikatora w kontaktach z administracją podatkową, dla podatników będących osobami fizycznymi nieprowadzącymi 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 skarbowej¹⁴². Tym samym rozwiązania zaproponowane w projekcie założeń były kierunkowo odmienne, aniżeli unormowania rozdziału 3 ustawy o swobodzie działalności gospodarczej¹⁴³.

Organ do spraw ochrony danych osobowych stwierdził także, iż przyjęcie propozycji Ministerstwa Finansów przedstawionej w projekcie założeń, umożliwi ministrowi właściwemu do spraw finansów publicznych, jako organowi prowadzącemu Centralny Rejestr Podmiotów – Krajową

¹³⁹ DOLiS-033-447/10

¹⁴⁰ Administracyjne numery identyfikacyjne (odpowiedniki polskiego numeru identyfikacyjnego Powszechnego Elektronicznego Systemu Ewidencji Ludności – numeru PESEL) nie mogą być w tych krajach wykorzystywane w innych, aniżeli administracyjne, celach, zaś obywatel posiada kilka numerów identyfikacyjnych, odrębnych w każdym sektorze jego współdziałania z administracją.

¹⁴¹ Dotychczas w Rzeczypospolitej Polskiej, zgodnie z art. 2 ust. 1 ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (t. j. Dz. U. z 2004 r. Nr 269, poz. 2681 z późn. zm.), wszyscy podatnicy mieli nadawany numer identyfikacji podatkowej (numer NIP) wykorzystywany w kontaktach z administracją podatkową lub celną (art. 11 ustawy o zasadach ewidencji i identyfikacji podatników i płatników).

¹⁴² Zmiana art. 15 ust. 1 ustawy o zasadach ewidencji i identyfikacji podatników i płatników przedstawiona na s. 25 projektu założeń.

¹⁴³ Art. 37 ust. 1 pkt 1 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (t. j. Dz. U. z 2007 r. Nr 155, poz. 1095 z późn. zm.) uznał 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.

Ewidencję Podatników¹⁴⁴, dokonywanie unifikacji w oparciu o jeden identyfikator zbiorów danych prowadzonych przez różne podmioty publiczne. W związku z tym Generalny Inspektor wskazał, że nakłada to na ministra właściwego do spraw finansów publicznych 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.

Zasadnicze wątpliwości Generalnego Inspektora Ochrony Danych Osobowych – z uwagi na zasady ochrony danych osobowych (zwłaszcza zasadę celowości i zakaz zbierania danych „na zapas”) – wzbudziła koncepcja przekształcenia Krajowej Ewidencji Podatników¹⁴⁵ w Centralny Rejestr Podmiotów – Krajową Ewidencję Podatników (CRP KEP). Zgodnie z obowiązującymi przepisami¹⁴⁶ Krajowa Ewidencja Podatników zawiera dane ze zgłoszeń identyfikacyjnych i aktualizacyjnych podatników¹⁴⁷. Tymczasem projekt założeń¹⁴⁸ przewidywał 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 miałby w istocie obejmować swoim zakresem osoby niebędące podatnikami (np. noworodki, osoby o polskim obywatelstwie pozostające na stałe za granicą) i to nawet takie, które nigdy takimi podatnikami się nie staną. Tworzenie takiego zbioru zostało również przez Generalnego Inspektora zakwestionowane jako dublowanie, utworzonego i mającego być prowadzonym na podstawie ustawy o ewidencji ludności i dowodach osobistych zbioru (rejestr) PESEL. Zarówno obowiązująca ustawa o ewidencji ludności i dowodach osobistych, jak i ustawa o ewidencji ludności, przewidują w swojej treści rozwiązania pozwalające na wykorzystywanie przez administrację podatkową danych zgromadzonych w zbiorze PESEL (od 1 sierpnia 2010 r. – rejestrze PESEL)¹⁴⁹.

Nie negując prawa administracji podatkowej do prowadzenia bazy danych osób, w stosunku do których zaistniało jakiekolwiek zdarzenie skutkujące powstaniem obowiązku podatkowego w rozumieniu ustawy – Ordynacja podatkowa, czyli bazy danych podatników, organ do spraw ochrony danych osobowych pozostawił pod rozważę autorów projektu założeń kwestię zakresu pozyskiwanych

¹⁴⁴ Zmiana art. 14 ustawy o zasadach ewidencji i identyfikacji podatników i płatników przedstawiona na s. 22 projektu założeń.

¹⁴⁵ Art. 14 obowiązującej ustawy o zasadach ewidencji i identyfikacji podatników i płatników.

¹⁴⁶ Art. 14 ust. 2 pkt 1 ustawy o zasadach ewidencji i identyfikacji podatników i płatników.

¹⁴⁷ Tzn. osób fizycznych, osób prawnych lub jednostek organizacyjnych niemających osobowości prawnej, podlegających na mocy ustaw podatkowych obowiązkowi podatkowemu – art. 7 § 1 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, t. j. Dz. U. z 2005 r. Nr 8, poz. 60 z późn. zm.

¹⁴⁸ zob. s. 6.

¹⁴⁹ Dane te mogłyby być udostępnianie organom podatkowym po wykazaniu przez te organy, iż są one niezbędne do realizacji ich ustawowych zadań (art. 44 h ust. 1 ustawy o ewidencji ludności i dowodach osobistych; art. 46 ust. 1 ustawy o ewidencji ludności), w tym również w drodze teletransmisji danych (art. 44 h ust. 5 ustawy o ewidencji ludności i dowodach osobistych; art. 48 ustawy o ewidencji ludności). Możliwe byłoby także skorzystanie z instytucji prawnej weryfikacji danych (art. 44 h ust. 6 i 7 ustawy o ewidencji ludności i dowodach osobistych; art. 49 ust. 1 i 3 ustawy o ewidencji ludności).

danych. Proponowany katalog tych danych¹⁵⁰ wydał się bowiem nadmiernie szeroki w stosunku do – deklarowanego w projekcie założeń – celu tworzenia takiej bazy. Generalny Inspektor zauważył, iż projekt założeń¹⁵¹ obliguje ministra właściwego do spraw wewnętrznych do niezwłocznego przekazywania ze zbioru (rejestr) PESEL do CRP KEP numeru telefonu i adresu e-mail osoby, której dane znajdują się w zbiorze (rejestrze) PESEL, podczas gdy zarówno obowiązująca ustawa o ewidencji ludności i dowodach osobistych (art. 44a ust. 1 pkt 2 w zw. z ust. 2 – 4), jak i ustawa o ewidencji ludności (art. 8), w ogóle nie przewidują gromadzenia w zbiorze (rejestrze) PESEL takich danych (informacji).

Z uwagi na zasadę ograniczenia czasowego Generalny Inspektor podniósł wątpliwość wobec – zamieszczonej w projekcie założeń – propozycji bezterminowego przechowywania danych osobowych w CRP KEP. 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 przedmiotem szczególnego zainteresowania ze strony organów Unii Europejskiej. Tymczasem przedstawiony projekt założeń pominął te kwestie milczeniem, przyjmując, iż raz pozyskane ze zbioru (rejestr) PESEL dane osobowe będą mogłyby być przechowywane przez administrację podatkową w CRP KEP aż do otrzymania informacji o zgonie osoby, której dane te dotyczą. Rozwiązanie takie nie jest zgodne z podejmowanymi przez organ do spraw ochrony danych osobowych działaniami zmierzającymi do unormowania okresu przechowywania danych osobowych w zbiorach policyjnych, czy też w innych zbiorach wykorzystywanych w zwalczaniu przestępczości.

W bieżącym okresie sprawozdawczym Generalny Inspektor kontynuował również opiniowanie – istotnego z punktu widzenia zasad ochrony danych osobowych – projektu *ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej*¹⁵².

GIODO odniósł się negatywnie do konstrukcji tego projektu, mając na względzie wagę rozwiązań jakie muszą być przyjęte, zwłaszcza w związku z koniecznością implementacji w całości Decyzji Ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (co może pociągać zmianę ustawy o ochronie danych osobowych) - dokonano szczegółowej analizy postanowień ww. dyrektywy.

W ramach prac legislacyjnych nad przedmiotowym projektem Generalny Inspektor przedstawił propozycje zmian do ustawy o ochronie danych osobowych, których celem miało być umożliwienie

¹⁵⁰ W zmianie do art. 5 ust. 2 i art. 14 ustawy o zasadach ewidencji i identyfikacji podatników i płatników (s. 22 projektu założeń).

¹⁵¹ zob. s. 22.

¹⁵² DOLiS-033-452/10

organowi do spraw ochrony danych osobowych sprawowania funkcji krajowego organu nadzoru¹⁵³. Generalny Inspektor poinformował jednocześnie, że wprowadzenie do projektu skutecznych mechanizmów zapewniających kontrolę Generalnego Inspektora Ochrony Danych Osobowych nad procedurą wymiany danych, jest warunkiem koniecznym akceptacji przez niezależny organ do spraw ochrony danych osobowych przedmiotowego projektu.

Niezależnie od wykazanej konieczności uzupełnienia opiniowanego projektu ustawy o przepisy nowelizujące ustawę o ochronie danych osobowych, Generalny Inspektor wskazał, iż jego wątpliwości budzą zmiany¹⁵⁴ do ustawy z dnia 6 kwietnia 1990 r. o Policji (t. j. Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.). GODO podniósł, że skoro proponowana nowelizacja istotnie rozszerza kompetencje Policji do przetwarzania informacji, w tym danych osobowych¹⁵⁵, to zachodzi potrzeba wzmocnienia i doprecyzowania mechanizmu¹⁵⁶ dokonywania przez Policję weryfikacji przydatności zebranych danych¹⁵⁷.

Generalny Inspektor zauważył, iż – co do zasady – czynności operacyjno-rozpoznawcze są prowadzone przez ustawowo uprawnione organy na podstawie zgody sądu wyrażonej w konkretnej sprawie. Wysoce wątpliwym jest zatem, by dane zebrane w tym trybie przez ustawowo uprawnione organy mogłyby być wykorzystywane w innym postępowaniu oraz przekazywane innym organom, na co zezwalałby przepis ustawy o Policji¹⁵⁸ w zaproponowanym brzmieniu.

GODO zauważył również, iż zastosowane w projektowanym przepisie ustawy o Policji ogólne odesłanie do „zasad i trybu określonego w odrębnych przepisach” nie pozwala na jednoznaczne ustalenie, czy w procesie przetwarzania, w tym przekazywania do i z państw trzecich oraz organizacji międzynarodowych, danych przez Policję zapewnione będą stosowne (pełne) gwarancje ochrony tych danych (zwłaszcza danych sensytywnych). Dlatego też stwierdzić należało, iż w przypadku zaakceptowania przez projektodawców propozycji Generalnego Inspektora Ochrony Danych Osobowych dotyczących wprowadzenia zmian do ustawy o ochronie danych osobowych, zająć może również potrzeba odpowiedniego dostosowania przepisów projektu ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej. W przeciwnym przypadku – Generalny

¹⁵³ W rozumieniu art. 25 decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz. Urz. UE L 350 z dnia 30.12.2008, s. 60.

¹⁵⁴ Zaproponowane w art. 28 projektu ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej.

¹⁵⁵ Zob. zwłaszcza art. 20 ust. 2aa ustawy o Policji, dodany przez art. 28 pkt 1 lit. b projektu ustawy o wymianie; art. 20 ust. 3 ustawy o Policji, w brzmieniu nadanym przez art. 28 pkt 1 lit. d projektu ustawy o wymianie; art. 20 ust. 5a ustawy o Policji, dodany przez art. 28 pkt 1 lit. f projektu ustawy o wymianie; art. 20 ust. 15 ustawy o Policji, w brzmieniu nadanym przez art. 28 pkt 1 lit. g projektu ustawy o wymianie.

¹⁵⁶ Przewidzianego aktualnie w art. 20 ust. 17 ustawy o Policji.

¹⁵⁷ Możliwymi do wykorzystania w tej kwestii byłyby zwłaszcza rozwiązania przyjęte obecnie w art. 22a ust. 8 i n. ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz. U. Nr 104, poz. 708 z późn. zm.

¹⁵⁸ Art. 20 ust. 16a pkt 1.

Inspektor Ochrony Danych Osobowych podtrzymywałby negatywne stanowisko wobec tego projektu ustawy¹⁵⁹.

Generalny Inspektor zmuszony był, wobec nieuwzględnienia zgłoszonych propozycji, poinformować o konieczności dokonania ponownej całościowej analizy tego projektu pod kątem zgodności z przepisami ustawy o ochronie danych osobowych¹⁶⁰.

I tak, GODO stwierdził, że dotychczasowe prace nad projektem ustawy potwierdziły wątpliwość, co do prawidłowości przyjętego przez projektodawcę rozwiązania polegającego na implementowaniu jednym aktem prawnym kilku – różniących się między sobą – aktów prawnych Unii Europejskiej¹⁶¹. Skutkuje to przyjęciem w projekcie ustawy unormowań godzących wprost w prawa osób fizycznych wynikające z europejskiego ustawodawstwa dotyczącego ochrony danych osobowych.

Podstawowym zarzutem, konsekwentnie zgłaszanym przez organ do spraw ochrony danych osobowych w trakcie całej procedury uzgodnień, było pominięcie w projekcie ustawy kompetencji Generalnego Inspektora Ochrony Danych Osobowych jako niezależnego krajowego organu nadzoru¹⁶². Już tylko ten brak był wystarczający do całkowitego zanegowania projektu ustawy jako niezgodnego z wiążącymi Rzeczypospolitą Polską aktami prawnymi Unii Europejskiej oraz art. 8 ust. 1 ustawy o ochronie danych osobowych.

Oprócz powyższego, projekt ustawy, wprowadzając ramy dla wymiany informacji (w tym danych osobowych) pomiędzy wskazanymi w nim podmiotami uprawnionymi, pomijał milczeniem kwestię zapewnienia ochrony praw osób, których dane te dotyczą¹⁶³.

¹⁵⁹ Wyrażone w piśmie z dnia 22 grudnia 2010 r. o sygn. DOLiS-033-452/10/50904.

¹⁶⁰ Pismo z dn. 16 marca 2011 r. znak: 11627/11.

¹⁶¹ Projektodawcy umknął bowiem fakt, iż decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz. Urz. UE L 386 z 29.12.2006, s. 89), powoływana dalej z zastosowaniem skrótu „decyzja ramowa 2006/960/WSiSW”, i decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. Urz. UE L 350 z dnia 30.12.2008, s. 60), powoływana dalej z zastosowaniem skrótu „decyzja ramowa 2008/977/WSiSW”, dotyczą jedynie zbliżonych, a nie tożsamyh stanów faktycznych. Przedmiotem decyzji ramowej 2006/960/WSiSW jest przetwarzanie (w tym przekazywanie) informacji i danych wywiadowczych, czyli: „każdego rodzaju informacji lub danych w posiadaniu organów ścigania” i „każdego rodzaju informacji lub danych w posiadaniu władz publicznych lub podmiotów prywatnych, które są dostępne organom ścigania bez stosowania środków przymusu...” – art. 2 pkt d decyzji ramowej 2006/960/WSiSW, zaś decyzja ramowa 2008/977/WSiSW dotyczy wprost przetwarzania (w tym przekazywania) danych osobowych („wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dotyczą dane”); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny lub jeden lub więcej szczególnych czynników określających jej tożsamość fizyczną, fizjologiczną, psychiczną, ekonomiczną, kulturową czy społeczną” – art. 2 pkt a decyzji ramowej 2008/977/WSiSW). Tym samym – o ile w przypadku decyzji ramowej 2006/960/WSiSW przekazaniu mogą podlegać wszelkie przydatne dla celów ścigania informacje – w tym niepełne, niepotwierdzone, niezwyfikowane, to decyzja ramowa 2008/977/WSiSW dotyczy już wprost przekazywania w ramach współpracy policyjnej i sądowej danych osobowych, a więc skonkretyzowanych informacji o osobie fizycznej. Co za tym idzie – poziom ochrony praw i wolności osób fizycznych musi być zdecydowanie wyższy, gdy przekazywanie ich danych odbywa się w oparciu o decyzję ramową 2008/977/WSiSW, aniżeli wówczas, gdy zastosowanie znajduje decyzja ramowa 2006/960/WSiSW. Tymczasem projekt ustawy nie tylko nie uwzględnia powyższego rozróżnienia, lecz w samych założeniach neguje jego istnienie.

¹⁶² W rozumieniu art. 25 decyzji ramowej 2008/977/WSiSW.

¹⁶³ Tymczasem w problematyce ochrony danych osobowych zagadnienie to ma bardzo dużą wagę, na co w ostatnim czasie wskazała Komisja Europejska w dokumencie: Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady,

Wobec – podniesionych wcześniej – zasadniczych uwag do projektu ustawy, zasygnalizowano wątpliwości o charakterze szczegółowym. I tak: przedstawiona w projekcie ustawy propozycja brzmienia art. 18 była w dalszym ciągu niezgodna z przepisami¹⁶⁴ decyzji ramowej 2008/977/WSiSW, jak również pozostawała niespójna z propozycją¹⁶⁵ nowego ujęcia znamion art. 47 ustawy o ochronie danych osobowych¹⁶⁶; wysoce wątpliwe było już samo założenie, które legło u podstaw sformułowania¹⁶⁷, zgodnie z którym dopuszczalne jest wprowadzenie identycznych zasad dla wymiany danych osobowych między polską Policją a organami państw członkowskich Unii Europejskiej (które to państwa są zobligowane normami prawa europejskiego do przyjęcia i przestrzegania regulacji dotyczących problematyki ochrony danych osobowych) oraz między Policją a organami państw trzecich (zwłaszcza nienależących do strefy Schengen), które to państwa w ogóle mogą nie posiadać jakiegokolwiek ustawodawstwa w zakresie ochrony danych osobowych¹⁶⁸; jak wskazuje tytuł¹⁶⁹,

Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”.

¹⁶⁴ zob. art. 13.

¹⁶⁵ Zamieszczoną w art. 31 pkt 2 projektu ustawy.

¹⁶⁶ W art. 18 ust. 1 pkt 4 projektu ustawy projektodawca proponuje bowiem, by warunkiem przekazania danych do państwa trzeciego było gwarantowanie przez to państwo poziomu ochrony danych osobowych takiego, jaki obowiązuje na terytorium państwa członkowskiego Unii Europejskiej, od którego podmiot uprawniony otrzymał informacje, zaś w art. 18 ust. 5 pkt 3 projektu ustawy – w sytuacji, gdy gwarancje powyższe nie mogą być spełnione – takiego poziomu ochrony, jaki obowiązuje na terytorium Rzeczypospolitej Polskiej. Zaproponowane unormowanie byłoby prawidłowe jedynie przy założeniu, że poziom ochrony danych osobowych na terytorium Rzeczypospolitej Polskiej jest niższy niż na terytorium pozostałych państw członkowskich. Natomiast założenie ustawodawcy europejskiego jest odmienne, tj. przewiduje on istnienie podobnego poziomu ochrony danych osobowych we wszystkich państwach członkowskich oraz zakłada jednolite kryteria oceny poziomu ochrony danych w państwie trzecim. Ponadto takie rozwiązanie spowodowałoby konieczność analizy tych gwarancji z punktu widzenia prawa innego państwa członkowskiego, a nie prawa polskiego, co w praktyce organów ścigania byłoby trudne. W konsekwencji, biorąc pod uwagę istniejący w decyzji ramowej 2008/977/WSiSW standard odpowiedniego poziomu ochrony i zakładając, że wszystkie państwa członkowskie Unii Europejskiej go wdrożyły, proponowana dyferencjacja nie jest uzasadniona. Dlatego też, w celu uniknięcia wskazanych sprzeczności, Generalny Inspektor Ochrony Danych Osobowych proponował, aby w tym zakresie odwołać się do zasad określonych w rozdziale 7 ustawy o ochronie danych osobowych (w brzmieniu zaproponowanym w projekcie ustawy). W konsekwencji art. 18 projektu ustawy powinien jedynie zawierać merytoryczne kryteria określone obecnie w art. 18 ust. 1 pkt 1 – 3 i ust. 3 oraz 4, jak również zapewniać, że jednocześnie muszą być spełnione kryteria określone w art. 47 ustawy o ochronie danych osobowych (w brzmieniu zaproponowanym w art. 31 pkt 2 projektu ustawy) i art. 48 ustawy o ochronie danych osobowych. W szczególności art. 18 ust. 5 pkt 3 projektu ustawy powinien być utożsamiony z nowym brzmieniem art. 47 ust. 2 ustawy o ochronie danych osobowych oraz jej art. 48.

¹⁶⁷ Dodawanego przez art. 25 pkt 1 lit. b projektu ustawy – art. 20 ust. 2aa ustawy z dnia 6 kwietnia 1990 r. o Policji, t. j. Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.

¹⁶⁸ Proponowany w art. 20 ust. 2aa ustawy o Policji zakres dopuszczalnej wymiany danych osobowych jest zbyt szeroki, gdyż – w przyjętym brzmieniu – dopuszcza taką wymianę między Policją a wszelkimi organizacjami międzynarodowymi, których statutowa działalność obejmuje zapobieganie lub zwalczanie przestępczości. Takie ujęcie dyspozycji art. 20 ust. 2aa ustawy o Policji nie daje się pogodzić nie tylko z – określonymi w ustawie o ochronie danych osobowych – zasadami ochrony danych osobowych, lecz również z uwarunkowaniami konstytucyjnymi. Przypomnieć należy, że członkostwo Rzeczypospolitej Polskiej w organizacjach międzynarodowych może znajdować oparcie w umowach międzynarodowych zawartych w różnej formie i na różnym szczeblu. Natomiast nie wszystkie z tych umów międzynarodowych mogą stanowić podstawę przekazywania danych osobowych. Wiążąca bowiem polskie podmioty publiczne, w tym niewątpliwie Policję, zasada legalizmu (art. 7 Konstytucji Rzeczypospolitej Polskiej) stanowi, iż przekazywanie przez ten organ danych osobowych innym podmiotom znajdować musi oparcie w przepisach prawa. W przypadku umów międzynarodowych przepisy zawierające upoważnienie do takiego przekazywania zawarte zaś mogą być jedynie w tych umowach międzynarodowych, które podlegają ratyfikacji, gdyż tylko takie umowy międzynarodowe są źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej – art. 87 ust. 1 Konstytucji Rzeczypospolitej Polskiej. Co więcej – w przypadku przetwarzania danych dla potrzeb zapobiegania i zwalczania przestępczości wysoce prawdopodobnym jest, że przedmiotem wymiany będą dane szczególnie chronione w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych

projekt ustawy miał dotyczyć: „wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej”. Tymczasem – zgodnie z przepisem¹⁷⁰ ustawy o Policji – postanowienia projektu ustawy (po jej ewentualnym uchwaleniu) znajdowałyby zastosowanie również w odniesieniu do wymiany informacji z Międzynarodową Organizacją Policji Kryminalnych (Interpol), której to organizacji w żadnym razie nie można uznać za organ ścigania państwa członkowskiego Unii Europejskiej.

Generalny Inspektor zwrócił uwagę, że pomimo uwzględnienia w projekcie ustawy środków zapewniających ochronę praw osób, których dane będą podlegać przetwarzaniu w ramach procedury wymiany informacji – o co wnosił od początku procedury legislacyjnej – zauważyć należy, że występuje w nim istotna niekonsekwencja w zakresie wyłączeń z katalogu przepisów ustawy o ochronie danych osobowych, które mają być stosowane¹⁷¹. Jednocześnie GIODO zauważył, iż wyliczenie przepisów ustawy o ochronie danych osobowych, które stosowane będą przy wymianie informacji¹⁷², skutkuje wyłączeniem obowiązywania w procedurze wymiany informacji przepisów karnych ustawy o ochronie danych osobowych, co – w ocenie organu do spraw ochrony danych osobowych – nie było działaniem zamierzonym przez projektodawcę. Organ do spraw ochrony danych osobowych nie pominął w swej opinii kwestii, iż przy wymianie informacji katalog przepisów ustawy o ochronie danych osobowych powinien być uzupełniony o przepisy wykonawcze wydane na podstawie art. 39 a ustawy o ochronie danych osobowych¹⁷³.

W bieżącym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych opiniował również, procedowany w Komisji Administracji i Spraw Wewnętrznych Sejmu Rzeczypospolitej Polskiej, *rządowy projekt ustawy o zmianie ustawy o dostępie do informacji*

(wprost mówi o tym projektowany art. 20 ust. 2b pkt 1 ustawy o Policji), co implikuje wymaganie, by umowa międzynarodowa dopuszczająca przekazywanie takich danych była umową międzynarodową ratyfikowaną za uprzednią zgodą wyrażoną w ustawie – art. 89 ust. 1 Konstytucji Rzeczypospolitej Polskiej. Powołany wyżej projektowany art. 20 ust. 2aa ustawy o Policji nie uwzględnia w swojej treści powyższych unormowań konstytucyjnych, statuując dopuszczalność przekazania danych osobowych przez Policję każdej organizacji międzynarodowej (której statutowa działalność obejmuje zapobieganie lub zwalczanie przestępczości) i na podstawie postanowień jakiejkolwiek umowy międzynarodowej (nie zaś ratyfikowanej albo ratyfikowanej za uprzednią zgodą wyrażoną w ustawie). Jednocześnie zaś proponowany przepis ustawy o Policji (art. 20 ust. 2aa *in fine*) przewiduje możliwość przekazywania przez Policję danych osobowych organizacjom międzynarodowym na podstawie prawa stanowionego przez te organizacje w sytuacji, gdy nadanie w polskim porządku prawnym mocy wiążącej prawa stanowionego przez organizację międzynarodową wymaga zachowania specjalnego trybu przewidzianego w art. 90 Konstytucji Rzeczypospolitej Polskiej.

¹⁶⁹ zob. także art. 1 ust. 1.

¹⁷⁰ Art. 20 ust. 2aa.

¹⁷¹ W zakresie nieuregulowanym w rozdziale 4 projektu ustawy, projektodawca nakazuje stosować art. 32 ust. 1 pkt 1, 2, 4 i 6 ustawy o ochronie danych osobowych oraz art. 33 ust. 1 i art. 34 te same ustawy, co za tym idzie – świadomie wyłączył z katalogu przepisów, które mają być stosowane, art. 32 ust. 1 pkt 3, 5 i 5a ustawy o ochronie danych osobowych. Tymczasem art. 33 ust. 1 ustawy o ochronie danych osobowych (oraz pośrednio art. 34 ust. 1 te same ustawy) odwołują się w swojej treści do art. 32 ust. 1 pkt 3, 5 i 5a ustawy o ochronie danych osobowych. Biorąc zatem pod uwagę aktualne brzmienie art. 33 ust. 1 ustawy o ochronie danych osobowych Generalny Inspektor poddał w wątpliwość, czy w procedurze wymiany informacji przewidziane w art. 32 ust. 1 pkt 3, 5 i 5a ustawy o ochronie danych osobowych prawa osób, których dane będą podlegać przetwarzaniu, istnieją, czy też są wyłączone.

¹⁷² Zgodnie z art. 26 projektu ustawy, przy wymianie informacji stosowane będą wyłącznie art. 12, art. 14 – 19, art. 26 ust. 1, art. 27 ust. 2 pkt 2, art. 32 ust. 1 pkt 1, 2, 4 i 6, art. 33 ust. 1 i art. 34 – 39 ustawy o ochronie danych osobowych.

¹⁷³ Ustawa o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej - uchwalona w dniu 16 września 2011 r. - została podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 10 października 2011 r., zaś weszła w życie z dniem 1 stycznia 2012 r.

publicznej oraz niektórych innych ustaw, do którego przedstawił obszerne stanowisko, wyrażając wiele istotnych zastrzeżeń do zawartych w nich założeń i konstrukcji prawnych.

Opiniując przedmiotowy projekt w pierwszej kolejności wskazał, iż o ile założenia do przedmiotowej ustawy były konsultowane w 2009 i 2010 roku, a ich kształt został pozytywnie oceniony przez polski organ do spraw ochrony danych osobowych, o tyle w wersji skierowanej pod obrady Sejmu projekt ten zawierał wiele rozwiązań, które nie były ujęte w założeniach i tym samym nie były dotąd poddane opiniowaniu GODO. Zarzut ten dotyczył przede wszystkim przepisów związanych z postulowanym utworzeniem centralnego repozytorium informacji publicznej. Niemniej Generalny Inspektor z zadowoleniem przyjął przygotowanie projektu, który stanowił istotny i ważny wkład w uzupełnianiu luk w systemie prawnym Rzeczypospolitej Polskiej. Organ do spraw ochrony danych osobowych poczynił uwagę, iż pomijając nawet wymagania wynikające z prawa europejskiego – tj. wdrożenie do prawa polskiego zasad dyrektywy Parlamentu Europejskiego i Rady w sprawie ponownego wykorzystania informacji sektora publicznego - brak ogólnej regulacji zasad ponownego wykorzystania informacji publicznej stanowił bardzo poważną przeszkodę w działalności gospodarczej, naukowej i społecznej. Uregulowanie tych kwestii w omawianym projekcie zostało przez Generalnego Inspektora uznane za słuszne i przeprowadzone w bardzo kompleksowy, nowoczesny i otwarty sposób. Stąd też sam duch ustawy, jak i zdecydowana większość proponowanych rozwiązań legislacyjnych, zasłużyło na wsparcie.

Generalny Inspektor przypomniał, iż publiczny charakter informacji wynika z faktu, że dotyczy „spraw publicznych” a nie z tego, że jest ona publicznie dostępna. Tym samym informacją publiczną staje się pewien zasób informacyjny, ze względu na jego treść, a nie ze względu na to, czy został ujawniony publicznie czy nie.

Najbardziej istotną zmianą, jaka pojawi się po wprowadzeniu do polskiego systemu prawnego zasad ponownego wykorzystania informacji publicznej, jest potwierdzenie, że informacja publiczna gromadzona przez podmioty publiczne w ramach i dla celów zgodnych z konstytucyjną zasadą praworządności, będzie w przyszłości przetwarzana dla celów zupełnie innych, nad którymi organy władzy publicznej stracą kontrolę. Generalny Inspektor zwrócił uwagę, że musimy w przyszłości godzić się na to, że nasze dane osobowe w zakresie, w jakim będą stanowiły informację publiczną, będą łączone z innymi danymi stanowiącymi informację publiczną a nie będącymi danymi osobowymi w celu tworzenia profilu osoby fizycznej.

Dokonując kompleksowej analizy przedmiotowego projektu Generalny Inspektor zasugerował, aby w dalszych pracach nad projektem podjąć działania mające wskazane poniżej cele.

Po pierwsze, zrezygnować z tworzenia regulacji prawnej dla centralnego repozytorium informacji publicznej i powrócić do tej idei w odrębnej nowelizacji po rozstrzygnięciu szeregu wskazanych przez niego wątpliwości.

Organ do spraw ochrony danych osobowych w swej opinii za bezdyskusyjne uznał, iż dane zawarte w rejestrach publicznych są informacją publiczną i podlegają zasadom dostępu do informacji publicznej oraz jej ponownego wykorzystywania.¹⁷⁴ Szczególne znaczenie dla polskiego organu ochrony danych ma ponowne wykorzystanie informacji publicznej zawierającej dane osobowe. Dotyczy to np. dostępu do – jawnej formalnie – księgi wieczystej prowadzonej dziś przy pomocy systemów teleinformatycznych, ale już nie do stanowiącej podstawę prawną części wpisów w księdze wieczystej – a nie do końca jawnej formalnie – ewidencji gruntów i budynków. Generalny Inspektor podniósł również jako problematyczną kwestię transparentności informacji w konfrontacji jawności formalnej danych z rejestrów publicznych. Zdaniem Generalnego Inspektora Ochrony Danych osobowych bez zmiany znaczenia pojęcia jawności formalnej lub bez odróżnienia go od „otwartego dostępu do informacji” (dostępności) grozi poważnym naruszeniem zasad ochrony prywatności przyjmowanie, że każdy zasób jawny formalnie powinien być dostępny do dowolnego ponownego wykorzystania. Czyniąc to spostrzeżenie zwrócił uwagę, że bardziej poprawnym byłoby posługiwanie się terminem „jawności danych rejestrowych” lub „jawności danych z rejestru” zamiast „jawności rejestrów”. W większości bowiem przypadków mamy do czynienia nie tyle z jawnością samego rejestru, lecz z jawnością jego odbicia, jakim jest zestaw danych – a co za tym idzie informacji – przetwarzanych w systemie teleinformatycznym, który z założenia nie jest rejestrem samym w sobie. Jednocześnie przywołał stanowisko doktryny prawa w Polsce w zakresie jawności formalnej danych rejestrowych, będącej obecnie podstawą do uznania zasobu rejestrowego lub innego zasobu wchodzącego w zakres informacji publicznej za możliwy do ponownego wykorzystania. Zwrócił uwagę, iż idea jawności formalnej – będąca „kamieniem węgielnym” rejestrów publicznych, nierozzerwalnie związana z fundamentalnymi wartościami ustrojowymi – prowadzi do prawnego zagwarantowania każdemu, bądź określonym osobom, dostępu do rejestru w celu poznania zawartych w nim informacji. W tym znaczeniu formułujemy zasadę „dostępności rejestru” odróżnianą do prawa ponownego. Generalny Inspektor rozważania na temat jawności skonkludował stwierdzeniem, iż rządowy projekt nie rozstrzygał problemu wskazanego przez doktrynę i powodował, że z jednej strony każdy zasób z zasady jawny (w tym np. elektroniczna księga wieczysta) oddany zostaje do ponownego wykorzystania na bardzo otwartych zasadach wynikających z ustawy, z drugiej strony każde – nawet minimalne – ograniczenie jawności formalnej wynikające z przepisów szczególnych traktowane będzie jako powód do odmowy przekazania informacji do ponownego wykorzystania. W kontekście rozważań o wdrożeniu do polskiego prawa idei otwartego rządu (*open government*), Generalny Inspektor wskazał, iż realizacja zasad otwartego rządu powinna obejmować tak administrację rządową, jak

¹⁷⁴ Należy pamiętać, że ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, rejestrem publicznym nazywa: rejestr, ewidencję, wykaz, listę, spis albo inną formę ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych.

i administrację samorządową, Prezydenta RP, Sejm, Senat oraz Sądy i Trybunały. Rządowy projekt nie był w tym zakresie konsekwentny. Choć większość przepisów dotyczących dostępu do informacji publicznej słusznie rozciągnęło prawa i obowiązki na wszystkie organy władzy publicznej (z akceptowalnym na gruncie art. 61 ust. 4 wyjątkiem dla Sejmu i Senatu), o tyle nie przewidywało już tak szerokiego katalogu podmiotowego, jeśli chodzi o prawo do ponownego wykorzystywania informacji publicznych. Nie jest jasne, w jakim zakresie zasady ponownego wykorzystania informacji publicznych odnoszą się do Sejmu i Senatu RP.¹⁷⁵ Przepisy dotyczące obowiązków organów samorządu terytorialnego oraz sądów w zakresie ponownego wykorzystania informacji publicznej powinny być opiniowane – odpowiednio – przez Komisję Wspólną Rządu i Samorządu Terytorialnego oraz Krajową Radę Sądownictwa, natomiast w posiadanym przez GODO materiale brak było informacji o takich konsultacjach. Ponadto Generalny Inspektor wskazał, iż rządowy projekt stanowi podstawę do ponownego wykorzystania informacji publicznej gromadzonych w zasobach infrastruktury informacyjnej państwa, nie wskazuje on w żadnym swym przepisie jaki jest stosunek unormowań ustawy o dostępie do informacji publicznej i jej ponownym wykorzystywaniu do ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej. Dotychczas zasady wynikające z ustawy o infrastrukturze informacji przestrzennej uznawano w dużym stopniu za *legi speciali* wobec ustawy o dostępie do informacji publicznej, jako że zasady dostępu do informacji były w niej szczegółowiej opisane i nie powodowały jawnej kolizji choćby z przepisami o biuletynie informacji publicznej. Niestety takiego rozumowania nie można kontynuować pod rządami ustawy o dostępie do informacji publicznej i jej ponownym wykorzystywaniu, jako że ustawa ta formułuje inne, bardziej otwarte zasady ponownego wykorzystania informacji publicznej, a jednocześnie tworzy „byty” absolutnie niekompatybilne z instytucjami infrastruktury informacji przestrzennej. Jednocześnie omawiany projekt w niektórych przepisach wydaje się wprost ingerować w przepisy o informacji przestrzennej (np. zmiany w zakresie ustawy - Prawo wodne), tym samym przyznając sobie wyższość nad przepisami ustawy o infrastrukturze informacji przestrzennej. Za największy merytoryczny mankament projektu Generalny Inspektor uznał wprowadzenie do ustawy nowego „bytu” jakim jest centralne repozytorium informacji publicznej (CRIP). Ta nowa instytucja wydaje się powielać rozwiązania, jakie w 2001 r. przyjęto dla biuletynu informacji publicznej (BIP). Jedynie trzy elementy odróżniają ideę CRIP od idei BIP: centralny charakter CRIP, konstrukcja CRIP jako zasobu informacyjnego w odróżnieniu od konstrukcji BIP’u jako jednolitego systemu stron w sieci

¹⁷⁵ Trzeba pamiętać, że regulacja z art. 61 ust. 4 Konstytucji dotyczy jedynie dostępu do informacji publicznej, o którego zasadach decyduje regulamin obu izb. Przepis ten natomiast nie przewiduje takiego wyłączenia dla zasad ponownego wykorzystania informacji publicznych. Ustawa powinna tym samym rozstrzygać, czy Sejm i Senat są objęte katalogiem podmiotowych z art. 23a ust. 2, czy też są z tego katalogu wyłączone w związku z respektowaniem zasady autonomii regulacyjnej Sejmu i Senatu.

teleinformatycznej¹⁷⁶, cechy informacji publicznej zamieszczanej w CRIP. Ponadto wątpliwości Generalnego Inspektora wzbudziły: niedookreślony zakres informacji przeznaczonej do umieszczenia w centralnym repozytorium informacji publicznej¹⁷⁷; zakres przedmiotowy obowiązku umieszczania informacji publicznej w CRIP¹⁷⁸, który wydawał się być skonstruowany uznaniowo, a nie obejmował np. organów administracji samorządowej, Sejmu RP, Senatu RP, sądów i trybunałów¹⁷⁹, ale obejmował uczelnie publiczne i Polską Akademię Nauk¹⁸⁰, które – jak wskazane zostało w uzasadnieniu projektu – nie były w tym zakresie konsultowane; wyraz „każdorazowe” w przepisie¹⁸¹ zobowiązującym Prezesa Rady Ministrów do „każdorazowego” określenia w drodze rozporządzenia kwestii w nim określonych, należało uznać jako zbędny, gdyż na mocy tej delegacji wydane powinno zostać jedno rozporządzenie; kwestia „metainformacji” w CRIP¹⁸² a „metadanych” dokumentu elektronicznego - nie wiadomo, czy metainformacje miałyby dotyczyć jakiejś zorganizowanej części informacji (np. całego rejestru publicznego), czy też, co wydawało się znacznie bardziej logiczne (biorąc pod uwagę przewidywane sposoby korzystania z CRIP) każdego dokumentu elektronicznego – oraz w przypadku, jeśli takie metainformacje miałyby dotyczyć każdego dokumentu elektronicznego - ewentualnej niejasności stosunku rozporządzenia wydanego na podstawie ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentu elektronicznego; brak zdefiniowania w prawie polskim pojęcia maszynowy odczyt¹⁸³, który uniemożliwia stwierdzenie, czy Prezes Rady Ministrów wypełni obowiązek wynikający z delegacji ustawowej; kwestia uprawnienia do weryfikacji zasobu informacyjnego, którego – w opinii organu do spraw ochrony danych osobowych – minister właściwy do spraw informatyzacji nie powinien posiadać wobec instytucji takich jak PAN, czy uczelnie publiczne; wyłączenie z zakresu informacji publicznej przeznaczonej do ponownego wykorzystania informacji będącej przedmiotem działalności badawczej uczelni i PAN¹⁸⁴ oraz stwierdzenie, iż informacją publiczną są (*a contrario*) informacje stanowiące przedmiot działalności

¹⁷⁶ W przypadku CRIP trzeba będzie „fizycznie” skopiować zasób i przekazać go ministrowi właściwemu do spraw informatyzacji; nie wystarczy umieszczenie linku do aktualizowanego zasobu wewnętrznego, jak w przypadku BIP.

¹⁷⁷ Sformułowanie zawarte w art. 9a ust. 1 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu: „informacja publiczna o szczególnym znaczeniu dla rozwoju innowacyjności i rozwoju społeczeństwa informatycznego” pozostawia Prezesowi Rady Ministrów duży zakres dyskrecjonalności co do zawartości CRIP. Może to prowadzić do umieszczania w CRIP wszystkiego, co już znajduje się w BIP. Tak duża dyskrecjonalność po stronie Prezesa Rady Ministrów, związana z nakładaniem obowiązków na podmioty niemieszczące się w strukturze administracji rządowej, nie może być realizowana w formie rozporządzenia.

¹⁷⁸ Określony w art. 9a ust. 2 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁷⁹ GIODO zaznaczył, iż takie rozumowanie należy uznać jednak za słuszne, jeśli ten wybiórczy charakter byłby określony z uwzględnieniem finansowych, technicznych i organizacyjnych możliwości stworzenia systemu teleinformatycznego, który będzie służył do obsługi CRIP oraz koniecznością dodatkowych konsultacji z zainteresowanymi podmiotami, gdyby taki obowiązek na nie również miał być rozszerzony.

¹⁸⁰ Przynajmniej w zakresie, o którym mowa w art. 23a ust. 3 pkt 4.

¹⁸¹ Art. 9a ust. 3 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁸² Delegacja do wydania rozporządzenia wynikająca z art. 9a ust.3 przewiduje określenie metainformacji zasobu informacyjnego przekazywanego do CRIP.

¹⁸³ Używane jest tylko w jednym akcie prawnym, tj. w załączniku do rozporządzenia Rady Ministrów z 10 lipca 1995 r. w sprawie określenia wzoru powszechnego świadectwa udziałowego.

¹⁸⁴ Art. 23a ust. 3 pkt 4 ustawy o dostępie do informacji publicznej i ponownym jej wykorzystaniu.

dydaktycznej uczelni¹⁸⁵ – GODO zasugerował, że wskazane byłoby poznać opinię środowiska akademickiego w tym zakresie; termin wejścia w życie przepisów w zakresie dotyczącym CRIP – 12 miesięcy od dnia ogłoszenia – wydaje się nierealny.

Po drugie, Generalny Inspektor zaproponował zmianę przepisów pod kątem uzyskania spójności z unormowaniami ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej, zmianę przepisów dotyczących ograniczenia prawa do ponownego wykorzystania informacji publicznych¹⁸⁶ oraz przepisu statuującego listę podmiotów zobowiązanych do udostępnienia informacji publicznej w celu ponownego wykorzystania na zasadach i w trybie określonych w ustawie¹⁸⁷, która nie wydaje się do końca spójna i jasna¹⁸⁸.

Po trzecie, organ do spraw ochrony danych osobowych zasugerował usunięcie z projektu: przepisów dotyczących CRIP; przepisu przewidującego umieszczenie w CRIP informacji publicznej o szczególnym znaczeniu dla rozwoju innowacyjności i rozwoju społeczeństwa informatycznego¹⁸⁹; przepisu określającego zakres podmiotowy obowiązku umieszczania informacji publicznej w CRIP¹⁹⁰; przepisu zawierającego delegację do wydania rozporządzenia przez Prezesa Rady Ministrów określającego *zasób informacyjny przeznaczony do umieszczenia w centralnym repozytorium, wraz ze wskazaniem podmiotu obowiązującego do jego przekazania oraz harmonogram przekazywania zasobu informacyjnego do centralnego repozytorium oraz wymagania techniczne opracowania tego zasobu*¹⁹¹, przepisu przewidującego delegację do wydania rozporządzenia określającego metainformację zasobu informacyjnego przekazywanego do CRIP¹⁹²; przepisu przewidującego weryfikację dokonywaną przez ministra właściwego do spraw informatyzacji, przekazywanego do CRIP zasobu informacyjnego pod względem spełniania wymogów określonych w przepisach wydanych przez Radę Ministrów¹⁹³; przepisu powielającego obowiązek regulowany już w przepisach ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne¹⁹⁴; przepisu przewidującego obowiązek umieszczenia w menu przedmiotowym strony podmiotowej BIP kategorii ponowne wykorzystanie informacji publicznej i umieszczenia tam wykazu informacji publicznych dostępnych

¹⁸⁵ W kolejnym przepisie wyłączono z zakresu informacji publicznej przekazywanej do ponownego wykorzystania informację będącą przedmiotem działalności edukacyjnej jednostek organizacyjnych systemu oświaty. Jeżeli porównamy oba omawiane przepisy, stanie się jasne, że informacją publiczną przeznaczoną do ponownego wykorzystania są przygotowywane przez pracowników uczelni publicznych podręczniki akademickie.

¹⁸⁶ Art. 5 i 5a ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu - nie wydaje się słuszne, by art. 5 ust.1 zawierał wprost odesłania do art. 5a. Jest bowiem oczywiste, że art. 5a stanowi *lex specialis* wobec art. 5 ust.1. Jednocześnie w art. 5 a posłużono się sformułowaniem „podlega ograniczeniu do czasu” bez wyjaśnienia, na czym polega takie ograniczenie.

¹⁸⁷ Art. 23a ust. 2 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁸⁸ Nie wiadomo dlaczego w pkt 1 wyróżniono Prezesa Rady Ministrów, mimo że w pkt 2 mowa jest o jednostkach sektora finansów publicznych. Nie jest również jasne, czy lista obejmuje podmioty takie jak: Prezydent RP, Sejm RP i Senat RP.

¹⁸⁹ Art. 9a ust. 1 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁹⁰ Art. 9a ust. 2 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁹¹ Art. 9a ust. 3 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁹² Art. 9a ust. 2 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁹³ Art. 9b ust. 2 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁹⁴ Art. 23f ust. 1 ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

w BIP w celu ponownego wykorzystywania¹⁹⁵; zmian wprowadzanych do ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej¹⁹⁶, ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej¹⁹⁷ oraz ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne¹⁹⁸, które mogą sugerować, iż dostępne do ponownego wykorzystania są tylko te rejestry publiczne, w których szczegółowej regulacji ustawowej dopuszczono ponowne wykorzystanie.

Po czwarte, Generalny Inspektor podniósł, iż zasadnym byłoby przeprowadzenie niezbędnych konsultacji, w szczególności z Krajową Radą Sądownictwa oraz z Konferencją Rektorów Akademickich Szkół Polskich z powodów, o których mowa powyżej, a także z uwagi na jedną z najważniejszych i najbardziej oczekiwanych w omawianej ustawie zmian przepisów ustawy o dostępie do informacji publicznej¹⁹⁹, likwidującą odrębności w postępowaniu sądowym, która jednak – jak wynika z uzasadnienia projektu – nie była konsultowana z Krajową Radą Sądownictwa, co mogłoby stać się przyczyną jej uznania za niekonstytucyjną z powodu uchybienia formalnego.

Ustawa z dnia 16 września 2011 r. o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw, podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 24 września 2011 r., została ogłoszona w Dzienniku Ustaw z dnia 28 września 2011 r. Nr 204, poz. 1195. Weszła ona w życie po upływie 3 miesięcy od dnia ogłoszenia, tj. z dniem 29 grudnia 2011 r. z wyjątkiem art. 1 pkt 5-7 i 10 w zakresie dotyczącym centralnego repozytorium informacji publicznej, które wchodzi w życie po upływie 12 miesięcy od dnia ogłoszenia, tj. 29 września 2012 r. Prezydent po ogłoszeniu tej ustawy w Dzienniku Ustaw zapowiedział, iż wystąpi do Trybunału Konstytucyjnego w trybie kontroli następcej o zbadanie zgodności z Konstytucją RP w zakresie dotyczącym poprawki Senatu wprowadzającej ograniczenie prawa do informacji publicznej.

Opiniując z kolei w minionym okresie sprawozdawczym 2010 roku projekt *ustawy o systemie informacji w ochronie zdrowia*²⁰⁰, na etapie procedowania go przez Parlament, GIODO pozostawał w sporze z autorami projektu w przedmiocie rozwiązań istotnych z punktu widzenia zasad przetwarzania danych osobowych szczególnie chronionych i działał celem zmiany rozwiązań zaakceptowanych przez Sejm. I tak, Generalny Inspektor poinformował Przewodniczącą Sejmowej Komisji Zdrowia oraz Rzecznika Praw Obywatelskich o tym, że w przyjętym przez Podkomisję nadzwyczajną sprawozdaniu dotyczącym rządowego projektu *ustawy o systemie informacji w ochronie zdrowia* nie uwzględniono szeregu zgłoszonych przez niego, istotnych zastrzeżeń.

¹⁹⁵ Art. 23h ust. 1 pkt ustawy o dostępie do informacji publicznej i jej ponownym wykorzystaniu.

¹⁹⁶ Zmiana polegająca na dodaniu art. 49a w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej.

¹⁹⁷ Zmiana polegająca na dodaniu nowego ust. 2 i 8 do art. 39 w ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej.

¹⁹⁸ Zmiana polegająca na dodaniu nowego ust. 4 do art. 15 w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

¹⁹⁹ Zmiana dotycząca art. 21 (zmiana brzmienia) oraz art. 22 (skreślenie).

²⁰⁰ DOLiS-033-338/10

Generalny Inspektor zauważył, iż w toku prac legislacyjnych prowadzonych przez Podkomisję nadzwyczajną jego głos był ignorowany. Skutkowało to przyjęciem przez Podkomisję nadzwyczajną projektu o takiej treści, która pozostaje w sprzeczności z – określonymi przez ustawę o ochronie danych – podstawowymi zasadami ochrony szczególnie chronionych danych o stanie zdrowia²⁰¹.

Generalny Inspektor brał aktywny udział w pracach Komisji Zdrowia dotyczących tego projektu i zgłaszał propozycje zmian zmierzających do zapewnienia jego zgodności z przepisami o ochronie danych osobowych. GODO zastrzegł sobie jednocześnie prawo do poinformowania innych organów państwa, jak również organizacji pozarządowych, o swoich zastrzeżeniach wobec projektu, podkreślając jednocześnie, że nie neguje samej potrzeby tworzenia zintegrowanego systemu teleinformatycznego służącego zarządzaniu w ochronie zdrowia.

Generalny Inspektor przedstawił pełne stanowisko wobec komentowanego projektu w związku z zaplanowanym na posiedzenie Sejmu RP rozpatrzeniem sprawozdania Komisji Zdrowia z prac nad tym dokumentem²⁰². GODO poinformował Marszałka Sejmu, że w trakcie obrad Komisji nie zdołano uwzględnić istotnych zastrzeżeń do przedmiotowego projektu ustawy, dlatego też postanowił przekazać swoje stanowisko pisemnie, podsumowując najpoważniejsze zarzuty wobec procedowanego projektu.

W 2011 r. GODO aktywnie uczestniczył w dalszych pracach nad tym projektem. W związku z przedstawieniem Generalnemu Inspektorowi Ochrony Danych Osobowych propozycji zmian – przyjętego przez Sejm Rzeczypospolitej Polskiej w dniu 25 marca 2011 r. – projektu *ustawy o systemie informacji w ochronie zdrowia*, zaprezentowane rozwiązania zyskały akceptację organu do spraw ochrony danych osobowych. GODO nie pominął jednak, iż propozycje te stanowią odpowiedź na szereg zastrzeżeń zgłaszanych dotychczas przez Generalnego Inspektora Ochrony Danych Osobowych, a więc mogą być potraktowane jako dopuszczalny kompromis pomiędzy oczekiwaniami organu do spraw ochrony danych osobowych z jednej strony a możliwościami resortu zdrowia z drugiej²⁰³.

²⁰¹ By zarzut ten nie mógł być uznany za gołosłowny, Generalny Inspektor wskazał przykład dyspozycji art. 20 w zw. z art. 19 ust. 1 projektu, które to przepisy – wbrew jednoznaczному brzmieniu art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych i – prawdopodobnie – niezgodnie z art. 51 ust. 1 oraz art. 92 ust. 1 Konstytucji Rzeczypospolitej Polskiej – przyznają ministrowi właściwemu do spraw zdrowia kompetencję do tworzenia i prowadzenia (lub tworzenia i zlecania prowadzenia) w drodze rozporządzenia, rejestrów medycznych zawierających zindywidualizowane dane o stanie zdrowia.

²⁰² Pismo z dn. 16 marca 2011 r. znak: 11535/11.

²⁰³ W pierwszej kolejności za odpowiadające stanowisku Generalnego Inspektora Ochrony Danych Osobowych uznać należy zaproponowane brzmienie art. 19 ust. 6b projektu. Przepis ten wychodzi bowiem naprzeciw, artykułowanemu przez organ do spraw ochrony danych osobowych w toku prac legislacyjnych stanowisku, zgodnie z którym osoby, których dane mają być przetwarzane w rejestrach medycznych, winny mieć zapewnioną realną możliwość zgłoszenia sprzeciwu, o którym mowa w art. 19 ust. 4 projektu. Doceniając zatem uwzględnienie zastrzeżeń organu do spraw ochrony danych osobowych, w opinii Generalnego Inspektora Ochrony Danych Osobowych zaproponowana regulacja wymaga jeszcze uzupełnienia. Po pierwsze – w art. 19 ust. 6b projektu brak jest wskazania, kiedy ma być dopełniony obowiązek informacyjny wobec osób, których dane mają być przetwarzane w rejestrach medycznych. Po drugie zaś – zachodzi potrzeba unormowania kwestii spełnienia obowiązku informacyjnego wobec tych osób, których dane już są przetwarzane w rejestrach medycznych, których to prowadzenie będzie kontynuowane po przeprowadzeniu przez ministra właściwego do spraw zdrowia *sui generis* postępowania konwalidacyjnego, o którym mowa w art. 53 projektu. To drugie zagadnienie mogłoby być uregulowane w przepisach przejściowych projektu.

Nie negując samej zasady prowadzenia rejestrów medycznych, Generalny Inspektor Ochrony Danych Osobowych wskazał, iż oczekuje ze strony projektodawców jasnej deklaracji, że ich zamiarem nie jest łączenie danych osobowych zawartych w poszczególnych rejestrach medycznych, co w konsekwencji mogłoby prowadzić do niedozwolonego profilowania osób i dlatego też wniósł o jednoznaczne rozstrzygnięcie tej wątpliwości w trakcie procedowania projektu przez Senat Rzeczypospolitej Polskiej. Jednakże biorąc pod uwagę, iż w dalszym ciągu minister właściwy do spraw zdrowia jest uprawniony do zlecania prowadzenia rejestrów medycznych²⁰⁴, w ocenie Generalnego Inspektora zachodzi konieczność szczegółowego doprecyzowania w projekcie kategorii podmiotów, którym takie zlecenie może być udzielone. Brak jednoznacznego uregulowania tej kwestii wzbudził wątpliwości co do zgodności projektu w tej części z ustawą o ochronie danych osobowych, jak również obawę, że powstanie niebezpieczeństwo utraty przez ministra właściwego do spraw zdrowia - jako administratora danych - kontroli nad danymi osobowymi zawartymi w tych rejestrach medycznych, których prowadzenie będzie zlecone.²⁰⁵

Niezwykle istotnym projektem, co do którego wypowiadał się Generalny Inspektor pod kątem zgodności z przepisami o ochronie danych osobowych, były projekty – poselski (PiS)²⁰⁶ – *ustawy o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw* i rządowy²⁰⁷ – *ustawy o zapewnieniu bezpieczeństwa w związku z organizacją turnieju finałowego UEFA EURO 2012 oraz o zmianie ustawy Kodeks karny, ustawy Kodeks postępowania karnego, ustawy Kodeks karny wykonawczy oraz niektórych innych ustaw*.

Opiniując projekt *ustawy o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw* Generalny Inspektor podniósł, iż dokonanie oceny pod kątem zgodności z przepisami ustawy o ochronie danych osobowych przedłożonego poselskiego projektu, było istotnie utrudnione ze względu na zastosowaną w nim terminologię. Zarówno brak stosownych definicji w projekcie ustawy nowelizującej, jak i pominięcie tych kwestii w – nader lakonicznym – uzasadnieniu, nie pozwoliły Generalnemu Inspektorowi Ochrony Danych Osobowych na poczynienie ustaleń, co do sposobu rozumienia przez projektodawcę użytych pojęć („przebieg pobytu [kibica] na stadionie klubu sportowego”²⁰⁸ i „dane osobopoznawcze [...] kibica”²⁰⁹). Nie znając przy tym zakresu informacji, które – zgodnie z założeniem projektodawcy – mają być zbierane dla „dokumentowania

²⁰⁴ zob. niezmieniony art. 19 ust. 1 projektu.

²⁰⁵ Ustawa ta została ogłoszona w Dzienniku Ustaw z dnia 2 czerwca 2011, Nr 113, poz. 657 jako ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia i weszła w życie z dniem 1 stycznia 2012 r., z wyjątkiem art. 7 ust. 1 pkt 3 i 4, art. 11 oraz art. 50 pkt 1, które wejdą w życie z dniem 1 sierpnia 2014 r.

²⁰⁶ DOLiS-033-174/11

²⁰⁷ DOLiS-033-83/11

²⁰⁸ Dodawany przez art. 1 pkt 2 projektu ustawy nowelizującej art. 16a ust. 1 pkt 1 oraz ust. 3 zdanie pierwsze ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, Dz. U. Nr 62, poz. 504 z późn. zm.

²⁰⁹ Dodawany przez art. 1 pkt 2 projektu ustawy nowelizującej art. 16a ust. 3 zdanie pierwsze ustawy o bezpieczeństwie imprez masowych.

przebiegu pobytu kibica na stadionie klubu sportowego” oraz mają składać się na „dane osobopoznawcze kibica”, organ do spraw ochrony danych osobowych nie był władny stwierdzić, czy zakres tych danych będzie adekwatny w stosunku do celu ich zbierania²¹⁰. W tym stanie rzeczy Generalny Inspektor Ochrony Danych Osobowych ograniczył się do zasygnalizowania wskazanych wyżej wątpliwości terminologicznych.

Generalny Inspektor podkreślił przy tym, że zasady określone w ustawie o ochronie danych osobowych nakładają na autorów projektu powinność niebudzącego wątpliwości sformułowania przepisów nowelizowanego aktu dotyczących zakresu przetwarzanych danych. Co za tym idzie GODO wskazał, że w projekcie ustawy nowelizującej powinien zostać określony w sposób jednoznaczny katalog danych osobowych podlegających zamieszczeniu w elektronicznym rejestrze kibiców²¹¹ oraz zapisany na elektronicznej karcie kibica²¹², przy czym zbiór danych osobowych przetwarzanych na potrzeby elektronicznego rejestru kibiców i elektronicznej karty kibica musi być zbiorem zamkniętym²¹³.

Następnie Generalny Inspektor wskazał, że względem zasady adekwatności przetwarzanych danych w stosunku do celów ich przetwarzania, przemawia za doprecyzowaniem dyspozycji przepisu²¹⁴, który przewiduje zamieszczanie we wniosku o zezwolenie na używanie podczas sportowej imprezy masowej rac oświetleniowych i flar sygnalizacyjnych, danych osobowych wnioskodawcy oraz wskazanie w tym wniosku osób pełnoletnich, które będą odpowiedzialne za zabezpieczenie, wniesienie na teren stadionu oraz użycie materiałów pirotechnicznych - nie normuje wszakże, jakie konkretnie dane osobowe będą zawarte w przedmiotowym wniosku. W opinii GODO takie ujęcie proponowanego przepisu ustawy o bezpieczeństwie imprez masowych, prowadzić może do przetwarzania dowolnych danych wskazanych wyżej osób.

Za co najmniej kontrowersyjną, z punktu widzenia ochrony danych osobowych, Generalny Inspektor uznał również propozycję²¹⁵, zgodnie z którą każda organizacja kibicowska jest zobligowana do przekazywania wszystkim klubom sportowym rejestru swoich członków²¹⁶. GODO postawił pytanie, czy tak daleko posunięty obowiązek udostępniania danych osobowych nie łamie praw osób

²¹⁰ Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

²¹¹ Dodawany przez art. 1 pkt 2 projektu ustawy nowelizującej art. 16a ust. 1 pkt 1 ustawy o bezpieczeństwie imprez masowych.

²¹² Dodawany przez art. 1 pkt 2 projektu ustawy nowelizującej art. 16a ust. 3 zdanie pierwsze ustawy o bezpieczeństwie imprez masowych.

²¹³ Z uwagi na dyspozycję art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych, projekt ustawy nowelizującej powinien również zawierać unormowania odnośnie okresu przechowywania przez klub sportowy danych w elektronicznym rejestrze kibiców (podobne zagadnienie zostało już uregulowane w art. 13 ust. 5 ustawy o bezpieczeństwie imprez masowych).

²¹⁴ Dodawanego przez art. 1 pkt 7 projektu ustawy nowelizującej – art. 65a ust. 3 ustawy o bezpieczeństwie imprez masowych.

²¹⁵ Zawartą w dodawanym przez art. 1 pkt 1 projektu ustawy nowelizującej art. 3 pkt 9a ustawy o bezpieczeństwie imprez masowych.

²¹⁶ Projektowany art. 3 pkt 9a lit. c ustawy o bezpieczeństwie imprez masowych.

zrzeszonych w organizacjach kibicowskich, jak również – czy nie będzie prowadził do zbierania przez kluby sportowe danych osobowych zbędnych i w nadmiernym rozmiarze.

Do projektu *ustawy o zapewnieniu bezpieczeństwa w związku z organizacją Turnieju Finałowego UEFA EURO 2012 oraz o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks wykroczeń oraz niektórych innych ustaw*, Generalny Inspektor zgłosił natomiast kilka istotnych uwag.

W pierwszej kolejności GODO uznał, że zawarte w przepisie art. 3 projektu ustawy o bezpieczeństwie EURO 2012 regulacje dotyczące zasad przetwarzania przez Policję informacji²¹⁷ w związku z organizacją Turnieju Finałowego UEFA EURO 2012, w większości stanowią powtórzenie unormowań już zamieszczonych w ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.). Powstało zatem pytanie o celowość dublowania w ustawie szczególnej, a takim aktem prawnym (w wypadku uchwalenia) będzie przedmiotowa ustawa, uregulowań istniejących w ustawie statuującej kompetencje Policji.

GODO wskazał, iż w projekcie ustawy o bezpieczeństwie EURO 2012 r. zaproponowano przepis²¹⁸, który nie zawiera w rzeczywistości jakichkolwiek treści merytorycznych, gdyż odsyła do zasad i trybu wymiany informacji (danych osobowych) określonych w bliżej niesprecyzowanych „odrębnych przepisach”.

Marginesowo Generalny Inspektor zauważył, iż nadanie Policji²¹⁹ kompetencji do przetwarzania informacji (danych osobowych) o osobach mogących stwarzać lub stwarzających zagrożenie dla bezpieczeństwa i porządku publicznego poza granicami Rzeczypospolitej Polskiej (jeżeli istnieje uzasadnione przypuszczenie, że osoby te będą przebywać na terytorium Rzeczypospolitej Polskiej) może stanowić wkroczenie w zakres uprawnień Agencji Wywiadu²²⁰, co nie wydaje się rozwiązaniem prawidłowym.

Zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych wzbudziła przede wszystkim konstrukcja²²¹ tzw. police screening, to jest dokonywania przez Policję, na wniosek upoważnionego organu UEFA, sprawdzeń osób ubiegających się o akredytację UEFA. Z uzasadnienia projektu ustawy o bezpieczeństwie EURO 2012²²² nie wynika w ogóle cel wprowadzenia tej instytucji prawnej, cel ten zaś jawi się organowi do spraw ochrony danych osobowych jako wysoce wątpliwy, choćby w świetle dyspozycji jednego z przepisów projektu ustawy o bezpieczeństwie EURO 2012²²³, który deklaruje niewiążący charakter opinii Policji dla organu UEFA decydującego o wydaniu

²¹⁷ W tym danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

²¹⁸ Art. 3 ust. 1 pkt 3 projektu ustawy o bezpieczeństwie EURO 2012.

²¹⁹ Art. 3 ust. 1 pkt 1 *in fine* projektu ustawy o bezpieczeństwie EURO 2012.

²²⁰ Określonych w art. 6 ust. 1 pkt 1 i 2 w zw. z ust. 2 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.

²²¹ Przewidziana w art. 6 projektu ustawy o bezpieczeństwie EURO 2012.

²²² zob. s. 24 uzasadnienia.

²²³ Art. 6 ust. 4 *in principio* projektu ustawy o bezpieczeństwie EURO 2012.

akredytacji UEFA. Jednocześnie zaś zakwestionował samo wprowadzenie do projektu ustawy o bezpieczeństwie EURO 2012 konstrukcji prawnej, która przewiduje zbieranie przez organ państwowy (Policję) informacji, w tym danych osobowych, bez wiedzy i zgody osób, których te dane dotyczą, celem ich przekazania podmiotowi prywatnemu (UEFA). Takie przetwarzanie danych może – w ocenie Generalnego Inspektora Ochrony Danych Osobowych – naruszać prawa i wolności osób, których dane będą w ten sposób przetwarzane. Jednocześnie nie sposób było pominąć milczeniem GODO faktu, iż zaproponowane brzmienie komentowanego przepisu kreuje – nieznanie współczesnemu polskiemu porządkowi prawnemu – postępowanie o charakterze arbitralnym. Opinia wydawana przez Policję w trybie określonym w tymże przepisie ma bowiem opierać się na informacjach zgromadzonych przez ten organ i niedostępnych dla osoby, która ma być podmiotem takiej opinii, nie będzie wymagać i nie będzie podlegać zaskarżeniu. Takie ujęcie kwestionowanego przepisu wzbudziło zasadnicze wątpliwości, co do zgodności z konstytucyjnymi prawami człowieka i obywatela²²⁴, jak również ratyfikowanymi przez Rzeczpospolitą Polską międzynarodowymi paktami praw człowieka.

W przepisach zmieniających projekt ustawy o bezpieczeństwie EURO 2012, w części obejmującej zmiany do ustawy o bezpieczeństwie imprez masowych²²⁵, poważne zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych wzbudziła regulacja dotycząca prowadzenia przez związek sportowy o zasięgu ogólnokrajowym w sprawach piłki nożnej, czyli Polski Związek Piłki Nożnej (PZPN), bazy danych „uczestników meczów piłki nożnej”²²⁶. Nie negując bowiem samej potrzeby powstania takiej bazy, co nie mieści się w zakresie właściwości organu do spraw ochrony danych osobowych, wskazać należało na zasadniczą wadliwość zaproponowanych unormowań z punktu widzenia ustawy o ochronie danych osobowych.

Po pierwsze – w kwestionowanych przepisach brak było wskazania celu prowadzenia przedmiotowej bazy, co stanowi naruszenie art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych, jak również uniemożliwia Generalnemu Inspektorowi dokonanie prawidłowej oceny, czy zakres danych osobowych mających podlegać przetwarzaniu spełnia kryterium adekwatności. Po drugie – wbrew jednoznaczному brzmieniu art. 26 ust. 1 pkt 4 ww. ustawy, w dodawanym przepisie ustawy o bezpieczeństwie imprez masowych nie wskazano okresu przechowywania danych osobowych w bazie danych prowadzonej przez PZPN. Po trzecie – w zakresie gromadzenia w przedmiotowej bazie danych informacji o zakazach wstępu na imprezę masową, o których mowa w art. 65 ustawy o bezpieczeństwie imprez masowych – zakazy wstępu na imprezę masową orzeczone jako środek

²²⁴ W szczególności art. 31 ust. 3, art. 41 ust. 1 i art. 45 ust. 1 Konstytucji Rzeczypospolitej Polskiej.

²²⁵ Ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, Dz. U. Nr 62, poz. 504 z późn. zm. (art. 25 projektu ustawy o bezpieczeństwie EURO 2012).

²²⁶ Art. 13 ust. 6 i 7 ustawy o bezpieczeństwie imprez masowych, dodany przez art. 25 pkt 5 projektu ustawy o bezpieczeństwie EURO 2012.

karny w razie ukarania za wykroczenie, baza danych prowadzona przez PZPN będzie dublować bazę danych prowadzoną przez Komendanta Głównego Policji na podstawie ustawy o bezpieczeństwie imprez masowych²²⁷, co stanowi zbędną redundancję danych.

Oprócz powyższych uwag o charakterze podstawowym, Generalny Inspektor zakwestionował także proponowane brzmienie przepisu *ustawy o bezpieczeństwie imprez masowych*, gdyż posłużono się w nim niejednoznacznym pojęciem kibica związanego z klubem (piłkarskim), a nie wskazano, o jaki charakter lub stopień więzi chodzi. Tym samym zakres przedmiotowej regulacji, a więc również – zakres przetwarzanych danych, stał się niejasny. Brak niezbędnej precyzji GODO zarzucić musiał też proponowanemu przepisowi ustawy o bezpieczeństwie imprez masowych²²⁸, w którym mowa jest o gromadzeniu w bazie danych prowadzonej przez PZPN innych informacji (aniżeli wymienione w art. 13 ust. 6 pkt 1 – 5 ustawy o bezpieczeństwie imprez masowych), w tym danych osobowych, a jednocześnie zakłada się anonimizację przedmiotowych informacji w stopniu uniemożliwiającym zidentyfikowanie osoby, której dotyczą. Uwzględniając definicję danych osobowych, takie ujęcie dyspozycji przepisu nazwać należało nielogicznym, albowiem warunkiem *sine qua non* uznania danego zestawu informacji o osobie fizycznej za dane osobowe tej osoby jest możliwość jej zidentyfikowania w oparciu o ten zestaw informacji.

Podkomisja nadzwyczajna do rozpatrzenia tych projektów podjęła decyzję, iż będą one rozpatrywane wspólnie, przy czym rządowy projekt będzie miał charakter wiodący. Po tym połączeniu projekt zyskał nazwę projektu *ustawy o zmianie ustawy o bezpieczeństwie imprez masowych oraz o zmianie niektórych innych ustaw*, a kwestia zapewnienia bezpieczeństwa w związku z organizacją Turnieju Finałowego UEFA EURO 2012 stała się jednym z rozdziałów nowego projektu.

Opiniując przedmiotowy projekt Generalny Inspektor podniósł, iż przedstawione w nim rozwiązania w sposób istotny wyeliminowały jego dotychczasowe zastrzeżenia zgłaszane w odniesieniu do tworzenia Centralnego Systemu Identyfikacji. Przyjęcie zaproponowanych zmian GODO ocenił jako korzystne z punktu widzenia zapewnienia zgodności przepisów ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 z późn. zm.) z zasadami ochrony danych osobowych. Niemniej jednak, mimo iż kwestia przetwarzania danych w Centralnym Systemie Identyfikacji zyskała regulację ustawową – zgodnie z postulatem GODO – analiza projektowanych unormowań nasunęła pewne dodatkowe wątpliwości. I tak, organ do spraw ochrony danych osobowych podniósł, iż najlepszym rozwiązaniem z punktu widzenia bezpieczeństwa danych byłoby nadanie Komendantowi Głównemu Policji statusu administratora prowadzącego zbiór danych zgromadzonych w Centralnym Systemie Identyfikacji. Jeśli pozostawiona byłaby jednak dotychczasowa propozycja polegająca na ustanowieniu administratorem „właściwego polskiego

²²⁷ Art. 37 pkt 2 i art. 40 pkt 2 (w szczególności lit. g).

²²⁸ Art. 13 ust. 6 pkt 6.

związku sportowego” (to jest PZPN-u), to należałoby doprecyzować²²⁹, iż podmiot ten jest administratorem prowadzonego zbioru danych zgromadzonych w Centralnym Systemie Identyfikacji.

Ponadto Generalny Inspektor - odnosząc się do nowszej z przedstawionych przez Ministerstwo Spraw Wewnętrznych i Administracji koncepcji funkcjonowania Centralnego Systemu Identyfikacji - poddał w wątpliwość realność zapisu dotyczącego okresu przechowywania danych w tym systemie, a stanowiącego, że dane są w nim zamieszczane przez okres dwóch lat od upływu ważności elektronicznego identyfikatora. Przy braku informacji o elektronicznym identyfikatorze w systemie powstało pytanie, w jaki sposób liczony będzie ten dwuletni okres dopuszczalnego przechowywania danych osobowych kibica; co więcej – jak obliczyć okres legalnej retencji danych kibica biorąc pod uwagę, iż może on posiadać kilka identyfikatorów o różnych okresach ważności. Wydawanie elektronicznych identyfikatorów w dalszym ciągu pozostaje przedmiotem indywidualnych uzgodnień pomiędzy osobą zainteresowaną (kibicem) a podmiotem wydającym (co do zasady – klubem piłkarskim lub podmiotem działającym na zlecenie takiego klubu).

GIODO ponownie zakwestionował – poddawaną w wątpliwość we wcześniejszych opiniach do projektu *ustawy o zmianie ustawy o bezpieczeństwie imprez masowych oraz o zmianie niektórych innych ustaw, a także o zapewnieniu bezpieczeństwa w związku z organizacją Turnieju Finałowego UEFA EURO 2012* - konstrukcję tzw. police screening, określoną w art. 14 projektu.

Wskutek przekazania do Biura GODO ostatecznej propozycji Ministerstwa Spraw Wewnętrznych i Administracji poprawek do projektu, Generalny Inspektor odniósł się do elektronicznych identyfikatorów (zwanych dotychczas również kartami kibica), których charakter uległ zasadniczej zmianie w przedstawionych rozwiązaniach. Wskazał, że o ile w aktualnym stanie prawnym elektroniczny identyfikator (karta kibica) jest *sui generis* legitymacją członkowską uprawniającą do zakupu biletu i wejścia na mecz rozgrywany przez określony klub piłkarski (który to lub w którego imieniu karta ta została wydana), to w świetle projektowanych unormowań elektroniczny identyfikator (karta kibica) staje się znakiem legitymizującym, którego posiadanie warunkuje zakupienie jakiegokolwiek biletu i wejście na jakikolwiek mecz piłkarski rozgrywany w Rzeczypospolitej Polskiej.²³⁰ Nie można zaś pominąć – co wskazywano uprzednio - że w myśl proponowanych przepisów ustawy o bezpieczeństwie imprez masowych, wydawanie elektronicznych identyfikatorów ma pozostać przedmiotem indywidualnych uzgodnień między osobą zainteresowaną (kibicem) a podmiotem wydającym (co do zasady – klubem piłkarskim lub podmiotem działającym na zlecenie

²²⁹ Projektowany art. 13 ust. 8 ustawy o bezpieczeństwie imprez masowych.

²³⁰ Na taki charakter elektronicznego identyfikatora wskazuje wprost (projektowany) art. 13 ust. 2c ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 z późn. zm.), zakazujący wydawania osobie zainteresowanej (kibicowi) więcej niż jednego elektronicznego identyfikatora w tym samym czasie oraz (proponowany) art. 13 ust. 9 pkt 1 w zw. z art. 13 ust. 4 tejże ustawy uzależniający przetwarzanie danych kibica w Centralnym Systemie Identyfikacji (a tym samym – dopuszczenie go do udziału w meczu piłki nożnej) od posiadania przez niego ważnego identyfikatora.

takiego klubu). Tak więc warunki, które trzeba spełnić, aby taki identyfikator otrzymać, przesłanki jego pozbawienia oraz okres ważności regulować ma umowa między osobą zainteresowaną a podmiotem wydającym oraz wewnętrzny regulamin uchwalany przez klub piłkarski (organizatora meczu piłki nożnej). GODO zakwestionował, że podmiot wydający elektroniczny identyfikator nie będzie w tym zakresie związany żadnymi przepisami rangi ustawowej i może podejmować swoje decyzje w sposób arbitralny. Co więcej – z przyczyn komercyjnych lub marketingowych może uzależnić wydanie elektronicznego identyfikatora od wyrażenia przez osobę zainteresowaną zgody na świadczenie jej usług dodatkowych przez partnera handlowego podmiotu wydającego (np. bank, firmę ubezpieczeniową, agencję reklamową). Skoro zaś posiadanie ważnego elektronicznego identyfikatora jest warunkiem *sine qua non* udziału konkretnej osoby w jakimkolwiek widowisku piłkarskim na terytorium Rzeczypospolitej Polskiej, czyli wpływa na zakres wolności takiej osoby, to GODO poddał w wątpliwość, przywołując normy zawarte w Konstytucji Rzeczypospolitej Polskiej, czy dopuszczalne jest takie uzależnienie osoby fizycznej od arbitralnej decyzji podmiotu prawa prywatnego, jak również – czy prawo może sankcjonować taki stopień władztwa podmiotu prywatnego (w tym przypadku – klubu piłkarskiego) nad obywatelem.

Generalny Inspektor dostrzegł jednak starania, jakie podjęło Ministerstwo Spraw Wewnętrznych i Administracji dla zapewnienia zgodności projektu przedmiotowej ustawy z – określonymi w ustawie o ochronie danych osobowych – zasadami ochrony tych danych. GODO nadmienił, iż dla uzyskania jak najpełniejszej zgodności – przedstawiona w ostatecznym stanowisku MSWiA koncepcja funkcjonowania Centralnego Systemu Identyfikacji powinna zostać jeszcze uzupełniona o regulacje ustawowe dotyczące zasad wydawania, pozbawiania i obowiązywania (np. okres ważności; ewentualne usługi dodatkowe) elektronicznych identyfikatorów²³¹.

W toku prac nad opiniowaniem projektów aktów prawnych, Generalny Inspektor przedstawił istotne uwagi w związku z dokumentem *Projekt założeń projektu ustawy o niektórych sposobach unikania konfliktu interesów*²³². Generalny Inspektor zmuszony był stwierdzić, że projekt ten zawierał propozycje unormowań pozostających w oczywistej sprzeczności z gwarantowanymi przez Konstytucję Rzeczypospolitej Polskiej prawami, jak prawem do ochrony życia prywatnego i rodzinnego²³³ i prawem do ochrony danych osobowych²³⁴. Bezprecedensowa skala obowiązków i ograniczeń, których nałożenie na obywateli proponuje się w przedmiotowym projekcie założeń, zrodziła u Generalnego Inspektora uzasadnione wątpliwości, czy projektowane regulacje –

²³¹ Ustawa ta podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 20 września 2011 r., ogłoszona w Dz. U. z dnia 12 października 2011 r. Nr 217, poz.1280 jako ustawa z dnia 31 sierpnia 2011 r. o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw, weszła w życie po upływie 30 dni od ogłoszenia, tj. z dniem 12 listopada 2011 r., z wyjątkiem art. 1 pkt 1-5, 7-16, 18 i 20-26, które weszły w życie po upływie 3 miesięcy od dnia ogłoszenia oraz z wyjątkiem art. 1 pkt 17, 19, 27 i 28, art. 5 pkt 1, 2, 4 i 5, art. 7 i art. 10, które weszły w życie z dniem 1 stycznia 2012 r.

²³² DOLiS-033-155/11

²³³ Art. 47 Konstytucji Rzeczypospolitej Polskiej.

²³⁴ Art. 51 Konstytucji Rzeczypospolitej Polskiej.

w przypadku ich uchwalenia – nie naruszałyby zasady proporcjonalności wyrażonej w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.

Już wstępna analiza projektu założeń doprowadziła Generalnego Inspektora do konstatacji, że krąg podmiotów, których dotknąć mają daleko idące ograniczenia sfery prywatności i wolności jest niesłychanie szeroki. O ile bowiem dotychczasowe przepisy antykorupcyjne²³⁵ wiązały możliwość istotnego ograniczenia praw osoby z faktem posiadania przez tę osobę określonego władztwa decyzyjnego, czyli kompetencji do samodzielnego decydowania o sytuacji prawnej lub faktycznej innych podmiotów albo chociaż istotnego wpływania na tę sytuację, to przedstawiony projekt założeń odnosił się, a więc zakładał nałożenie ograniczeń, wobec 59 kategorii podmiotów. Co więcej – w zakresie stopnia wkroczenia w sferę praw i wolności traktuje w sposób właściwie równorzędny osoby pozostające na krańcowo różnych stopniach hierarchii administracyjnej, czyli posiadające zasadniczo różny zakres uprawnień decyzyjnych²³⁶. Zrodziło to u Generalnego Inspektora pytanie o zgodność proponowanych unormowań z zasadą równego traktowania osób znajdujących się w podobnej sytuacji prawnej proklamowaną w art. 32 Konstytucji Rzeczypospolitej Polskiej.

Przechodząc do zastrzeżeń szczegółowych, w pierwszej kolejności Generalny Inspektor podniósł niecelowość i praktyczną niewykonalność unormowań zaproponowanych w projekcie założeń.

W związku z powyższym Generalny Inspektor zwrócił uwagę na treść art. 47 Konstytucji Rzeczypospolitej Polskiej przyznającego prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym oraz art. 8 ratyfikowanej przez Rzeczpospolitą Polską *Konwencji o ochronie praw człowieka i podstawowych wolności*²³⁷, zgodnie z którym każdy ma prawo do poszanowania swojego życia rodzinnego i nie jest dopuszczalna ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. GODO zaoponował przeciwko nałożeniu na osoby wykonujące zadania publiczne obowiązku składania informacji o zatrudnieniu w administracji publicznej ich krewnych do drugiego stopnia włącznie, powinowatych pierwszego stopnia albo osób związanych z tytułu przysposobienia, opieki lub kurateli.

²³⁵ Zob. np. ustawa z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, t. j. Dz. U. z 2006 r. Nr 216, poz. 1584 z późn. zm., ustawa z dnia 21 listopada 2008 r. o służbie cywilnej, Dz. U. Nr 227, poz. 1505 z późn. zm., ustawy samorządowe.

²³⁶ Np. osoby zajmujące kierownicze stanowiska państwowe w rozumieniu ustawy z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe, t. j. Dz. U. z 2011 r. Nr 79, poz. 430 oraz zatrudnione w organach administracji publicznej na „szeregowych” stanowiskach, czy też początkujących pracowników służby cywilnej lub zagranicznej.

²³⁷ Sporządzonej w Rzymie dnia 4 listopada 1950 r., Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.

Następnie Generalny Inspektor podniósł, że poprzez nieprawidłowo określony krąg osób zobowiązanych, przedstawiony projekt założeń przewiduje wprowadzenie nieproporcjonalnych – w jego ocenie – ograniczeń, które – bez uzasadnionej przyczyny – będą istotnie utrudniać, czy wręcz uniemożliwiać im, normalne funkcjonowanie w społeczeństwie.

Ustosunkowując się do stanowiska projektodawcy wobec zastrzeżeń do przedmiotowego projektu założeń, Generalny Inspektor zakwestionował pogląd wyrażony przez projektodawcę, zgodnie z którym sam fakt wchodzenia w skład podmiotu władzy publicznej (niezależnie od sprawowanej w tym podmiocie funkcji czy zajmowanego stanowiska) przesądza o przynależności danej osoby do kategorii osób pełniących funkcje publiczne. GODO stwierdził, iż pogląd ten ignoruje okoliczność, że w podmiotach władzy publicznej istnieje (co do zasady) hierarchiczne podporządkowanie osób i różny zakres ich władztwa decyzyjnego. Powtórzył swój zarzut, że stosowanie takiej samej ingerencji w prywatność osób znajdujących się na krańcowo różnych stopniach hierarchii służbowej i posiadających zasadniczo różny zakres uprawnień decyzyjnych nie wydaje się zgodne ze statuowaną w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej zasadą proporcjonalności. Za takim stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych dodatkowo przemawia okoliczność, iż zarówno dotychczasowe przepisy antykorupcyjne, jak i doktryna oraz orzecznictwo, wiązały możliwość istotnego ograniczenia praw osoby z faktem posiadania przez tę osobę określonego władztwa decyzyjnego. Generalny Inspektor w wątpliwość poddał także tezę, zgodnie z którą wszystkie kategorie osób wymienione w projekcie założeń²³⁸ to osoby posiadające tę samą cechę czy należące do tej samej klasy. Co więcej – sam projekt założeń wymienia osoby sprawujące niewątpliwie istotne funkcje publiczne²³⁹, w odniesieniu do których uregulowania ustawy powstałej w oparciu o projekt założeń miałyby się stosować jedynie częściowo, co czyni dodatkowo zasadnym zarzut organu do spraw ochrony danych osobowych co do naruszenia w proponowanych unormowaniach zasady równego traktowania proklamowanej w art. 32 Konstytucji Rzeczypospolitej Polskiej.

Generalny Inspektor odniósł się ponadto do stwierdzeń odpierających zarzut niecelowości i praktycznej niewykonalności unormowań zawartych w projekcie, podkreślając, iż kontrola – przewidzianych w projekcie założeń – kilkuset tysięcy do miliona rocznie oświadczeń majątkowych wymagać będzie zasadniczej rozbudowy aparatu urzędniczego i aparatu ścigania. Przy braku zaś podjęcia takich działań, które w aktualnej sytuacji budżetowej nie wydają się zresztą możliwe, zachodzić będzie konieczność ograniczenia się do weryfikowania samego faktu złożenia oświadczeń majątkowych przez osoby zobowiązane (w określonym przepisami terminie), bez merytorycznej oceny ich zawartości. Tym samym zgromadzona w tych oświadczeniach majątkowych wielka liczba

²³⁸ zob. s. 13 – 16.

²³⁹ Członkowie organów rad i zespołów opiniodawczych i doradczych Prezesa Rady Ministrów i Rady Ministrów, członkowie zarządu Narodowego Banku Polskiego, osoby kierujące komórkami organizacyjnymi Narodowego Banku Polskiego i ich zastępcy, członkowie Rady Polityki Pieniężnej, sędziowie Trybunału Stanu.

informacji (w tym danych osobowych) stanie się w istocie całkowicie nieprzydatna uprawnionym organom dla realizacji ich ustawowych zadań, co stanowić będzie naruszenie art. 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej.

Biorąc pod uwagę podniesione liczne zastrzeżenia co do zgodności zaproponowanych unormowań z przepisami Konstytucji Rzeczypospolitej Polskiej oraz ustawy o ochronie danych osobowych, Generalny Inspektor wnosił o zaniechanie prac nad projektem założeń w jego aktualnej formie i o ewentualnie przygotowanie nowego dokumentu uwzględniającego w swojej treści dotychczas zgłoszone zastrzeżenia i uwagi zainteresowanych podmiotów.

GIODO kontynuował również – po dwuletniej przerwie – spór z Ministerstwem Spraw Wewnętrznych i Administracji, zgłaszając zasadnicze uwagi do nowej wersji projektu *ustawy o centralnej ewidencji pojazdów oraz centralnej ewidencji kierowców*²⁴⁰. Generalny Inspektor stwierdził, iż projekt ten w znacznej mierze nie uwzględnia istotnych zastrzeżeń zgłoszonych przez Generalnego Inspektora Ochrony Danych Osobowych w toku dotychczasowych prac, jak również nie zawiera w swojej treści odzwierciedlenia ustaleń poczynionych w ramach procedury legislacyjnej dotyczącej ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. Nr 30, poz. 151). W tym stanie rzeczy organ do spraw ochrony danych osobowych czuł się w obowiązku przypomnieć, że dokonane już w zmianach²⁴¹ do ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (t. j. Dz. U. z 2005 r. Nr 108, poz. 908 z późn. zm.) przekształcenie centralnej ewidencji kierowców, zwanej dalej „CEK”, czyli rejestru administracyjnego, w rejestr „skazań i ukarań bezpośrednio związanych z ruchem drogowym”, choć zostało zaakceptowane przez Generalnego Inspektora Ochrony Danych Osobowych, rodzi daleko idące skutki w zakresie konieczności ochrony praw osób, których dane będą w tym rejestrze przetwarzane. Podnieść należało²⁴², iż dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, podlegają szczególnej ochronie i przetwarzanie danych tego rodzaju bez zgody osoby, której dane te dotyczą, wymaga przepisu szczególnego rangi ustawowej, stwarzającego przy tym pełne gwarancje ochrony takich danych. Nie mogła zatem zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych sytuacja, w której projekt ustawy o centralnej ewidencji pojazdów oraz centralnej ewidencji kierowców w ogóle nie przewiduje usunięcia z CEK danych dotyczących kierowania pojazdem w stanie nietrzeźwości, w stanie po użyciu alkoholu lub środka działającego podobnie do alkoholu²⁴³.

²⁴⁰ DOLiS-033-325/08, znak: 21043/11. W poprzednich wersjach skierowanych do zaopiniowania przez organ do spraw ochrony danych osobowych ustawa ta nosiła tytuł: „ustawa o centralnej ewidencji pojazdów i centralnej ewidencji kierowców oraz o zmianie niektórych innych ustaw”.

²⁴¹ Wprowadzonych przez art. 125 pkt 10 ustawy o kierujących pojazdami, z mocą obowiązującą od dnia 1 stycznia 2013 r.

²⁴² Zgodnie z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

²⁴³ Unormowanie takie nie tylko jest niezgodne z zasadami ochrony danych osobowych, lecz również pozostaje w oczywistej sprzeczności z przepisami dotyczącymi zatarcia skazań (art. 106 – 108 ustawy z dnia 6 czerwca 1997 r. –

Generalny Inspektor odniósł się też do kwestii udostępniania przez ministra właściwego do spraw wewnętrznych²⁴⁴ danych zgromadzonych w centralnej ewidencji pojazdów, zwanej dalej „CEP”, i „CEK”. GODO stwierdził, że zaproponowane brzmienie przepisu projektu ustawy o centralnej ewidencji pojazdów oraz centralnej ewidencji kierowców²⁴⁵ jest nie do zaakceptowania z punktu widzenia zasad ochrony danych osobowych. GODO przypomniał, iż ustawa o ochronie danych osobowych nakłada na administratora danych obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w tym obowiązek zapewnienia, aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnie z tymi celami²⁴⁶. Generalny Inspektor nie mógł przy tym pominąć, że przyjęta w projekcie ustawy o centralnej ewidencji pojazdów oraz centralnej ewidencji kierowców konstrukcja, zgodnie z którą minister właściwy do spraw wewnętrznych (administrator danych zgromadzonych w CEP i CEK) po stwierdzeniu, iż dane powierzone mu przez podmiot są niepełne, dokonuje ich uzupełnienia w oparciu o dane zawarte w CEP i CEK, pozostawała w rażącej sprzeczności z samą istotą (wypracowanej w ramach uzgodnień między Ministerstwem Spraw Wewnętrznych i Administracji a organem do spraw ochrony danych osobowych) instytucji prawnej weryfikacji danych. Generalny Inspektor Ochrony Danych Osobowych czuł się w obowiązku podkreślić, że Ministerstwo Spraw Wewnętrznych i Administracji zgodziło się na rozwiązanie, w myśl którego podmiot wnioskujący o weryfikację danych otrzymuje jedynie potwierdzenie zgodności przekazanych danych albo raport o niezgodności danych, w żadnym razie nie może jednak uzyskać w tym trybie danych poprawionych, czy też uzupełnionych.

GODO wskazał, iż konieczność dołożenia przez administratora danych (ministra właściwego do spraw wewnętrznych) szczególnej staranności w celu ochrony interesów osób, których dane znajdują się w CEK, w tym zapewnienia, by dane te były przetwarzane zgodnie z prawem, przemawia za zachowaniem trybu wnioskowego w odniesieniu do udostępniania danych z tego rejestru.

Niezależnie od powyższego GODO podniósł, że w świetle zasady równoprawności przesłanek przetwarzania danych osobowych określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych,

Kodeks karny, Dz. U. Nr 88, poz. 553 z późn. zm.) i zatacza ukarań (art. 46 ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń, t. j. Dz. U. z 2010 r. Nr 46, poz. 275 z późn. zm.).

²⁴⁴ Jako administratora danych – art. 2 ust. 2 i art. 15 ust. 2 projektu ustawy o centralnej ewidencji pojazdów oraz centralnej ewidencji kierowców.

²⁴⁵ Art. 31 projektu.

²⁴⁶ Skoro celem utworzenia CEP i CEK było zgromadzenie przez organ administracji publicznej (ministra właściwego do spraw wewnętrznych) informacji (danych) o pojazdach i ich właścicielach lub posiadaczach (CEP) oraz kierowcach, niektórych osobach nieposiadających uprawnień do kierowania pojazdami, a także osobach szkolących i egzaminujących kierowców albo uczestniczących w procedurze nadawania uprawnień do kierowania pojazdami (CEK), to zbiory te nie mogą być wykorzystywane jako zbiory referencyjne służące do odpłatnego (patrz art. 39 pkt 3 projektu ustawy o centralnej ewidencji pojazdów oraz centralnej ewidencji kierowców) porównywania zawartych w nich informacji z danymi zebranymi przez inne – nieokreślone nawet w przepisach – podmioty.

niezrozumiałe było użycie w projektowanym akcie²⁴⁷ sformułowania o przekazywaniu przez ubezpieczyciela do CEK danych dotyczących zawartej umowy obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadacza pojazdu: „bez wiedzy i zgody osoby, której te dane dotyczą”.

GIODO kontynuował także monitorowanie procesu legislacyjnego w związku z trwającymi w Podkomisji nadzwyczajnej do rozpatrzenia poselskiego projektu *ustawy o czynnościach operacyjno-rozpoznawczych oraz rządowego projektu ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw*, pracami dotyczącymi poselskiego projektu ustawy o czynnościach operacyjno-rozpoznawczych²⁴⁸. Generalny Inspektor zwrócił uwagę przewodniczącego podkomisji na istniejące w obowiązującej ustawie o ochronie danych osobowych ograniczenia kompetencji Generalnego Inspektora Ochrony Danych Osobowych w odniesieniu do zbiorów danych, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego oraz żołnierzy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego. Generalny Inspektor musiał zauważyć, iż w stosunku do takich zbiorów danych niezależny organ do spraw ochrony danych osobowych został, z jednej strony – pozbawiony możliwości przeprowadzenia kontroli²⁴⁹, z drugiej zaś – uniemożliwiono mu wydawanie decyzji administracyjnych dotyczących przetwarzania danych osobowych²⁵⁰. GIODO nadmienił, że pozostawione mu uprawnienie do skierowania do organu powołanego do ścigania przestępstw zawiadomienia o popełnieniu przestępstwa przez kierownika jednostki organizacyjnej, jej pracownika lub inną osobę fizyczną będącą administratorem danych, którego (których) działanie lub zaniechanie wyczerpuje znamiona przestępstwa określonego w ustawie o ochronie danych osobowych²⁵¹, uznał w tej sytuacji za iluzoryczne, gdyż na Generalnym Inspektorze Ochrony Danych Osobowych ciąży obowiązek dołączenia do zawiadomienia dowodów dokumentujących podejrzenie popełnienia przestępstwa²⁵², zaś zebranie takich dowodów przez organ do spraw ochrony danych osobowych bez skontrolowania zbioru danych nie wydaje się prawdopodobne. Choć kwestia nadzoru nad służbami specjalnymi niezależnego organu do spraw ochrony danych osobowych (w zakresie problematyki ochrony danych osobowych) nie jest w państwach członkowskich Unii Europejskiej rozstrzygnięta w sposób jednakowy, to GIODO uznaje za dominujący pogląd, że kontrola taka powinna być zachowana, oczywiście przy uwzględnieniu specyficznego charakteru działalności tych służb. Jednocześnie Generalny Inspektor nie pominął, iż sprawowanie takiego nadzoru znajduje silne oparcie w aktach prawa unijnego, spośród których

²⁴⁷ Zob. art. 60 pkt 4 projektu ustawy o centralnej ewidencji pojazdów oraz centralnej ewidencji kierowców, art. 43b ust. 2 ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, Dz. U. Nr 124, poz. 1152 z późn. zm.

²⁴⁸ DOLiS-033-137/10

²⁴⁹ Art. 43 ust. 2 w zw. z art. 14 pkt 1, 3 – 4 i art. 15 ustawy o ochronie danych osobowych.

²⁵⁰ Art. 43 ust. 2 w zw. z art. 12 pkt 2 i art. 18 ustawy o ochronie danych osobowych.

²⁵¹ Art. 19 ustawy o ochronie danych osobowych.

²⁵² Art. 19 *in fine* ustawy o ochronie danych osobowych.

w pierwszej kolejności wymienił decyzję ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. Urz. UE L 350 z 30.12.2008, s. 60), powoływaną dalej z zastosowaniem skrótu „decyzja ramowa”²⁵³. W ocenie Generalnego Inspektora Ochrony Danych Osobowych prawidłowa implementacja do polskiego porządku prawnego postanowień decyzji ramowej nie będzie możliwa przy zachowaniu aktualnie obowiązujących uregulowań ustawy o ochronie danych osobowych. Co więcej – wskazane w części wstępnej niniejszego pisma unormowania ustawy o ochronie danych osobowych zdają się pozostawać w jaskrawej sprzeczności z wyrażonymi w dokumencie Komisji Europejskiej z dnia 4 listopada 2010 r. Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”²⁵⁴ – tendencjami europejskimi zmierzającymi z jednej strony – do wzmocnienia praw osób fizycznych w procesie przetwarzania danych osobowych, z drugiej zaś – do rozszerzenia uprawnień niezależnych organów do spraw ochrony danych osobowych.

W związku z powyższym Generalny Inspektor zasugerował rozważenie zmian do ustawy o ochronie danych osobowych zwiększających kompetencje Generalnego Inspektora Ochrony Danych Osobowych wobec cywilnych służb specjalnych²⁵⁵. Ze względu na koniec kadencji Sejmu prace nad przedmiotowym projektem zostały zaniechane zgodnie z zasadą dyskontynuacji.

W niniejszym okresie sprawozdawczym 2011 roku, Generalny Inspektor przygotował wystąpienie w nawiązaniu do dotychczasowej korespondencji oraz spotkań w sprawie zastrzeżeń do projektu *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o współpracy w zwalczaniu przestępczości, w szczególności przestępczości*

²⁵³W myśl art. 25 ust. 1 decyzji ramowej, krajowy organ nadzoru (w Rzeczypospolitej Polskiej jest nim Generalny Inspektor Ochrony Danych Osobowych) wypełnia w sposób całkowicie niezależny swoje zadania w zakresie doradztwa i monitorowania stosowania na terytorium danego państwa członkowskiego przepisów przyjętych przez państwa członkowskie zgodnie z tą decyzją ramową. Przysługują mu przy tym – szczegółowo opisane w art. 25 ust. 2 lit. a i b decyzji ramowej – uprawnienia dochodzeniowe i interwencyjne, jak również prawo do podejmowania postępowań prawnych w przypadku naruszenia krajowych przepisów przyjętych na mocy tej decyzji ramowej lub do powiadamiania organów sądowych o takich naruszeniach (art. 25 ust. 2 lit. c decyzji ramowej).

²⁵⁴KOM(2010)609

²⁵⁵Mogłyby one polegać na wprowadzeniu w tej ustawie następujących rozwiązań prawnych: 1) art. 15 ust. 2 ustawy o ochronie danych osobowych otrzymuje brzmienie: „2. W toku kontroli zbiorów, o których mowa w art. 43 ust. 1 pkt 1a przetwarzanych przez Służbę Kontrwywiadu Wojskowego i Służbę Wywiadu Wojskowego, inspektor przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej.”; 2) art. 18 ust. 2a ustawy o ochronie danych osobowych otrzymuje brzmienie: „2a. Decyzje Generalnego Inspektora, o których mowa w ust. 1, w odniesieniu do zbiorów określonych w art. 43 ust. 1 pkt 1a przetwarzanych przez Służbę Kontrwywiadu Wojskowego i Służbę Wywiadu Wojskowego, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa.”; 3) art. 43 ust. 2 ustawy o ochronie danych osobowych otrzymuje brzmienie: „2. W odniesieniu do zbiorów, o których mowa w ust. 1 pkt 3, oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez Służbę Kontrwywiadu Wojskowego i Służbę Wywiadu Wojskowego, Generalnemu Inspektorowi nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1, 3-5 oraz w art. 15-18”.

*zorganizowanej*²⁵⁶, w którym poinformował, że podtrzymuje wątpliwości wyrażane w uprzedniej korespondencji.

Generalny Inspektor podniósł, że biorąc pod uwagę fakt, iż Stany Zjednoczone są państwem trzecim²⁵⁷ i to niedającym na swoim terytorium gwarancji ochrony danych osobowych takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, to jedynie postanowienia umowy międzynarodowej zawieranej pomiędzy Rzeczpospolitą Polską a Stanami Zjednoczonymi (i to ratyfikowanej za uprzednią zgodą wyrażoną w ustawie – art. 89 ust. 1 Konstytucji Rzeczypospolitej Polskiej) mogą zapewnić prawidłowe przetwarzanie danych pomiędzy Stronami oraz odpowiednie gwarancje ochrony danych osobowych. Zachowując tak daleko posuniętą ostrożność, Generalny Inspektor Ochrony Danych Osobowych zwrócił ponownie uwagę na następujące kwestie: a) szczególne znaczenie wobec przetwarzania danych wrażliwych, do których niewątpliwie należą dane o kodzie genetycznym, co powinno znaleźć odzwierciedlenie w projekcie; b) wątpliwości, jakie budzi włączenie do polskiego porządku prawnego mechanizmu zautomatyzowanego przeszukiwania profili DNA. GODO zaakcentował, iż jest to instrument nieznanym dotychczas prawu wielu państw europejskich, w tym prawu polskiemu.

W świetle powyższego zaproponowane w powołanym przepisie projektu umowy kryteria wydały się Generalnemu Inspektorowi niewystarczające. Zasugerował więc rozważenie ich uzupełnienia poprzez wskazanie, że przeszukiwanie może być prowadzone nie tylko „wyłącznie w indywidualnych przypadkach i zgodnie z prawem wewnętrznym państw obu Umawiających się Stron”, ale również wtedy, „gdy jest to niezbędne z uwagi na charakter przestępstwa”. Podniósł przy tym, że proponowane doprecyzowanie kryteriów zautomatyzowanego przeszukiwania zagwarantowałoby wykorzystywanie powyższego instrumentu w sposób proporcjonalny i adekwatny do charakteru przestępstw, zapobiegając jednocześnie potencjalnym nadużyciom w przypadku przestępstw, które w istocie nie wymagają jego zastosowania.

Kontynuując opiniowanie projektu przedmiotowej Umowy, która w trakcie procesu uzgodnieniowego zyskała tytuł *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o współpracy w dziedzinie zapobiegania i zwalczania poważnej przestępczości*²⁵⁸, Generalny Inspektor poddał pod rozagę projektodawcy – zwracając się jednocześnie z prośbą o stosowne wyjaśnienia w tym zakresie – zagadnienie odmiennego niż w przepisach polskich, uregulowania kwestii ochrony przekazywanych danych osobowych dotyczącego: a) nieobjęcia danych dotyczących skazań reżimem szczególnej ochrony; b) istotnego

²⁵⁶ DOLiS-033-134/10

²⁵⁷ W rozumieniu art. 7 pkt 7 ustawy o ochronie danych osobowych.

²⁵⁸ DOLiS-033-134/10. Pierwszy projekt przedmiotowej Umowy pod nazwą Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki Północnej o współpracy w zwalczaniu przestępczości, w szczególności przestępczości zorganizowanej, został przedstawiony w piśmie z dnia 6 kwietnia 2010 r. od Podsekretarza Stanu w MSWiA.

ograniczenia praw osób, których dane podlegać będą przekazaniu (obowiązek informacyjny realizowany tylko na wniosek i z szerokimi możliwościami odstąpienia od udzielenia informacji²⁵⁹); c) uznania prowadzenia postępowania administracyjnego jako dopuszczalnego celu uzasadniającego przetwarzanie przez stronę otrzymującą przekazanych jej danych osobowych²⁶⁰.

W 2011 r. Generalny Inspektor, w związku z ustaleniami poczynionymi w trakcie posiedzenia Podkomisji nadzwyczajnej²⁶¹, ponownie przekazał swoje, pierwotnie skierowane do Szefa Kancelarii Sejmu²⁶², stanowisko odnośnie projektu *ustawy o kredycie konsumenckim*²⁶³.

W pierwszej kolejności organ do spraw ochrony danych osobowych zgłosił, iż zastrzeżenia budzi sposób sformułowania jednego z artykułów²⁶⁴ projektu, gdyż określony w tym przepisie katalog informacji, w tym danych osobowych, które zawierać ma 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 danych osobowych, co stwarza niebezpieczeństwo pozyskiwania przez kredytodawców danych zbędnych, w nadmiarze, i – w konsekwencji – naruszenia zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Identyczna uwaga zgłoszona została również wobec innego proponowanego przepisu²⁶⁵. GIODO wskazał też, że w sprzeczności z zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane, pozostaje także dyspozycja kolejnego²⁶⁶ przepisu projektu, bowiem skoro termin „dane osobowe” obejmuje swoim zakresem wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, użycie w kwestionowanym przepisie pojęcia „dane konsumenta” bez bliższego jego sprecyzowania²⁶⁷ nie pozwala na ustalenie, jakie informacje o konsumencie winny być zawarte w projekcie umowy, o którym mowa w tym przepisie²⁶⁸.

W analizowanym okresie sprawozdawczym Generalny Inspektor udzielił również odpowiedzi na pismo dotyczące dokumentu *Projekt założeń projektu ustawy o lobbingu*²⁶⁹, w którym wyraził stanowisko odnośnie braku w projekcie założeń propozycji wprowadzenia przepisu materialnego, nakładającego na lobbystę zawodowego wymóg niekaralności za umyślne przestępstwo lub umyślne

²⁵⁹ Art. 13 ust. 12 projektu.

²⁶⁰ Art. 13 ust. 2 pkt 3 projektu.

²⁶¹ Posiedzenie Podkomisji nadzwyczajnej odbyło się dnia 4 stycznia 2010 r.

²⁶² Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 21 grudnia 2010 r. zawierające uwagi do rządowego projektu ustawy o kredycie konsumenckim, DOLiS-033-450/10/50279.

²⁶³ DOLiS-033-450/10

²⁶⁴ Art. 30 ust. 1 ustawy.

²⁶⁵ Art. 35 ust. 1 zdanie wstępne.

²⁶⁶ Art. 12 *in fine*.

²⁶⁷ Choćby przez odesłanie do art. 30 ust. 1 pkt 1.

²⁶⁸ Ustawa o kredycie konsumenckim została ogłoszona w Dzienniku Ustaw z dnia 17 czerwca 2011 r. Nr 126, poz. 715, jako ustawa z dnia 12 maja 2011 r. o kredycie konsumenckim i weszła w życie z dniem 18 grudnia 2011 r.

²⁶⁹ DOLiS-033-174/10

przestępstwo skarbowe oraz wymóg, by nie toczyło się przeciwko niemu postępowanie karne o – ścigane z oskarżenia publicznego – przestępstwo umyślne. Tym samym nierozstrzygnięta została wątpliwość organu do spraw ochrony danych osobowych, czy przy braku takiego przepisu materialnego (czyli nieokreśleniu w projektowanej ustawie o lobbingu wymagań formalnych dla przyznania prawa wykonywania zawodu lobbysty zawodowego) dopuszczalne jest nakładanie na osobę ubiegającą się o wpis do rejestru lobbystów zawodowych, obowiązku składania oświadczenia o niekaralności za umyślne przestępstwo lub umyślne przestępstwo skarbowe, jak również oświadczenia, iż nie toczy się wobec niej postępowanie karne o przestępstwo umyślne ścigane z oskarżenia publicznego²⁷⁰.

Następnie GODO wskazał, że z punktu widzenia zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane, celowym byłoby zastąpienie sformułowania²⁷¹ „dane identyfikacyjne lobbysty uczestniczącego w spotkaniu”, jednoznacznym określeniem zakresu danych osobowych lobbysty, jaki ma być zamieszczony w sprawozdaniu ze spotkania przedstawicieli lobbowanego podmiotu z lobbystami (lobbystą).

Opiniując ten projekt, GODO podniósł również, że wobec wprowadzenia obowiązku²⁷² publikacji w Biuletynie Informacji Publicznej list obecności na posiedzeniach Komisji Wspólnej Rządu i Samorządu Terytorialnego oraz list obecności ze spotkań rad i zespołów powoływanych na podstawie przepisu ustawy o Radzie Ministrów²⁷³, względ na zasadę adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane, przemawia za określeniem w projekcie założeń katalogu danych osobowych, jakie zawierać mają przedmiotowe listy.

W 2011 roku organ do spraw ochrony danych osobowych podtrzymał – wyrażane już w 2009 roku²⁷⁴ – negatywne stanowisko wobec zamieszczonej w przepisie art. 1 pkt 59 *projektu ustawy o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw* – propozycji brzmienia art. 102 ust. 2 ustawy Prawo lotnicze²⁷⁵. W opinii Generalnego Inspektora Ochrony Danych Osobowych brak jest argumentów przemawiających za – proklamowaną w znowelizowanym art. 102 ustawy – Prawo lotnicze – całkowitą jawnością danych zawartych w rejestrze personelu lotniczego, zwłaszcza, że rejestr ten zawierał dotychczas tak osobiste dane, jak numer PESEL członka personelu lotniczego oraz adres jego miejsca zamieszkania²⁷⁶. Organ do spraw ochrony danych osobowych stał na stanowisku, iż projektodawcy nie wskazali w trakcie prac legislacyjnych powodów, dla których tego rodzaju dane

²⁷⁰ zob. s. 17 projektu założeń.

²⁷¹ zob. s. 25 projektu założeń.

²⁷² zob. s. 26 projektu założeń.

²⁷³ Art. 7 ust. 4 pkt 4 i 5 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów, t. j. Dz. U. z 2003 r. Nr 24, poz. 199 z późn. zm.

²⁷⁴ DOLiS-035-1783/09/39652 oraz DOLiS-035-1783/09/42791.

²⁷⁵ Ustawa z dnia 3 lipca 2002 r. – Prawo lotnicze, t. j. Dz. U. z 2006 r. Nr 100, poz. 696 z późn. zm.

²⁷⁶ zob. obowiązujące rozporządzenie Ministra Infrastruktury z dnia 3 września 2003 r. w sprawie licencjonowania personelu lotniczego, Dz. U. Nr 165, poz. 1603 z późn. zm.

należące do sfery prywatności człowieka miałyby być danymi jawnymi, a co więcej – zaproponowane ujęcie dyspozycji art. 102 ust. 2 ustawy – Prawo lotnicze²⁷⁷, w ocenie Generalnego Inspektora Ochrony Danych Osobowych narusza zasadę adekwatności przetwarzanych (w niniejszej sprawie – udostępnianych) danych w stosunku do celów, w jakich są one przetwarzane (udostępniane). Nie można było przy tym pominąć, że brzmienie kwestionowanego przepisu uniemożliwi utajnienie numerów PESEL, czy adresów zamieszkania członków personelu lotniczego w nowym rozporządzeniu wydanym na podstawie delegacji zawartej w ustawie – Prawo lotnicze²⁷⁸. Z przytoczonych powodów organ do spraw ochrony danych osobowych wniosł o odstąpienie od proponowanej zmiany tego przepisu.

Niezależnie od powyższego Generalny Inspektor Ochrony Danych Osobowych wniosł o uzupełnienie delegacji z ustawy – Prawo lotnicze²⁷⁹ o upoważnienie ministra właściwego do spraw transportu do określenia zakresu danych zamieszczanych w prowadzonych przez Prezesa Urzędu Lotnictwa Cywilnego: liście audytorów krajowych²⁸⁰, liście audytorów wewnętrznych²⁸¹ oraz rejestrze osób posiadających CMC²⁸².

Generalny Inspektor zwrócił również uwagę, że w projekcie ustawy nowelizującej ustawę – Prawo lotnicze przewiduje się wprowadzenie przez Prezesa Urzędu Lotnictwa Cywilnego rejestru zarejestrowanych agentów, a w projekcie ustawy nowelizującej brak jest w ogóle przepisu regulującego zakres danych, które ma zawierać ten rejestr.

W bieżącym okresie sprawozdawczym GODO kontynuował zgłaszanie uwag do poselskiego *projektu ustawy o języku migowym i innych środkach wspierania komunikowania się*, procedowanego przez Komisję Polityki Społecznej i Rodziny. Opiniując go podniósł, iż projekt²⁸³ powiela rozwiązania istniejące w obowiązującym systemie prawa. Przywołał art. 24 i art. 25 ustawy o ochronie danych osobowych, statuujące obowiązek informacyjny odpowiednio w przypadku zbierania danych osobowych od osoby, której one dotyczą, oraz zbierania danych osobowych nie od osoby, której one dotyczą, zwracając uwagę na okoliczności, gdy administrator danych jest z tego obowiązku zwolniony, np. w przypadku dobrowolnego zgłoszenia się osoby uprawnionej wraz z osobą przybraną do urzędu i dobrowolnego podania przez nich swoich danych²⁸⁴ lub jeżeli dane te są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1, na podstawie

²⁷⁷ Przewidziane w art. 1 pkt 59 projektu ustawy nowelizującej.

²⁷⁸ W art. 104 ust. 1 pkt 4 lit. d ustawy – Prawo lotnicze (art. 1 pkt 62 lit. a projektu ustawy nowelizującej).

²⁷⁹ Art. 189 ust. 2 i art. 189a ust. 2 ustawy – Prawo lotnicze (w brzmieniu nadanym przez art. 1 pkt 122 projektu ustawy nowelizującej i w brzmieniu nadanym przez art. 1 pkt 123 projektu ustawy nowelizującej).

²⁸⁰ Art. 188d ust. 1 ustawy – Prawo lotnicze, dodany przez art. 1 pkt 121 projektu ustawy nowelizującej.

²⁸¹ Art. 188d ust. 2 ustawy – Prawo lotnicze, dodany przez art. 1 pkt 121 projektu ustawy nowelizującej.

²⁸² Art. 188b ust. 7 ustawy – Prawo lotnicze, dodany przez art. 1 pkt 121 projektu ustawy nowelizującej.

²⁸³ Art. 8 ust. 2 projektu ustawy.

²⁸⁴ Art. 24 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

przepisów prawa²⁸⁵. Taka sytuacja będzie miała miejsce w przypadku załatwiania spraw przez osobę uprawnioną korzystającą z pomocy osoby przybranej w podmiotach, o których mowa w art. 6 projektowanej ustawy, to jest organach administracji publicznej, jednostkach systemu (jednostki systemu Państwowego Ratownictwa Medycznego), podmiotach leczniczych, jednostkach Państwowej Straży Pożarnej i Strażach Gminnych. Organ do spraw ochrony danych osobowych wskazał, iż w jego opinii podmioty te należą do kategorii podmiotów, o których mowa w art. 25 ust. 2 pkt 5 ustawy o ochronie danych osobowych, a co za tym idzie nie muszą one wypełniać obowiązku informacyjnego, gdyż korzystają ze zwolnienia z tego obowiązku przewidzianego *expressis verbis* w ustawie o ochronie danych osobowych. Dlatego też rozwiązanie zapisane w projekcie należy uznać za zbędne, w związku z czym GODO zwrócił się z prośbą o skreślenie zawierającego je przepisu²⁸⁶.

Do Generalnego Inspektora został również przedłożony **Projekt założeń do projektu ustawy o cudzoziemcach**²⁸⁷, do którego nie zgłosił uwag, jednakże przypomniał, iż zarówno w świetle ustawy o ochronie danych osobowych, jak i norm prawa europejskiego, organem uprawnionym do kontroli zgodności procesu przetwarzania danych z przepisami o ochronie danych osobowych jest niezależny organ do spraw ochrony danych osobowych (w Rzeczypospolitej Polskiej – Generalny Inspektor Ochrony Danych Osobowych). Tym samym jakiegokolwiek przepisy szczególne nadające innemu podmiotowi kompetencje w tej dziedzinie nie mogą skutkować ograniczeniem uprawnień Generalnego Inspektora Ochrony Danych Osobowych. Co za tym idzie – stanowisko organu do spraw ochrony danych osobowych o niekwestionowaniu dokumentu **Projekt założeń do projektu ustawy o cudzoziemcach** zachowuje aktualność jedynie przy założeniu, że – przewidziane w tym dokumencie²⁸⁸ – nadanie Szefowi Urzędu do Spraw Cudzoziemców kompetencji nadzorczych nad prawidłowością działania Systemu Pobyt nie będzie oznaczało jakiegokolwiek ograniczenia uprawnień kontrolnych Generalnego Inspektora Ochrony Danych Osobowych wynikających z przepisów ustawy o ochronie danych osobowych w odniesieniu do tego systemu.

W związku z opiniowanym **projektem ustawy o zmianie ustawy o systemie oświaty oraz o zmianie niektórych innych ustaw**²⁸⁹ Generalny Inspektor zmuszony był zaproponować liczne zmiany dotyczące katalogów danych osobowych. I tak, GODO wskazał, że dookreślić należy zakres

²⁸⁵ Administratorem danych, do którego odsyła przepis art. 25 ust. 2 pkt 5 jest organ państwowy, organ samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne (art. 3 ust. 1 ustawy o ochronie danych osobowych) i podmioty publiczne realizujące zadania publiczne (art. 3 ust. 2 pkt 1 ustawy o ochronie danych osobowych).

²⁸⁶ Ustawa ta pod tytułem ustawa z dnia 18 października 2011 r. o języku migowym i innych środkach komunikowania się, ogłoszona w Dz. U. z dnia 18 października 2011 r. Nr 209, poz. 1243, weszła w życie w dniu 1 kwietnia 2012 r. z wyjątkiem art. 7 i art. 8, które weszły w życie z dniem ogłoszenia tego aktu prawnego.

²⁸⁷ DOLiS-033-57/11

²⁸⁸ zob. s. 167 tego dokumentu.

²⁸⁹ DOLiS-033-78/11

informacji zawartych w protokołach, o których mowa w projektowanych przepisach²⁹⁰; dookreślić zakres informacji zawartych w raporcie ewaluacji, o ile będzie zawierał on dane osobowe²⁹¹; dookreślić zakres informacji zawartych w protokole kontroli, o ile będzie zawierał on dane osobowe, tak aby jasnym było, jakie dane osobowe będą w nim zawarte²⁹²; poprawić przepis zawierający odesłania do przepisów nieistniejących²⁹³; we wskazanych artykułach dodać wyrazy „w zakresie niezbędnym do prowadzenia tej kontroli”²⁹⁴; w jednym z projektowanych przepisów usunąć wyraz „w szczególności” i dodać postanowienia precyzyjnie określające zakres danych osobowych, które mają być zawarte w akcie nadania stopnia awansu zawodowego nauczyciela²⁹⁵.

Ponadto Generalny Inspektor zauważył, iż aktualność zachowują uwagi organu do spraw ochrony danych osobowych, przedstawione Ministrowi Edukacji Narodowej²⁹⁶, dotyczące konieczności 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.

W bieżącym okresie sprawozdawczym GIODO zgłosił uwagi do poselskiego *projektu ustawy o jawności i działalności lobbingowej w procesie stanowienia prawa*²⁹⁷. Generalny Inspektor stwierdził, że z punktu widzenia unormowań zawartych w ustawie o ochronie danych osobowych stosownego doprecyzowania wymagałyby niektóre z projektowanych przepisów²⁹⁸, przewidujących przetwarzanie, w tym upublicznianie, danych osób biorących udział w procesie stanowienia prawa²⁹⁹, ale nie wskazujących, jakie dane tych osób będą przetwarzane. Takie ujęcie kwestionowanych przepisów prowadzić może w opinii GIODO do przetwarzania dowolnych danych wskazanych wyżej

²⁹⁰ W art. 1 pkt 7 projektu stanowiącego o treści art. 5f zmienianej ustawy o systemie oświaty, dookreślić zakres informacji zawartych w protokole, o którym mowa w ust. 11 tego artykułu, podobnie, należy dookreślić zakres informacji zawartych w protokole, o którym mowa w art. 78v ust. 8.

²⁹¹ Dookreślić zakres informacji zawartych w raporcie ewaluacji, o którym mowa w ust. 2 tego artykułu, o ile będzie zawierał on dane osobowe, a nie tylko wskazanie poziomów spełnienia wymagań, o których mowa w art. 78h ust. 6.

²⁹² W art. 1 pkt 67 projektu stanowiącego o treści m.in. art. 78m zmienianej ustawy o systemie oświaty, dookreślić zakres informacji zawartych w protokole kontroli, o którym mowa w ust. 3 tego artykułu, o ile będzie zawierał on dane osobowe, tak, aby jasnym było, jakie dane osobowe będą w nim zawarte.

²⁹³ W art. 1 pkt 67 projektu stanowiącego o treści m.in. art. 78t ust. 1 pkt 3 i w art. 78v ust. 2 pkt 9 zmienianej ustawy o systemie oświaty, postanowienia ww. przepisów zawierają odesłania do przepisów nieistniejących.

²⁹⁴ W art. 1 pkt 69 i w art. 1 pkt 81 projektu stanowiącego o treści m.in. art. 90 ust 20 projektu stanowiącego o treści m.in. art. 80a ust 4 zmienianej ustawy o systemie oświaty.

²⁹⁵ W art. 2 pkt 5 lit. c projektu stanowiącego o treści art. 9b ust 5 zmienianej ustawy Karta nauczyciela, usunąć w zdaniu pierwszym ww. przepisu wyraz „w szczególności” i dodać postanowienia precyzyjnie określające zakres danych osobowych, które mają być zawarte w akcie nadania stopnia awansu zawodowego nauczyciela.

²⁹⁶ np. w korespondencji Generalnego Inspektora z dnia 25 sierpnia 2010 r., DOLiS-035-2099/10/34028.

²⁹⁷ DOLiS-033-137/11

²⁹⁸ Art. 8 ust. 2 lit. a, b, e i g oraz art. 9 ust. 2 lit. b – d.

²⁹⁹ Odpowiednio: osób zgłaszających wnioski w trakcie spotkań dotyczących projektu aktu prawnego – art. 8 ust. 2 lit. a; uczestników takich spotkań – art. 8 ust. 2 lit. b; autorów ekspertyz, opinii i konsultacji prawnych dotyczących projektu aktu prawnego – art. 8 ust. 2 lit. e; osób, które były uprawnione do prac nad projektem – art. 8 ust. 2 lit. g i art. 9 ust. 2 lit. c; autora projektu – art. 9 ust. 2 lit. b; autorów poprawek do projektu – art. 9 ust. 2 lit. d.

osób, a tym samym do naruszenia jednej z podstawowych zasad ochrony danych osobowych, to jest zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane.

W niniejszym okresie sprawozdawczym wpłynął do zaopiniowania rządowy projekt *ustawy o kontroli w administracji rządowej*³⁰⁰. Generalny Inspektor zakwestionował przepis art. 10 ust. 2 projektowanej ustawy, w którym posłużono się sformułowaniem „kierownicy jednostek kontrolujących określą, w porozumieniu, skład zespołu kontrolującego (...)”. Z treści tego przepisu projektu nie wynikało bowiem, jakie dane osobowe członków zespołu kontrolującego będą w takim przypadku przetwarzane. Powyższe może rodzić wątpliwości interpretacyjne w przedmiocie sposobu wskazywania osób wykonujących czynności kontrolne, a ponadto naruszać wspomnianą zasadę adekwatności. W kolejnym przepisie³⁰¹ projektu ustawy GODO zaproponował, aby określić katalog danych osobowych przetwarzanych na okoliczność sporządzania protokołu z przebiegu oględzin oraz z przyjęcia ustnych wyjaśnień lub oświadczeń poprzez wymienienie, jakie konkretnie dane osób uczestniczących w kontroli podlegają przetwarzaniu. Natomiast we wstępie do wyliczenia w przepisie art. 37 ust. 2 projektu ustawy zasugerował utworzenie zamkniętego katalogu danych i informacji wchodzących w skład projektu wystąpienia pokontrolnego. Użycie wyrażenia „w szczególności” w odniesieniu do danych osobowych wymienionych w pkt 2 może sugerować, iż przetwarzaniu będą podlegały jeszcze inne – poza wskazanymi w tym punkcie - dane osobowe.

Mając na względzie powyższe, Generalny Inspektor zaproponował takie zredagowanie treści skomentowanych przepisów projektu ustawy, aby w sposób niebudzący wątpliwości wynikało z nich, jakie dane osobowe adresatów danej normy podlegają przetwarzaniu.

Na uwzględnienie w bieżącym okresie sprawozdawczym zasługuje opinia Generalnego Inspektora dotycząca projektu *ustawy o zmianie ustawy o nawozach i nawożeniu oraz ustawy o odpadach*, w której GODO stwierdził, że z punktu widzenia zasad ochrony danych zastrzeżenie budzi sposób sformułowania przepisu art. 3 ust. 4 ustawy z dnia 10 lipca 2007 roku o nawozach i nawożeniu (Dz. U. Nr 147, poz. 1033) w brzmieniu nadanym przez art. 1 pkt 4 lit. c opiniowanego projektu³⁰². GODO podniósł, że projektowany przepis ustawy o nawozach i nawożeniu nie wyznacza maksymalnego okresu przechowywania takiej umowy, co uznał za rozwiązanie pozostające w sprzeczności z art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych. GODO zauważył, że skoro powołany przepis ustawy o ochronie danych osobowych nakazuje, by dane były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania, to jeśli projektodawca przyjął, iż zachodzi konieczność

³⁰⁰ DOLiS-033-164/11

³⁰¹ Art. 33 ust. 2 pkt 1

³⁰² Zgodnie z dyspozycją zakwestionowanego przepisu (w związku z art. 3 ust. 3 ustawy o nawozach i nawożeniu) strony umowy zbicia do bezpośredniego rolniczego wykorzystania nawozów naturalnych są zobowiązane do przechowywania takiej umowy (zawierającej dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych) przez okres co najmniej 4 lat od dnia jej zawarcia.

przechowywania danych przez strony, winien jednoznacznie wskazać w ustawie o nawozach i nawożeniu czas tego przechowywania.

Opiniując projekt *rozporządzenia Rady Ministrów w sprawie zintegrowanego systemu informacji o nieruchomościach* Generalny Inspektor zgłosił następujące uwagi. Po pierwsze, zaproponował zmianę definicji „urządzenia interfejsowego”³⁰³ na „interfejs”. Natomiast w przypadku pozostawienia dotychczasowej definicji (choć ze względu na jej znaczenie w dalszej części rozporządzenia w ocenie Generalnego Inspektora Ochrony Danych Osobowych może ona budzić wątpliwości interpretacyjne) przy redagowaniu jej rozszerzenia zasugerował rozważenie użycia zwrotu: „zespół urządzeń i oprogramowania umożliwiającego komunikację (...)”, ponieważ komunikacja pomiędzy systemami odbywa się za pomocą wielu urządzeń interfejsowych³⁰⁴. Po drugie GODO zwrócił uwagę, iż w projekcie³⁰⁵ użyto nieprecyzyjnego sformułowania „formy odrębnego zbioru danych” do oznaczenia wyróżnika dwóch wersji tego samego obiektu pochodzących z dwóch różnych kopii danych ewidencji gruntów i budynków, w związku z czym zwrot ten należałoby doprecyzować. Po trzecie, z uwagi na to, iż z kontekstu, w jakim użyto pojęcia „zbiorów”³⁰⁶ należy przypuszczać, że chodzi o obiekty lub zestawy danych dotyczących obiektów będących elementami zbioru danych przestrzennych centralnego repozytorium, Generalny Inspektor zasugerował przeredagowanie stosownych przepisów, gdyż jest to znaczenie niewłaściwe. Ponadto zaproponowane zostało dodanie wykazu zdarzeń lub ogólnego opisu rodzaju zdarzeń, które inicjują automatyczne wytworzenie zawiadomienia o zmianach danych PESEL³⁰⁷. Proponowane uzupełnienie ma na celu doprecyzowanie zakresu przepisu oraz wyjaśnienie kontekstu, w jakim użyto wyrazu „automatycznie”. Generalny Inspektor zauważył również, iż szerokie wykorzystanie interfejsów do innych rejestrów publicznych bez precyzyjnego odnoszenia się do zakresu uprawnień dotyczących pozyskiwania danych z tych rejestrów oraz kontroli uprawnień i obowiązków w tym zakresie rodzi ryzyko nadużyć. Dlatego też wskazał, iż podmioty, na które nakłada się takie zadania, powinny opracować i wprowadzić odpowiednie mechanizmy kontroli w zakresie realizacji swoich obowiązków. Organ do spraw ochrony danych osobowych, z uwagi na niezakończenie prac legislacyjnych nad projektem, zwrócił się z prośbą o informowanie go o sposobie i trybie dalszego procedowania nad tym projektem oraz zastrzegł sobie prawo do zgłaszania do niego dalszych uwag.

Uzupełniając wskazać należy, iż w IV kwartale 2011 r. Generalny Inspektor Ochrony Danych Osobowych - oprócz kontynuowania swojego udziału w związku z postępowaniem prac legislacyjnych nad projektami opiniowanymi w wersjach pierwotnych – przedstawił także swoje stanowisko wobec

³⁰³ § 2 pkt 6 projektu rozporządzenia.

³⁰⁴ Ostatecznie projektodawca uwzględnił pierwsze z zaproponowanych przez GODO rozwiązań.

³⁰⁵ § 5 ust. 4 projektu.

³⁰⁶ § 9 pkt 2 i 3 projektu rozporządzenia.

³⁰⁷ § 13 projektu rozporządzenia.

szeregu projektów rozporządzeń o istotnym znaczeniu z punktu widzenia ochrony danych osobowych, zwracając projektodawcom uwagę na ich braki i proponując stosowne zmiany.

Do organu do spraw ochrony danych osobowych w IV kwartale trafił ponadto pakiet dwóch rozporządzeń do ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej, dotyczących bazy danych SIO.

Zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych w projekcie *rozporządzenia Ministra Edukacji Narodowej w sprawie procedury weryfikacji dostępu do bazy danych SIO*³⁰⁸, wzbudziła dyspozycja przepisu § 11 tego aktu, zgodnie z którym dostęp do systemu SIO uzyskuje się jedynie w oparciu o nadawany niepowtarzalny, poufny identyfikator. Uwzględniając, że przedstawiony do zaopiniowania projekt rozporządzenia miał – w myśl art. 76 ustawy o systemie informacji oświatowej – określać procedurę dostępu do bazy danych SIO, wątpliwości organu do spraw ochrony danych osobowych wywołał brak w tym przepisie wymagań dla uwierzytelniania się upoważnionych osób w systemie SIO, takich jak: podawanie hasła, PIN – u, czy użycie tokenu.

W projekcie *rozporządzenia Ministra Edukacji Narodowej w sprawie warunków technicznych dla sprzętu oraz oprogramowania służącego prowadzeniu lokalnych baz danych SIO, a także warunków technicznych przekazywania i pozyskiwania danych z bazy danych SIO*³⁰⁹ organ do spraw ochrony danych osobowych zwrócił uwagę na konieczność zawężenia pojęcia „zabezpieczenie” użytego w § 11 projektu, w kontekście, w którym projektodawca miał na myśli zabezpieczenie poufności danych podczas ich teletransmisji, nie zaś o ich zabezpieczenie przed np. przypadkową utratą lub zniszczeniem. Otrzymując kolejną wersję projektu, Generalny Inspektor zauważył nieprawidłowe posługiwanie się w zmienionym stosownie do powyżej omówionej uwagi przepisie pojęciem „mechanizmy szyfrowania danych osobowych”. Mechanizmy szyfrowania danych odnoszą się bowiem do danych niezależnie od ich rodzaju (dane osobowe, dane finansowe, dane pomiarowe itp.), wobec czego nie istnieją specjalne mechanizmy szyfrowania np. wyłącznie danych osobowych, wobec czego zaproponował stosowną zmianę jego brzmienia³¹⁰.

Do Generalnego Inspektora wpłynął również do zaopiniowania pakiet projektów rozporządzeń wydawanych na podstawie ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.), do których zgłoszone zostały liczne uwagi.

³⁰⁸ DOLiS-033-391/11; rozporządzenie wydawane na podstawie delegacji zawartej w art. 99 ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej, Dz. U. Nr 139, poz. 814 z późn. zm.

³⁰⁹ Rozporządzenie wydawane na podstawie delegacji zawartej w art. 99 ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej, Dz. U. Nr 139, poz. 814 z późn. zm.

³¹⁰ Generalny Inspektor zaproponował zmianę brzmienia § 11 projektu – w poprawionej wersji § 9: „Do celów zabezpieczenia poufności przekazywania danych osobowych do bazy danych SIO i pozyskiwania danych z bazy danych SIO wykorzystuje się mechanizmy szyfrowania danych.”

W projekcie *rozporządzenia Ministra Edukacji Narodowej w sprawie egzaminów eksternistycznych*³¹¹ Generalny Inspektor zwrócił uwagę, iż katalog danych osobowych, jakie w określonym przypadku mają być zamieszczone w różnego rodzaju protokołach, winien każdorazowo mieć charakter zamknięty, co nie jest możliwe przy użyciu sformułowania „w szczególności” poprzedzającego wstęp do wyliczenia elementów określających skład protokołów.³¹² Celem uniknięcia wątpliwości, jakie dane osobowe – poza wymienionymi – mogą zostać pozyskane i wpisane do protokołów oraz wyeliminowania możliwości naruszenia zasady adekwatności danych w stosunku do celu ich przetwarzania, organ do spraw ochrony danych osobowych zaproponował usunięcie tego sformułowania z treści odpowiednich przepisów.

W celu doprecyzowania, jakie rodzaje dokumentów wymienionych w przepisach projektowanego rozporządzenia (w tym, w szczególności zawierających dane osobowe), należy zaklasyfikować jako dokumentację egzaminów eksternistycznych, organ do spraw ochrony danych osobowych zasugerował zmianę treści § 32 ust. 2 w zakresie wprowadzenia odesłań do wskazania innej – poza arkuszami egzaminacyjnymi oraz kartami odpowiedzi i protokołami sprawdzania arkuszy egzaminacyjnych – dokumentacji egzaminów eksternistycznych przechowywanej według zasad określonych w odrębnych przepisach. Do przedstawienia takiej uwagi skłonił Generalnego Inspektora przepis § 8 projektu, w którym mowa jest o konieczności dołączenia do wniosku o dopuszczenie do egzaminu eksternistycznego kserokopii dokumentu zawierającego datę urodzenia i numer ewidencyjny PESEL. Pozyskanie kserokopii takiego dokumentu prowadzi bowiem do przetwarzania danych w bardzo szerokim zakresie i mając na względzie zasady dotyczące ochrony danych osobowych rodzi wątpliwość, czy kserokopie dokumentów dołączanych do wniosku o dopuszczenie do egzaminu są „pozostałą” (poza arkuszami egzaminacyjnymi oraz kartami odpowiedzi i protokołami sprawdzania arkuszy egzaminacyjnych) dokumentacją egzaminów eksternistycznych. Generalny Inspektor wskazał ponadto, iż z projektu rozporządzenia nie wynika cel pozyskania tychże danych. Jako odrębną kwestię poddał w wątpliwość niezbędność przechowywania kserokopii dokumentów potwierdzających tożsamość po zakończeniu postępowania egzaminacyjnego.

Zakwestionowany został przepis § 17 ust. 1 projektu przewidujący czynność sprawdzania tożsamości osób zdających przez przewodniczącego zespołu nadzorującego przebieg egzaminów eksternistycznych z poszczególnych zajęć edukacyjnych, jednak bez określenia sposobu, jak również dokumentów, na podstawie których ta czynność jest dokonywana. Zapis o sprawdzeniu tożsamości osób zdających pojawia się również w treści § 29 ust. 2 projektu, jako jeden z elementów protokołu przebiegu egzaminu eksternistycznego wraz z określeniem „lista osób zdających” bez podania, jakie

³¹¹ Rozporządzenie wydawane na podstawie art. 10 ust. 5 ustawy z dnia 7 września 1991 r. o systemie oświaty, Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.

³¹² § 14 ust. 2 i 3 oraz § 29 ust. 2 projektu.

dane osobowe lista ta zawiera. Wobec powyższego Generalny Inspektor zaproponował zredagowanie treści zakwestionowanych przepisów w sposób niebudzący wątpliwości co do tego, w jaki sposób dokonuje się sprawdzenia tożsamości osoby zdającej oraz określenie, jakie dane osobowe zawiera lista osób zdających.

Uwaga dotycząca konieczności dochowania zasadzie tworzenia zamkniętych katalogów danych w przypadku pozyskiwania danych osobowych sformułowana w odniesieniu do projektu rozporządzenia w sprawie egzaminów eksternistycznych została również podniesiona wobec projektu ***rozporządzenia Ministra Edukacji Narodowej w sprawie publicznych placówek kształcenia ustawicznego, publicznych placówek kształcenia praktycznego i publicznych ośrodków dokształcania i doskonalenia zawodowego oraz kształcenia ustawicznego w formach pozaszkolnych***³¹³, w zakresie przepisów dotyczących treści skierowania³¹⁴ oraz zaświadczenia³¹⁵.

Organ do spraw ochrony danych osobowych nie pominął milczeniem kwestii, iż treść § 23 ust. 2 określającego, co stanowi dokumentację przebiegu kształcenia zakładaną dla każdej formy prowadzonego kształcenia, wydaje się przekraczać poza zakres delegacji ustawowej. Jednocześnie zasugerował, iż w przypadku podjęcia przez projektodawcę decyzji o pozostawieniu kwestionowanego przepisu, zaproponował, zgodnie z zasadą celowości, określenie, jakie dane osobowe przetwarzane są w ramach listy obecności wchodzącej w skład dziennika zajęć edukacyjnych. Natomiast w odniesieniu do rejestru wydanych zaświadczeń, o którym mowa w kwestionowanym przepisie § 23 ust. 2 pkt 4, Generalny Inspektor wskazał, iż zasadnym byłoby określenie jasnych zasad jego funkcjonowania.

W projekcie ***rozporządzenia Ministra Edukacji Narodowej zmieniającego rozporządzenie w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów i słuchaczy oraz przeprowadzania egzaminów w szkołach publicznych***³¹⁶ organ do spraw ochrony danych osobowych poddał w wątpliwość, sugerując potrzebę zmiany przepisów § 115 ust. 1 i § 115a ust. 1 projektu, dotyczących obowiązku złożenia deklaracji przystąpienia do egzaminu zawodowego na zasadach określonych w przepisach w sprawie egzaminów eksternistycznych oraz deklaracji do przystąpienia do egzaminu zawodowego jako egzaminu eksternistycznego poprzez wypełnienie formularza rejestracji. Projektodawca nie określił bowiem ani wzoru formularza, ani nie podał, jakie dane osób zdających będą na tę okoliczność przetwarzane.

Do Generalnego Inspektora został również przedłożony do zaopiniowania pakiet projektów rozporządzeń Ministra Sprawiedliwości, do których Generalny Inspektor Ochrony Danych Osobowych przedstawił istotne zastrzeżenia.

³¹³ Rozporządzenie wydawane na podstawie art. 68a ust. 5 i 6 ustawy z dnia 7 września 1991 r. o systemie oświaty, Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.

³¹⁴ § 12 ust. 2 projektu.

³¹⁵ § 13 projektu.

³¹⁶ Rozporządzenie wydawane na podstawie art. 22 ust. 2 pkt 4 ustawy z dnia 7 września 1991 r. o systemie oświaty.

W projekcie *rozporządzenia Ministra Sprawiedliwości w sprawie sposobu i trybu złożenia wniosku do Krajowego Rejestru Sądowego spółki, której umowę zawarto przy wykorzystaniu wzorca umowy spółki z ograniczoną odpowiedzialnością udostępnianego w systemie teleinformatycznym*³¹⁷ wątpliwości Generalnego Inspektora Ochrony Danych Osobowych o zasadniczym charakterze wzbudziła kwestia wiarygodności procesu uwierzytelniania osoby przygotowującej wniosek o wpis do rejestru spółki z ograniczoną odpowiedzialnością - której umowę zawarto przy wykorzystaniu wzorca tej spółki, udostępnianego w systemie teleinformatycznym. Z przepisów projektu wynika, iż wniosek o wpis spółki do rejestru może być opatrzony podpisem elektronicznym³¹⁸ składanym przez podanie nazwy użytkownika i hasła³¹⁹, który to mechanizm jest pozbawiony weryfikacji użytkownika w zakresie tego, czy jest osobą, której dane podał. Użycie w § 4 ust. 2 projektu sformułowania „podpis elektroniczny składa się przez podanie nazwy użytkownika i hasła” sugeruje, że podpis elektroniczny jest powiązaniem podpisywanego dokumentu z identyfikatorem i hasłem, zniekształcając tym samym pojęcie podpisu elektronicznego. Organ do spraw ochrony danych osobowych zwrócił uwagę, iż bardziej zasadne byłoby stwierdzenie w kwestionowanym przepisie, że do wykonania operacji złożenia podpisu elektronicznego wymagane jest podanie nazwy użytkownika oraz hasła.

Ponadto wątpliwość organu do spraw ochrony danych osobowych zrodził brak określenia w § 5 ust. 3 projektu, w jaki sposób miałyby nastąpić potwierdzenie tożsamości osoby podpisującej wniosek, która nie posiada statusu użytkownika. Skoro wniosek o wpis spółki do rejestru składa się przy wykorzystaniu systemu teleinformatycznego na udostępnionych w tym systemie formularzach³²⁰, a dostęp do tego systemu uzyskuje użytkownik przez swoje konto³²¹, to jedynym sposobem podpisania tego wniosku przez osobę, która nie posiada statusu użytkownika, byłaby jego fizyczna obecność w momencie wypełniania wniosku przez użytkownika i wpisanie tekstu na klawiaturze. W związku z czym powstała zasadnicza wątpliwość, czy taka w istocie była intencja projektodawcy, a jeśli tak - to jakie miałyby być mechanizmy weryfikacji tożsamości takich osób. Podniesionych wątpliwości nie rozwiewa treść innego przepisu projektu³²², gdzie mowa jest o innych użytkownikach mających podpisać wniosek, których „przy przygotowaniu wniosku należy wskazać”. Jeżeli przyjąć dopuszczenie podpisania wniosku przez inne osoby niż użytkownik przygotowujący wniosek, Generalny Inspektor podniósł w swej argumentacji, iż należałoby wprowadzić wiarygodny mechanizm weryfikacji tożsamości owych innych użytkowników.

³¹⁷ Rozporządzenie wydawane na podstawie delegacji zawartej w art. 19 ust. 7 ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym, Dz. U. z 2007 r. Nr 168, poz. 1186 z późn. zm.

³¹⁸ § 4 ust. 1 projektu.

³¹⁹ § 4 ust. 2 projektu.

³²⁰ § 3 ust. 1 projektu.

³²¹ § 3 ust. 2 projektu.

³²² § 6 ust. 2 projektu.

Odnosząc się do projektu *rozporządzenia Ministra Sprawiedliwości w sprawie trybu zakładania konta w systemie teleinformatycznym, sposobu korzystania z systemu teleinformatycznego i podejmowania w nim czynności związanych z zawiązaniem spółki z ograniczoną odpowiedzialnością przy wykorzystaniu wzorca umowy oraz wymagań dotyczących podpisu elektronicznego*³²³, Generalny Inspektor wskazał na niejasność użytego w nim w § 3 ust. 1 pkt 1 określenia „identyfikator dokumentu tożsamości” przy jednoczesnym braku, jakich danych będzie wymagał system teleinformatyczny służący do obsługi zawiązania spółki z ograniczoną odpowiedzialnością. W wątpliwość poddany został również projekt przepisu § 3 ust. 1 pkt 3 dotyczącego weryfikacji imienia, nazwiska oraz numeru PESEL w zbiorze PESEL przy zakładaniu konta w systemie teleinformatycznym. Nie wynika bowiem z niego, co jest przedmiotem weryfikacji - czy to, że osoba składająca wniosek, jest tą za którą się podaje, czy tylko fakt, że osoba o danym imieniu i nazwisku ma nadany, wskazany we wniosku numer PESEL i że dane te są zgodne między sobą. Organ do spraw ochrony danych osobowych wyjaśnił, że przy takiej konstrukcji przedmiotem weryfikacji może być tylko powiązanie określonej z imienia i nazwiska osoby ze wskazanym numerem PESEL i sprawdzenie, czy dane te występują w zbiorze PESEL, w związku z czym zaproponował stosowną zmianę brzmienia kwestionowanego przepisu. Jednocześnie wskazał, iż sposób weryfikowania danych składanych przez użytkownika przy zakładaniu konta (weryfikacja imienia, nazwiska oraz numeru PESEL w zbiorze PESEL) nie gwarantuje tego, że konta nie założy osoba podszywająca się pod inną osobę, podając jej imię i nazwisko oraz numer PESEL.

Uwagę Generalnego Inspektora zwrócił również fakt, iż projektowane przepisy dotyczące hasła w systemie teleinformatycznym służącym do obsługi zawiązania spółki i złożenia wniosku o jej wpis³²⁴, nie odnoszą się do minimalnych wymagań bezpieczeństwa, w związku z czym nie jest możliwe stwierdzenie, czy parametry stosowanych haseł spełniają minimalne wymagania w tym zakresie określone w przepisach, w tym w przepisach o ochronie danych osobowych. Powyższe skłoniło organ do spraw ochrony danych osobowych do zaproponowania uzupełnienia treści przepisu o stosowne określenie parametrów haseł. Treść zawarta w § 3 ust. 3 projektu nie daje podstaw do stwierdzenia, czy założenia dotyczące parametrów stosowanych haseł spełniają minimalne wymagania bezpieczeństwa określone w przepisach prawa (w tym w przepisach dotyczących ochrony danych osobowych).

Wątpliwości w treści projektu wzbudziło zastosowanie pojęcia podpisu elektronicznego do uwierzytelniania się. Z definicji podpisu elektronicznego zawartej w ustawie o podpisie

³²³ Rozporządzenie wydawane na podstawie delegacji zawartej w art. 157¹ § 6 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych, Dz. U. z 2000 r. Nr 94, poz. 1037 z późn. zm.

³²⁴ § 3 ust. 3 projektu.

elektronicznym³²⁵ wynika, że „podpis elektroniczny” zawiera w sobie informacje o określonych danych, np. nazwie użytkownika i hasle oraz dane identyfikujące użytkownika, które są z tymi poprzednimi danymi połączone. Projektodawca natomiast w treści przepisu dotyczącego podpisu elektronicznego³²⁶ stwierdził, iż podpis taki uzyskuje się podając tylko identyfikator i hasło; nie wskazał jednocześnie źródła, skąd ma być pobierana informacja o tożsamości użytkownika, która musi być znana, aby podpis został wykonany. Zgodnie ze znaczeniem pojęcia procesu uwierzytelniania się podczas procesu uzyskiwania dostępu do systemu informatycznego, przed wykonaniem tego procesu rejestrujący nie powinien mieć dostępu do jakichkolwiek danych osobowych zarejestrowanych w tym systemie. Samo podanie identyfikatora i hasła w procesie uwierzytelnienia nie zapewnia powiązania ich z danymi służącymi do wiarygodnej identyfikacji osoby składającej podpis elektroniczny. Stąd użycie pojęcia „podpis elektroniczny, który nie jest podpisem bezpiecznym weryfikowanym przy użyciu kwalifikowanego certyfikatu” jest nieuzasadnione. Opisanego w kwestionowanym przepisie mechanizmu nie można uznać za składanie podpisu elektronicznego, a jedynie za zwykły proces uwierzytelniania się przy użyciu identyfikatora i hasła. W procesie składania podpisu niezbędne są bowiem nie tylko identyfikator i hasło, ale dodatkowo klucz kryptograficzny do wykonania procesu podpisu. W przypadku podpisu bezpiecznego klucz ten pobiera się z wystawionego certyfikatu. Dla procesu opisanego w komentowanym przepisie nie wskazano, skąd ma być pobrany odpowiedni klucz i w związku z powyższym proces, który wykorzystuje tylko identyfikator i hasło, nie można nazwać podpisem elektronicznym.

Generalny Inspektor poczynił spostrzeżenie, iż z projektowanych przepisów nie wynika, w jaki sposób osoba nieposiadająca statusu użytkownika może podpisać formularz umowy spółki. Zgodnie z projektem podpisanie formularza jest możliwe tylko w systemie teleinformatycznym³²⁷, co oznacza, że operację tę może wykonać tylko użytkownik systemu. Jednocześnie inny przepis stanowi, iż osoba nieposiadająca statusu użytkownika może również podpisać umowę, jeżeli została wskazana w systemie teleinformatycznym przez użytkownika i jej tożsamość została potwierdzona przez użytkownika³²⁸. W projekcie nie wyjaśnia się, co oznacza pojęcie statusu użytkownika, w związku z tym należałoby uznać, iż osoba niemająca statusu użytkownika nie jest użytkownikiem systemu, a co za tym idzie – nie może wykonywać żadnych operacji w tym systemie. Zaniepokojenie organu do spraw ochrony danych osobowych wzbudził ponadto brak określenia w projekcie sposobu, w jaki

³²⁵ Zgodnie z definicją podpisu elektronicznego, zawartą w art. 3. ust. 1 ustawy z dnia 18 września 2011 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.), podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

³²⁶ § 5 ust 3 projektu.

³²⁷ § 6 ust. 1 projektu.

³²⁸ § 6 ust. 1 projektu.

miałoby nastąpić potwierdzenie przez użytkownika tożsamości osoby uprawnionej do podpisania umowy, nieposiadającej tego statusu.

GIODO wypowiedział się także na temat zgodności z przepisami o ochronie danych osobowych projektu **rozporządzenia Ministra Sprawiedliwości w sprawie zbierania informacji na temat używania przez oskarżonego środków odurzających, substancji psychotropowych lub środków zastępczych**³²⁹, co do którego w pierwszej kolejności podniósł, iż klauzula zgody³³⁰ na gromadzenie i przetwarzanie przez Krajowe Biuro do Spraw Przeciwdziałania Narkomanii danych tej osoby w celu umożliwienia wykonywania czynności, o których mowa w pkt 3), była zarówno zbędna, jak i wprowadzająca w błąd tę osobę, wnioskując o jej wykreślenie z projektu. Z chwilą dokonania wpisu do ewidencji osób uprawnionych do zebrania informacji na temat używania przez oskarżonego środków odurzających, substancji psychotropowych lub środków zastępczych przetwarzanie danych specjalisty terapii uzależnień odbywa się na podstawie i w trybie określonym przepisami prawa³³¹, nie zaś w oparciu o zgodę tej osoby.

Organ do spraw ochrony danych osobowych poddał ponadto w wątpliwość konstrukcję zgody badanego na przeprowadzenie wywiadu³³². Nie mogło bowiem umknąć uwadze Generalnego Inspektora Ochrony Danych Osobowych brzmienie aktów prawnych o randze wyższej, aniżeli opiniowany projekt, w myśl których oskarżony jest obowiązany poddać się oględzinom zewnętrznym ciała oraz innym badaniom niepołączonym z naruszeniem integralności ciała³³³, a także badaniom psychologicznym i psychiatrycznym³³⁴, jak również, że sąd, a w postępowaniu przygotowawczym prokurator, zarządza zebranie przez osoby, które na zasadach wskazanych w ustawie uzyskały certyfikat specjalisty terapii uzależnień, informacji na temat używania przez oskarżonego środków odurzających, substancji psychotropowych lub środków zastępczych”.³³⁵ Tym samym akty prawne wyższego rzędu nakładają na oskarżonego określone obowiązki.

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych zgłosił również uwagi do innych projektów aktów prawnych. Opiniując projekt **rozporządzenia Rady Ministrów zmieniającego rozporządzenie w sprawie programu badań statystycznych statystyki**

³²⁹ Rozporządzenie wydane na podstawie delegacji zawartej w art. 70a ust. 2 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii – Dz. U. Nr 179, poz. 1485 z późn. zm., dodany przez art. 1 pkt 17 ustawy z dnia 1 kwietnia 2011 r. o zmianie ustawy o przeciwdziałaniu narkomanii oraz niektórych innych ustaw, Dz. U. Nr 117, poz. 678.

³³⁰ Zamieszczona w pkt 4) załącznika nr 1 do opiniowanego projektu.

³³¹ W ustawie o przeciwdziałaniu narkomanii, ustawie z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego – Dz. U. Nr 89, poz. 555 z późn. zm., opiniowanym projekcie.

³³² Zaproponowanej w części wstępnej Kwestionariusza zebrania informacji przez SPECJALISTĘ TERAPII UZALEŻNIEŃ (załącznik nr 2 do opiniowanego projektu).

³³³ Art. 74 § 2 pkt 1 ustawy – Kodeks postępowania karnego.

³³⁴ Art. 74 § 2 pkt 2 ustawy – Kodeks postępowania karnego.

³³⁵ Art. 70a ust. 1 ustawy o przeciwdziałaniu narkomanii (dodany przez art. 1 pkt 17 ustawy o zmianie ustawy o przeciwdziałaniu narkomanii oraz niektórych innych ustaw).

*publicznej na rok 2011*³³⁶, podniósł wątpliwości dotyczące nowych unormowań dotyczących badań o symbolu 1.25.01(056) „Budżety gospodarstw domowych” i badania o symbolu 1.29.06(083) „Kadra medyczna ochrony zdrowia”. W przypadku obu tych badań³³⁷ projektodawca zaproponował bowiem wykorzystanie danych administracyjnych zebranych w ramach narodowego spisu powszechnego ludności i mieszkań w 2011 roku. Organ do spraw ochrony danych osobowych zakwestionował takie rozwiązanie ze względu na przepisy ustawy z dnia 4 marca 2010 r. o narodowym spisie powszechnym ludności i mieszkań w 2011 roku, które wprost zakazują wykorzystywania danych zgromadzonych w spisie dla celów innych niż określone w art. 10 ustawy o statystyce publicznej³³⁸, jak również nakazują usunięcie zgromadzonych w spisie danych dotyczących imienia i nazwiska, numeru PESEL, numeru identyfikacji podatkowej (NIP) i numeru telefonu oraz adresu nie później niż po upływie 2 lat od dnia zakończenia spisu³³⁹. Powyższe skłoniło Generalnego Inspektora do zaoponowania przeciwko zmianom wprowadzanym mocą kwestionowanych przepisów do załącznika do rozporządzenia Rady Ministrów z dnia 9 listopada 2010 r. w sprawie programu badań statystycznych statystyki publicznej na rok 2011 (Dz. U. Nr 239, poz. 1594 z późn. zm.).

W bieżącym okresie sprawozdawczym Generalny Inspektor zgłosił również istotne uwagi do projektu *rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej w sprawie szkolenia osób ubiegających się o uprawnienia do kierowania pojazdami, instruktorów i wykładowców*³⁴⁰. Po pierwsze zakwestionował przepis § 15 ust. 4 projektu nakładający na instruktorów obowiązek składania swoim pracodawcom oświadczeń na piśmie o wykonywaniu pracy w innym miejscu aniżeli ośrodek szkolenia kierowców, jako unormowanie nie mieszczące się w zakresie delegacji ustawowej oraz budzące zasadnicze wątpliwości co do zgodności z Konstytucją Rzeczypospolitej Polskiej.³⁴¹ Wyjątki od konstytucyjnej zasady wolności wyboru i wykonywania zawodu oraz wyboru miejsca pracy, jak również ograniczenia w zakresie korzystania z prawa do ochrony życia prywatnego i decydowania o swoim życiu osobistym wymagają bezwzględnie regulacji rangi ustawowej³⁴². Jeśli dodać do powyższego regulację art. 51 ust. 1 Konstytucji Rzeczypospolitej Polskiej³⁴³, to niezgodność z Konstytucją Rzeczypospolitej Polskiej tego rozwiązania jawiła się jako oczywista.

³³⁶ Rozporządzenie wydawane na podstawie delegacji zawartej w art. 18 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej, Dz. U. Nr 88, poz. 439 z późn. zm.

³³⁷ Odpowiednio § 1 pkt 3 lit. a i b oraz § 1 pkt 4 lit. a i b projektu.

³³⁸ Art. 10 ust. 3 zdanie pierwsze ustawy o statystyce publicznej.

³³⁹ Art. 10 ust. 6 ustawy o statystyce publicznej.

³⁴⁰ Rozporządzenie wydane na podstawie delegacji zawartej w art. 32 ust. 3 ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami, Dz. U. Nr 30, poz. 151 z późn. zm.

³⁴¹ Podkreślić należy, że Konstytucja Rzeczypospolitej Polskiej w art. 65 ust. 1 deklaruje wolność wyboru i wykonywania zawodu oraz wyboru miejsca pracy, zaś w art. 47 statuuje prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

³⁴² Art. 65 ust. 1 zdanie drugie oraz art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.

³⁴³ Nikt nie może być obowiązany do ujawniania informacji dotyczących jego osoby inaczej niż na podstawie ustawy.

Projekt ten jednocześnie, nie zawierając wzoru zaświadczenia potwierdzającego uczestnictwo w warsztatach doskonalenia zawodowego – którego obowiązek określenia w drodze rozporządzenia nakłada na ministra właściwego do spraw transportu ustawa o kierujących pojazdami³⁴⁴ - nie wykonywał w sposób wyczerpujący delegacji ustawowej. Organ do spraw ochrony danych osobowych zwrócił uwagę projektodawcy na konieczność poprawienia przepisu³⁴⁵ operującego w swojej treści niejednoznacznym pojęciem „dane osobowe” kandydata na instruktora lub instruktora, bez sprecyzowania, o jakie dane chodzi (z wyjątkiem wskazania, iż musi to być data urodzenia lub nr PESEL kandydata na instruktora lub instruktora – jeżeli kandydat na instruktora lub instruktor go posiada). Zaproponowane brzmienie pozwalałoby zatem na zamieszczanie w dzienniku lekcyjnym kursu, oprócz daty urodzenia/nr PESEL, dowolnych danych kandydata na instruktora lub instruktora. Takie sformułowanie przepisu pozostaje w sprzeczności z zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Marginesowo Generalny Inspektor wskazał, iż zmiana nazwy dokumentu stwierdzającego uprawnienia do kierowania tramwajem „pozwolenie na kierowanie tramwajem”, dokonana przez ustawodawcę w ustawie o kierujących pojazdami³⁴⁶, nie znalazła żadnego odzwierciedlenia w przedłożonym do zaopiniowania projekcie.

Opiniując projekt *rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej w sprawie egzaminowania osób ubiegających się o uprawnienia do kierowania pojazdami, szkolenia, egzaminowania i uzyskiwania uprawnień przez egzaminatorów oraz wzorów dokumentów stosowanych w tych sprawach*³⁴⁷ organ do spraw ochrony danych osobowych zgłosił uwagi do przepisu § 45 ust. 1 pkt 3 lit. b tiret pierwsze, posługującego się niedookreślonym pojęciem „dane osobowe” kandydata na egzaminatora lub egzaminatora, bez sprecyzowania, o jakie dane chodzi (z wyjątkiem wskazania, iż musi to być data urodzenia lub nr PESEL kandydata na egzaminatora lub egzaminatora – jeżeli kandydat na egzaminatora lub egzaminator go posiada). Takie brzmienie umożliwiałoby zamieszczanie w dzienniku lekcyjnym kursu, oprócz daty urodzenia/nr PESEL, dowolnych danych kandydata na egzaminatora lub egzaminatora, pozostając w sprzeczności z zasadą statuowaną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Względ na tę zasadę skłonił Generalnego Inspektora do konieczności uregulowania zakresu danych zamieszczanych w wykazie osób prowadzących zajęcia teoretyczne (§ 45 ust. 1 pkt 3 lit. b tiret trzecie projektu) oraz ewidencji osób przystępujących do egzaminu (§ 66 ust. 3 projektu). Opiniowany projekt zawierał również usterkę polegającą na nieuwzględnieniu w swojej treści zmiany nazwy dokumentu stwierdzającego posiadanie

³⁴⁴ Delegacja ustawowa z art. 40 ust. 1 pkt 3 lit. e ustawy o kierujących pojazdami.

³⁴⁵ § 27 pkt 3 lit. b tiret pierwsze projektu.

³⁴⁶ Art. 7 ust. 1 pkt 1 ustawy o kierujących pojazdami.

³⁴⁷ Rozporządzenie wydawane na podstawie delegacji zawartej w art. 66 ust. 1 pkt 1 – 5, 7 i 8 ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami, Dz. U. Nr 30, poz. 151 z późn. zm.

uprawnienia do kierowania tramwajem, wynikającą z ustawy o kierujących pojazdami, na „pozwolenie na kierowanie tramwajem”.³⁴⁸ Ponadto katalog danych osobowych, które mają być zamieszczane w zaświadczeniu potwierdzającym uczestnictwo w warsztatach doskonalenia zawodowego egzaminatorów³⁴⁹, poprzedzony został sformułowaniem „co najmniej” i zyskał w ten sposób charakter otwarty, co także prowadzić może do naruszenia – powoływanej wyżej – zasady adekwatności, w związku z czym Generalny Inspektor zasugerował usunięcie tego sformułowania z przepisu.

Zasadnicze wątpliwości Generalnego Inspektora wzbudził przedłożony mu do zaopiniowania projekt *rozporządzenia Ministra Zdrowia w sprawie sposobu i trybu prowadzenia rejestru ukaranych pielęgniarek i położnych oraz sposobu i trybu wykonywania prawomocnych orzeczeń sądów pielęgniarek i położnych*³⁵⁰. W pierwszej kolejności organ do spraw ochrony danych osobowych wskazał, iż nie wykonuje prawidłowo delegacji z ustawy o samorządzie pielęgniarek i położnych. Z jednej strony bowiem znalazły się w jego treści przepisy wykraczające poza zakres tej delegacji³⁵¹, z drugiej zaś – brak jest unormowań, których można by oczekiwać w akcie prawnym mającym uregulować: „sposób i tryb prowadzenia rejestru ukaranych pielęgniarek i położnych”.³⁵²

W myśl delegacji ustawowej przedmiotem unormowania w przedstawionym do zaopiniowania projekcie ma być sposób i tryb prowadzenia rejestru ukaranych pielęgniarek i położnych oraz sposób i tryb wykonania prawomocnych orzeczeń sądów pielęgniarek i położnych. Tymczasem – odmiennie aniżeli ma to miejsce w przypadku przewodniczącego właściwej okręgowej rady pielęgniarek i położnych³⁵³, któremu projekt nadaje pewne kompetencje w zakresie wykonania orzeczeń sądów pielęgniarek i położnych³⁵⁴ – żaden z podmiotów wskazanych w projektowanej regulacji – tj. minister właściwy do spraw zdrowia³⁵⁵ oraz Prezes Naczelnej Rady Pielęgniarek i Położnych³⁵⁶ – nie jest organem uprawnionym do podejmowania rozstrzygnięć w postępowaniu wykonawczym toczącym się po uprawomocnieniu orzeczenia sądu pielęgniarek i położnych. Generalny Inspektor, nie negując zatem praktycznej potrzeby doręczania ministrowi właściwemu do spraw zdrowia oraz Prezesowi Naczelnej Rady Pielęgniarek i Położnych prawomocnych orzeczeń sądu pielęgniarek i położnych, stwierdził, iż zaproponowana konstrukcja prawna nie dotyczy kwestii wykonywania prawomocnych orzeczeń sądów pielęgniarek i położnych, a zatem nie powinna być zamieszczona w projekcie.

³⁴⁸ Art. 7 ust. 1 pkt 1 ustawy o kierujących pojazdami, do którego treści odwołuje się zresztą § 2 pkt 2 projektu.

³⁴⁹ Określony w § 56 ust. 1 projektu.

³⁵⁰ Rozporządzenie na podstawie delegacji zawartej w art. 87 ustawy z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych, Dz. U. Nr 174, poz. 1038.

³⁵¹ Zarzut przekroczenia delegacji ustawowej odnosi się do § 3 ust. 1 pkt 2 i ust. 2 projektu.

³⁵² Art. 87 pkt 1 ustawy o samorządzie pielęgniarek i położnych oraz § 1 pkt 1 projektu.

³⁵³ zob. § 3 ust. 1 pkt 1 projektu.

³⁵⁴ zob. § 5 ust. 2, § 7 ust. 2, § 9 i § 10.

³⁵⁵ Art. 73 ust. 1 ustawy o samorządzie pielęgniarek i położnych w zw. z § 3 ust. 1 pkt 2 projektu.

³⁵⁶ Art. 73 ust. 1 ustawy o samorządzie pielęgniarek i położnych w zw. z § 3 ust. 1 pkt 2 projektu.

Za jeszcze bardziej niezrozumiałe organ do spraw ochrony danych osobowych uznał wprowadzenie do analizowanego projektu przepisu § 3 ust. 2, regulującego sposób postępowania po uchyleniu prawomocnego orzeczenia sądu pielęgniarek i położnych, a więc niepozostającego w jakimkolwiek związku z zagadnieniem wykonywania prawomocnych orzeczeń sądów pielęgniarek i położnych. Co więcej – w opinii organu do spraw ochrony danych osobowych unormowanie to, jako dotyczące doręczania wyroków Sądu Najwyższego, a więc przetwarzania danych szczególnie chronionych, powinno być zamieszczone w przepisie rangi ustawowej (art. 27 ust. 2 pkt 1 ustawy o ochronie danych osobowych), nie zaś w rozporządzeniu.

Generalny Inspektor wskazał również, iż wysoce kontrowersyjny jest sposób zrealizowania w projekcie wytycznej zawartej w delegacji ustawowej³⁵⁷, albowiem zagadnieniu rejestru ukaranych pielęgniarek i położnych poświęcony został zaledwie jeden lakoniczny przepis § 2 projektu, w którym przesądzono jedynie, że rejestr ten będzie prowadzony w systemie teleinformatycznym. Pominięto zaś milczeniem choćby kwestię przekazywania danych (informacji) do tego rejestru (np. kto przekazuje i w jaki sposób), jak również zasady udostępniania danych z rejestru. Zauważyć zaś wypada, iż ustawa o samorządzie pielęgniarek i położnych określiła tylko katalog danych zamieszczanych w rejestrze ukaranych pielęgniarek i położnych³⁵⁸, okres przechowywania tych danych³⁵⁹ oraz ogólną przesłankę udostępnienia danych z rejestru³⁶⁰, w pozostałym zakresie przekazując sprawę rejestru ukaranych pielęgniarek i położnych do unormowania w rozporządzeniu. Z nieznanych powodów projektodawca zdecydował jednak, by zaniechać regulowania w projekcie wskazanej wyżej problematyki, a informacje o ukaraniu pielęgniarki (położnej) gromadzić w okręgowych rejestrach pielęgniarek i położnych prowadzonych na podstawie przepisu ustawy o zawodach pielęgniarki i położnej³⁶¹. Takie brzmienie przepisów projektu – w ocenie organu do spraw ochrony danych osobowych – nie tylko pozostaje w sprzeczności z ustawą o samorządzie pielęgniarek i położnych³⁶², lecz jest również niezgodne z przepisami ustawy o zawodach pielęgniarki i położnej³⁶³, które stanowią, że w okręgowych rejestrach pielęgniarek i położnych mogą być zamieszczane tylko informacje o: ograniczeniu w wykonywaniu zawodu³⁶⁴, zawieszeniu prawa wykonywania zawodu³⁶⁵ i skreśleniu z rejestru pielęgniarek lub rejestru położnych³⁶⁶. Tymczasem projekt przewiduje³⁶⁷, że w okręgowych rejestrach pielęgniarek i położnych miałyby się także znaleźć informacje o ukaraniu: karą

³⁵⁷ Z art. 87 pkt 1 ustawy o samorządzie pielęgniarek i położnych.

³⁵⁸ Art. 85 ust. 2 ustawy o samorządzie pielęgniarek i położnych.

³⁵⁹ Art. 86 ust. 1 ustawy o samorządzie pielęgniarek i położnych.

³⁶⁰ „Interes prawny” – art. 85 ust. 1 zdanie drugie ustawy o samorządzie pielęgniarek i położnych.

³⁶¹ Art. 48 ustawy z dnia 15 lipca 2011 roku o zawodach pielęgniarki i położnej (Dz. U. Nr 174, poz. 1039) – § 4 projektu.

³⁶² Dyspozycja art. 87 ustawy o samorządzie pielęgniarek i położnych.

³⁶³ Z art. 48 ust. 1 i 2 w zw. z art. 44 ust. 1 ustawy o zawodach pielęgniarki i położnej.

³⁶⁴ Art. 48 ust. 1 i ust. 2 zdanie pierwsze w zw. z art. 44 ust. 1 pkt 13.

³⁶⁵ Art. 48 ust. 1 i ust. 2 zdanie pierwsze w zw. z art. 44 ust. 1 pkt 23.

³⁶⁶ Art. 48 ust. 1 i ust. 2 zdanie pierwsze w zw. z art. 44 ust. 1 pkt 26.

³⁶⁷ § 4 projektu.

upomnienia³⁶⁸, karą nagany³⁶⁹, karą pieniężną³⁷⁰, karą zakazu pełnienia funkcji kierowniczych w podmiotach leczniczych przez okres wskazany w prawomocnym orzeczeniu sądu pielęgniarek i położnych³⁷¹ i karą zakazu pełnienia funkcji z wyboru w organach samorządu przez okres wskazany w prawomocnym orzeczeniu sądu pielęgniarek i położnych.³⁷² Projektowane rozporządzenie nie dość zatem, iż w sposób sprzeczny z zasadą hierarchiczności aktów prawnych wprowadza zmiany do ustawy o zawodach pielęgniarki i położnej, to czyni w istocie zbędną zamieszczoną w ustawie o samorządzie pielęgniarek i położnych regulację dotyczącą rejestru ukaranych pielęgniarek i położnych.

W przedstawionym do zaopiniowania w 2011 r. projekcie *rozporządzenia Ministra Infrastruktury w sprawie wzorów i sposobu prowadzenia w formie elektronicznej centralnych rejestrów osób posiadających uprawnienia budowlane, rzeczoznawców budowlanych oraz ukaranych z tytułu odpowiedzialności zawodowej w budownictwie*³⁷³ wątpliwości Generalnego Inspektora wzbudziła pozycja zawarta w karcie osobowej, karcie zawodowej osoby posiadającej uprawnienia budowlane oraz karcie zawodowej rzeczoznawcy budowlanego – „Uwagi”. Jednocześnie o zakresie danych i informacji zamieszczanych w rejestrach osób posiadających uprawnienia budowlane, rzeczoznawców budowlanych przesądza przepis ustawy – Prawo budowlane³⁷⁴, nie przewidując możliwości zbierania dodatkowych, bliżej nieokreślonych informacji. Jedynie w odniesieniu do rejestru ukaranych z tytułu odpowiedzialności zawodowej w budownictwie, ustawa – Prawo budowlane³⁷⁵ precyzuje, iż w zakresie informacji o nałożonej karze z tytułu odpowiedzialności zawodowej obejmującej dane identyfikujące decyzję o nałożeniu kary oraz dane dotyczące nałożonej kary mieszczą się inne uwagi dotyczące kary. Przez wzgląd na statuowaną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych zasadę adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane, organ do spraw ochrony danych osobowych zasugerował zatem usunięcie z przedmiotowych kart wzmiankowaną pozycję, tak aby zapobiec zbieraniu na podstawie analizowanych przepisów danych osób w zakresie szerszym niż - po pierwsze- przewidział to ustawodawca, a po drugie - niż jest to konieczne dla celu przetwarzania gromadzonych danych.

³⁶⁸ Art. 60 ust. 1 pkt 1 ustawy o samorządzie pielęgniarek i położnych w zw. z § 4 projektu.

³⁶⁹ Art. 60 ust. 1 pkt 2 ustawy o samorządzie pielęgniarek i położnych w zw. z § 4 projektu.

³⁷⁰ Art. 60 ust. 1 pkt 3 ustawy o samorządzie pielęgniarek i położnych w zw. z § 4 projektu.

³⁷¹ Art. 60 ust. 1 pkt 4 ustawy o samorządzie pielęgniarek i położnych w zw. z § 4 projektu.

³⁷² Art. 60 ust. 1 pkt 5 ustawy o samorządzie pielęgniarek i położnych w zw. z § 4 projektu.

³⁷³ Rozporządzenie wydawane na podstawie delegacji zawartej w art. 88a ust. 6 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane, Dz. U. z 2010 r. Nr 243, poz. 1623 z późn. zm.

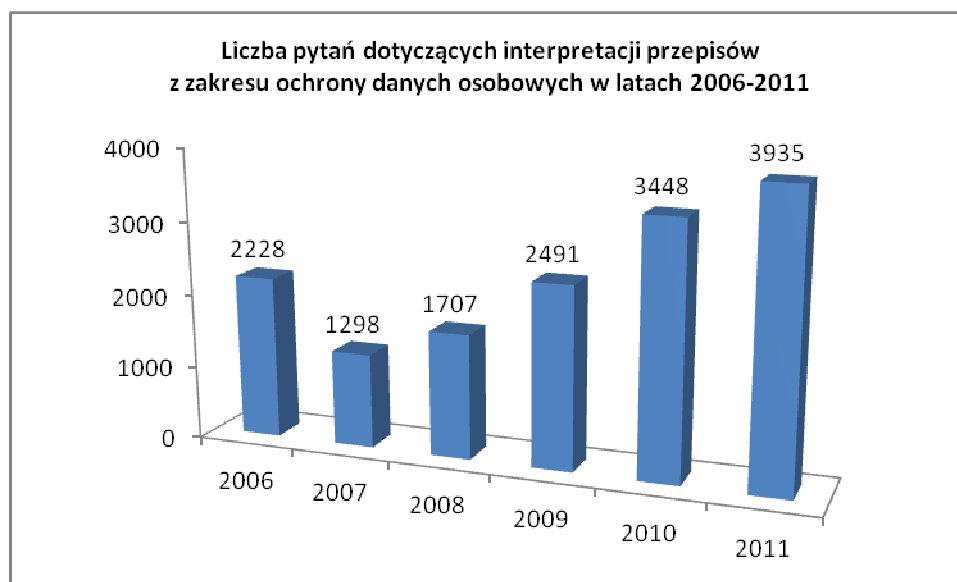
³⁷⁴ Art. 88a ust. 2 ustawy – Prawo budowlane.

³⁷⁵ Art. 88a ust. 4 ustawy – Prawo budowlane.

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 2011 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **3935 pytań prawnych** z prośbą o interpretację obowiązujących w obszarze ochrony danych osobowych przepisów prawa, bądź sygnalizujących różnego rodzaju problemy interpretacyjne związane z ich przestrzeganiem. Należy zaznaczyć, że w roku 2010 wpłynęło 3448 pytań z zakresu ochrony danych osobowych, zaś w 2009 r. – 2491, co jednoznacznie wskazuje na systematyczny wzrost zainteresowania obywateli oraz instytucji prywatnych i publicznych problematyką przetwarzania danych osobowych i jest wynikiem powszechnej świadomości w kwestiach związanych z koniecznością prawidłowego ich przetwarzania. Porównanie liczby pytań skierowanych do Generalnego Inspektora w latach 2009–2011 przedstawia Wykres 40.



Wykres 40: Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GIODO w latach 2009–2011.

W porównaniu z ubiegłym rokiem, w okresie objętym sprawozdaniem o 487 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 działania popularyzujące ideę

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”.

6.1. Interpretacja przepisów

Przedstawiona poniżej analiza **pytań prawnych**, które w 2011 r. wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych, w głównej mierze dotyczyć będzie problematyki przetwarzania wrażliwych danych osobowych w sektorze medycznym. Natomiast drugą grupę będą stanowiły te wybrane pytania prawne, które z uwagi na treść odnoszą się do bardzo różnorodnych zagadnień.

6.1.1. Odpowiedzi na pytania traktujące o danych wrażliwych dotyczących stanu zdrowia

W roku 2011 Generalny Inspektor Ochrony Danych Osobowych analizował szereg istotnych zagadnień dotyczących przetwarzania danych szczególnie chronionych dotyczących stanu zdrowia.

Jedno z pierwszych pytań tego typu zawierało prośbę o wydanie opinii prawnej **w sprawie przekazywania Ministrowi Zdrowia przez jednostkę podległą, danych osobowych pacjentów leczonych antywirusowo w ramach programu zdrowotnego "Leczenie antyretrowirusowe osób żyjących z wirusem HIV w Polsce w latach 2010 – 2011"**.³⁷⁶ W odpowiedzi Generalny Inspektor zwrócił uwagę na brak prawidłowych podstaw prawnych dla przetwarzania w ten sposób danych osobowych osób zakażonych HIV i chorych na AIDS. Wskazał na brak podstawy prawnej zarówno dla prowadzenia ogólnopolskiej bazy powyższych danych przez Krajowe Centrum ds. AIDS, jak i ewentualnego ich przekazywania Ministerstwu Zdrowia. W opinii przedstawiono stanowisko, że podstawy takiej nie stanowią regulacje prawne nie mające rangi ustawowej, w tym wskazane, ale nieobowiązujące już rozporządzenia Rady Ministrów z dnia 13 września 2005 r. w sprawie Krajowego Programu Zwalczania AIDS i zapobiegania zakażeniom HIV (Dz. U. Nr 189, poz. 1590). Wobec jednoznacznej dyspozycji art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych dla prowadzenia opisaną w pytaniu bazy danych, konieczne jest istnienie przepisu ustawy spełniającego określone kryteria³⁷⁷. Generalny Inspektor zauważył, że w celu zapewnienia takich gwarancji normy ustawowe powinny określać zakres danych, podmioty uprawnione do ich przetwarzania, w tym zasady ich udostępniania. Rozporządzenie natomiast może jedynie konkretyzować regulacje ustawowe, nie zaś stanowić samoistną podstawę dla przetwarzania danych tzw. szczególnie chronionych. Podsumowując swoje rozważania Generalny Inspektor stwierdził, że przetwarzanie danych w „komputerowym

³⁷⁶ DOLiS-035- 174/11/6546

³⁷⁷ Zgodnie z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych szczególnie chronionych, do jakich należą dane o stanie zdrowia, jest dopuszczalne, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

systemie bazy danych” prowadzonym przez Krajowe Centrum ds. AIDS odbywa się bez zachowania niezbędnych gwarancji wymaganych w przypadku przetwarzania danych szczególnie chronionych. Z uwagi na powyższe wyrażono nadzieję, że przedstawiony problem wynikający z potrzeby monitorowania przez Ministra Zdrowia wykorzystania i dystrybucji leków antyretrowirusowych, spowoduje niezwłoczne podjęcie przez Ministra działań dostosowujących przetwarzanie danych osobowych w przedmiotowej bazie do przepisów ustawy o ochronie danych osobowych poprzez stworzenie stosownych podstaw prawnych do wykonywania operacji na danych wrażliwych. Zadeklarowano również współpracę w tym zakresie, jako że organ do spraw ochrony danych osobowych ma nie tylko prawo, ale wręcz obowiązek opiniowania projektów aktów prawnych dotyczących ochrony danych osobowych, jak również inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Do Generalnego Inspektora Ochrony Danych Osobowych skierowało także **pytanie Centrum Medyczne Sp. z o. o. dotyczące wniosku komendanta policji o udostępnienie ze zbioru danych Centrum Medycznego pełnej listy zadeklarowanych w przychodni pacjentów.**³⁷⁸ W odpowiedzi Generalny Inspektor wskazał, że zasady gromadzenia danych przez Policję są przedmiotem regulacji odrębnych w stosunku do ustawy o ochronie danych osobowych. Podstawę prawną dla takich działań Policji - jako organu prowadzącego postępowanie karne - może stanowić art. 15 K.p.k., który nakłada na wszystkie instytucje państwowe i samorządowe obowiązek udzielania w zakresie swego działania pomocy organom prowadzącym postępowanie karne w terminie wyznaczonym przez te organy. Generalny Inspektor zaznaczył, że pomoc ta ogranicza się „wyłącznie do procesu karnego, ale „rozumianego szeroko - poczynając od postępowania sprawdzającego, lecz z wyłączeniem czynności operacyjno-rozpoznawczych”³⁷⁹ dokonywanych m.in. na podstawie przepisów ustawy z dnia 6 kwietnia 1990 r. o Policji (t. j. Dz. U. 2007 r. Nr 43, poz. 277 z późn. zm.). Niewątpliwie podmiot występujący o udostępnienie określonych informacji powinien w sposób prawidłowy wskazać podstawę prawną upoważniającą go do uzyskania danych. W załączonym do pisma wniosku prawdopodobnie zamiast powołanego powyżej art. 15 K.p.k. omyłkowo podany został art. 15 Kodeksu karnego. Generalny Inspektor pouczył, że w sytuacjach, gdy skierowane do administratora danych żądanie udzielenia danych osobowych budzi wątpliwości pod względem jego podstaw prawnych, dobrym rozwiązaniem może być zwrócenie się do Policji z prośbą o wyjaśnienie tych wątpliwości. Oprócz przepisów Kodeksu postępowania karnego obowiązek udzielenia pomocy Policji przy realizacji zadań ustawowych określają także inne ustawy. Zgodnie z art. 14 ust. 1 ustawy o Policji w granicach swych zadań Policja w celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń wykonuje czynności: operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-

³⁷⁸ DOLiS-035-1992/11/31666

³⁷⁹ por. Kodeks postępowania karnego. Komentarz. Warszawa 2008, Wydawnictwo Prawnicze LexisNexis.

porządkowe. Policjanci wykonując czynności, o których mowa w art. 14, mają prawo m.in. żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i jednostki obowiązane są, w zakresie swojego działania, do udzielenia tej pomocy, w zakresie obowiązujących przepisów prawa (art. 15 ust. 1 pkt 6). Zgodnie z art. 20 ust. 2a ustawy o Policji, Policja może pobierać, uzyskiwać, gromadzić, przetwarzać i wykorzystywać w celu realizacji zadań ustawowych informacje, w tym dane osobowe, o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osobach o nieustalonej tożsamości lub usiłujących ukryć swoją tożsamość oraz o osobach poszukiwanych, także bez ich wiedzy i zgody. Informacje, do przetwarzania których uprawniona jest Policja - zgodnie z ust. 2b cytowanego artykułu - mogą obejmować m.in. dane osobowe, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych, z tym że dane dotyczące kodu genetycznego wyłącznie o niekodujących regionach genomu.

W omawianym 2011 roku Generalny Inspektor odpowiedział również na **pytanie, czy wypełniony przez lekarza Druk ZUS ZLA, a w tym jego odpowiednia kopia przekazywana przez pracownika do pracodawcy oraz posła na Sejm RP to dokument zawierający wrażliwe dane osobowe wskazujący na stan zdrowia**. W odpowiedzi³⁸⁰ Generalny Inspektor podniósł, że art. 27 ust. 1 ustawy o ochronie danych osobowych wskazuje szczególne typy danych osobowych, określane powszechnie w piśmiennictwie jako wrażliwe dane osobowe albo dane szczególnie chronione. Katalog danych wrażliwych ma charakter zamknięty i obejmuje dane m.in. o stanie zdrowia. Organ do spraw ochrony danych osobowych wskazał przy tym, że Europejski Trybunał Sprawiedliwości (ETS) uznał, że informacja o zranieniu się osoby fizycznej w stopę i przebywaniu na zwolnieniu lekarskim jest informacją o stanie zdrowia w rozumieniu art. 8 ust. 1 dyrektywy 95/46/WE³⁸¹. Ponadto Generalny Inspektor zaznaczył, że art. 27 jest *lex specialis* względem art. 23 ustawy o ochronie danych osobowych. Wprawdzie także ustanawia zakaz przetwarzania danych osobowych, to jednak odmiennie reguluje przesłanki uchylające ten zakaz. Zakaz przetwarzania wrażliwych danych osobowych zostaje uchylony w wyniku spełnienia przez administratora danych którejkolwiek z przesłanek wymienionych w art. 27 ust. 2. Przetwarzanie wrażliwych danych osobowych jest legalne wówczas, gdy - na przykład jest - niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie. Zakresem zastosowania omawianej przesłanki objęte jest nie tylko zatrudnienie typu pracowniczego, lecz także inne typy stosunków zatrudnienia, np. cywilnoprawne, ustrojowe czy administracyjnoprawne.

³⁸⁰ DOLIS-035-751/11/18597

³⁸¹ Wyrok ETS z dnia 20 listopada 2003 r. w sprawie *Bodil Lindqvist*, Zb. Orz. 2003, nr 11A, s. I-12971.

Generalny Inspektor podkreślił, że w pracowniczych stosunkach zatrudnienia należy uwzględnić ograniczenia wynikające z innych przepisów, w szczególności z art. 22¹ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) i powołał treść art. 27 ust. 2 pkt 6. Dodał również, że na podstawie art. 22¹ § 4 Kodeksu pracy pracodawca może żądać podania innych danych osobowych niż wymienione, jeżeli obowiązek ich podania wynika z odrębnych przepisów. Od pracownika pracodawca może natomiast żądać dodatkowo innych danych osobowych, a także imion i nazwisk oraz dat urodzenia jego dzieci, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, a także numeru PESEL pracownika. Źródłem uprawnień pracownika są nie tylko przepisy szczególne w stosunku do Kodeksu Pracy, lecz także postanowienia zawarte w autonomicznych źródłach prawa pracy. Przykładem przepisów nakładających na pracownika obowiązek podania wrażliwych danych osobowych są przepisy ustawy z 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby lub macierzyństwa (t. j. Dz. U. z 2005 r. Nr 31, poz. 267 z późn. zm.), w szczególności jej art. 62 ust. 1.³⁸² W związku z powyższym, jeśli administrator danych przetwarza dane osobowe, w tym określane powszechnie w piśmiennictwie jako wrażliwe dane osobowe albo dane szczególnie chronione, to spoczywa na nim – stosownie do przepisów o ochronie danych osobowych – szereg obowiązków wskazanych w tej ustawie, zaś w przypadku przetwarzania danych w systemie informatycznym – w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) - powinien również przestrzegać zasad przetwarzania danych osobowych określonych w przepisach odrębnych.

Kolejne istotne pytanie **dotyczyło udzielania informacji o stanie zdrowia nieprzytomnego pacjenta**. W odpowiedzi³⁸³ Generalny Inspektor wskazał regulacje prawne zawarte w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t. j. Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.) – m.in. przepisy rozdziałów 3 i 4 czy też art. 26³⁸⁴ oraz w rozporządzeniu Ministra

³⁸² Ubezpieczony obowiązany jest dostarczyć płatnikowi zasiłków bądź składek (pracodawcy) zaświadczenie lekarskie o czasowej niezdolności do pracy z powodu choroby lub pobytu w stacjonarnym zakładzie opieki zdrowotnej nie później niż w ciągu 7 dni od daty jego otrzymania. Wzór takiego zaświadczenia określają przepisy rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 1 października 2010 r. zmieniające rozporządzenie w sprawie szczegółowych zasad i trybu wystawiania zaświadczeń lekarskich, wzoru zaświadczenia lekarskiego i zaświadczenia lekarskiego wydanego w wyniku kontroli lekarza orzecznika Zakładu Ubezpieczeń Społecznych, Dz. U. z 2010 r. Nr 189, poz. 1270.

³⁸³ DOLiS-035-3313/61850

³⁸⁴ Art. 26 ust. 1. Podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta. 2. Po śmierci pacjenta, prawo wglądu w dokumentację medyczną ma osoba upoważniona przez pacjenta za życia. 3. Podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną również: 1) podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych; 2) organom władzy publicznej, Narodowemu Funduszowi Zdrowia, organom samorządu zawodów medycznych oraz konsultantom krajowym i wojewódzkim, w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności kontroli i nadzoru; 2a) podmiotom, o których mowa w art.

Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. Nr 252, poz. 1697) – m.in. § 75, czy też przepisy rozdziału 7. Poinformował również, że na gruncie ustawy o ochronie danych osobowych, stosownie do jej postanowień zawartych w art. 26 ust. 1, administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Ta generalna zasada znajduje swoje rozwinięcie w przepisach ustawy określających m.in. wymogi, jakie powinien spełnić administrator w celu zapewnienia bezpieczeństwa danych w procesie ich przetwarzania. Ponadto zwrócił uwagę na treść art. 36 ust. 1 ustawy o ochronie danych osobowych.³⁸⁵ Organ do spraw ochrony danych osobowych podkreślił, że dobór odpowiednich środków powinien uwzględniać charakter przetwarzanych danych. Oznacza to, że w przypadku danych tzw. „sensytywnych”, wymienionych w art. 27 ust. 1 ustawy (np. danych o stanie zdrowia), zastosowane środki powinny zapewniać im bardziej intensywną ochronę. Niemniej jednak zgodnie z art. 27 ust. 2 pkt 3 ustawy przetwarzanie szczególnie chronionych danych osobowych jest dopuszczalne, jeżeli 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. Generalny Inspektor przypomniał, iż „żywotnymi interesami” są w tym przypadku kwestie związane z ochroną życia, zdrowia i bezpieczeństwa osobistego. Istotne jest zatem – dla oceny możliwości zastosowania ww. przesłanki – aby przetwarzanie danych było niezbędne w określonej sytuacji faktycznej do ochrony żywotnych interesów osoby fizycznej, a ponadto, aby osoba, której dane dotyczą, lub inna osoba, nie były w stanie udzielić zgody na piśmie, tj. przynajmniej podpisać sporządzonego uprzednio oświadczenia, lub wyrazić prawnie skutecznej zgody z uwagi na okoliczność,

119 ust. 1 i 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, w zakresie niezbędnym do przeprowadzenia kontroli na zlecenie ministra właściwego do spraw zdrowia; 3) ministrowi właściwemu do spraw zdrowia, sądom, w tym sądom dyscyplinarnym, prokuraturom, lekarzom sądowym i rzecznikom odpowiedzialności zawodowej, w związku z prowadzonym postępowaniem; 4) uprawnionym na mocy odrębnych ustaw organom i instytucjom, jeżeli badanie zostało przeprowadzone na ich wniosek; 5) organom rentowym oraz zespołom do spraw orzekania o niepełnosprawności, w związku z prowadzonym przez nie postępowaniem; 6) podmiotom prowadzącym rejestry usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów; 7) zakładom ubezpieczeń, za zgodą pacjenta; 8) lekarzowi, pielęgniarce lub położnej, w związku z prowadzeniem procedury oceniającej podmiot udzielający świadczeń zdrowotnych na podstawie przepisów o akredytacji w ochronie zdrowia, w zakresie niezbędnym do jej przeprowadzenia; 9) wojewódzkiej komisji do spraw orzekania o zdarzeniach medycznych, o której mowa w art. 67e ust. 1, w zakresie prowadzonego postępowania; 10) spadkobiercom w zakresie prowadzonego postępowania przed wojewódzką komisją do spraw orzekania o zdarzeniach medycznych, o której mowa w art. 67e ust. 1; 11) osobom wykonującym czynności kontrolne na podstawie art. 39 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657), w zakresie niezbędnym do ich przeprowadzenia. 4. Dokumentacja medyczna może być udostępniona także szkole wyższej lub instytutowi badawczemu do wykorzystania w celach naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy.

³⁸⁵ Art. 36 ust. 1 stanowi, że administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

iż nie są w stanie działać z rozeznaniem, oraz by nie miały opiekuna prawnego lub kuratora³⁸⁶. Niewywiązanie się z powyższych obowiązków może w konsekwencji prowadzić do powstania odpowiedzialności karnej na podstawie art. 51 i 52 ustawy.³⁸⁷ Rozważając możliwość telefonicznego przekazywania informacji o stanie zdrowia pacjenta należy mieć zatem na uwadze powyższe regulacje. Niewątpliwie do takiej formy udzielania informacji należy podchodzić z dużą dozą ostrożności. Generalny Inspektor podkreślił, że aby wykluczyć w tym przypadku ryzyko udostępnienia danych osobowych osobom do tego nieupoważnionym, należy zapewnić określone mechanizmy służące dostatecznej weryfikacji tożsamości rozmówcy i jego uprawnienia do uzyskiwania informacji o pacjencie (np. poprzez podanie umówionego hasła).

Generalny Inspektor z własnej inicjatywy skierował również pisma mające na celu zmianę praktyk podejmowanych przez administratorów danych bądź sugerujące potrzebę dokonania zmian w przepisach prawa.

Jednym z pierwszych takich stanowisk było **pismo z dnia 14 stycznia 2011 r. kierowane do Ministra Zdrowia³⁸⁸ traktujące o przetwarzaniu danych osobowych pacjentów w związku z opieką farmaceutyczną, polegającą na czuwaniu przez farmaceutę nad prawidłowym przebiegiem farmakoterapii, w celu uzyskania określonych jej efektów poprawiających jakość życia pacjenta**. Po weryfikacji przepisów - przede wszystkim ustawy z dnia 19 kwietnia 1991 r. o izbach aptekarskich (t. j.: Dz. U. z 2008 r. Nr 136, poz. 856 z późn. zm.) - Generalny Inspektor uznał, iż przepisy te wskazując na możliwość sprawowania przez farmaceutów opieki farmaceutycznej nad pacjentem, nie regulują kwestii przetwarzania danych osobowych pacjenta przez takiego farmaceutę. Stosownie bowiem do art. 2a ust. 1 pkt 7 ustawy o izbach aptekarskich, wykonywanie zawodu farmaceuty ma na celu ochronę zdrowia publicznego i obejmuje udzielanie usług farmaceutycznych polegających w szczególności na: sprawowaniu opieki farmaceutycznej polegającej na dokumentowanym procesie, w którym farmaceuta, współpracując z pacjentem i lekarzem, a w razie potrzeby z przedstawicielami innych zawodów medycznych, czuwa nad prawidłowym przebiegiem farmakoterapii w celu uzyskania określonych jej efektów poprawiających jakość życia pacjenta. Analizując przedmiotowy problem, organ do spraw ochrony danych osobowych zwrócił uwagę na szeroko rozumiane prawo do prywatności oraz gwarancje wynikające z przepisów Konstytucji

³⁸⁶ A. Drozd, Najnowsze wydanie: Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Warszawa 2008, Wydawnictwo Prawnicze LexisNexis, wydanie IV, s. 504.

³⁸⁷ Art. 51 ust. 1 i 2, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Art. 52, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabránieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

³⁸⁸ DOLiS-035-80/11/ 1600

Rzeczypospolitej Polskiej.³⁸⁹ Wskazał również wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r.³⁹⁰ traktujący o działaniach państwa ingerujących w wolności obywatelskie.³⁹¹ Generalny Inspektor Ochrony Danych Osobowych zauważył, że z art. 2a ust. 1 pkt 7 ustawy o izbach aptekarskich nie wynika, czy i jakie dane osobowe pacjentów może przetwarzać farmaceuta w związku z opieką farmaceutyczną, nie wskazuje także, że przetwarzanie danych osobowych pacjenta może się odbywać bez jego zgody, oraz nie stwarza pełnych gwarancji ochrony wrażliwych danych osobowych. Organ do spraw ochrony danych osobowych stwierdził, iż podstawą prawną przetwarzania przez farmaceutów danych osobowych pacjentów nie może być przepis art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych, bowiem pomimo, iż przetwarzanie danych osobowych pacjentów będzie prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych, czy też leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, brak jest jednak zapewnienia pełnych gwarancji ochrony danych osobowych. W związku z tym Generalny Inspektor Ochrony Danych Osobowych uznał za niezbędne wystąpienie o zmianę przepisów prawa, celem właściwego ujęcia podstawy prawnej, jak i sposobu przetwarzania danych osobowych (zwłaszcza szczególnie chronionych) pacjentów, wobec których jest sprawowana przez farmaceutów opieka farmaceutyczna.

W odpowiedzi udzielonej dnia 7 marca 2011 r. Minister Zdrowia w pełni zgodziła się z argumentacją Generalnego Inspektora informując jednocześnie, że kwestie poruszone w wystąpieniu rozpatrzone zostaną w toku prac nad nowelizacją ustawy o izbach aptekarskich.

W celu wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych przez podmioty publiczne, Generalny Inspektor wystosował **pismo z dnia 18 stycznia 2011 r. do Prezesa Narodowego Funduszu Zdrowia³⁹² w sprawie wymagań określonych w Komunikacie dla Świadczeniodawców wypisujących zlecenia na zaopatrzenie w wyroby medyczne będące przedmiotami ortopedycznymi i środkami pomocniczymi Oddziału Wojewódzkiego Narodowego Funduszu Zdrowia, dotyczącym zasadności wypisywania zleceń lekarskich na zaopatrzenie w przedmioty ortopedyczne i środki pomocnicze zgodnie z obowiązującymi przepisami wydanym przez Małopolski Oddział Wojewódzki NFZ.** Zdaniem Generalnego Inspektora powyższy komunikat opublikowany przez Małopolski Oddział Wojewódzkiego NFZ w dniu 21 października 2010 r.

³⁸⁹ Zgodnie z art. 31 ust. 3, ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw. Zgodnie z art. 47, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

³⁹⁰ sygn. K. 32/2004

³⁹¹ Trybunał Konstytucyjny stwierdził, że „konieczność w demokratycznym państwie prawnym to zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić określone wartości w sposób lub stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawo lub wolność ograniczają”.

³⁹² DOLiS-035-108/11/2155

zawierał budzącą istotne zastrzeżenia interpretację zapisów zarządzenia Nr 58/2009/DSOZ Prezesa NFZ z dnia 29 października 2009 r. w sprawie określenia warunków zawierania i realizacji umów w rodzaju zaopatrzenia w wyroby medyczne będące przedmiotami ortopedycznymi oraz środkami pomocniczymi oraz rozporządzenia Ministra Zdrowia z dnia 29 sierpnia 2009 r. w sprawie świadczeń gwarantowanych z zakresu zaopatrzenia w wyroby medyczne będące przedmiotami ortopedycznymi oraz środki pomocnicze (Dz. U. Nr 139, poz. 1141 z późn. zm.). Jak zauważył Generalny Inspektor, zarządzenie nakładało na lekarzy obowiązek szczegółowego wpisywania na zleceniu na zaopatrzenie rozpoznania chorobowego, jakie występuje u pacjenta. Generalny Inspektor podniósł, że zgodnie ze wskazaniem Ogólnopolskiej Izby Gospodarczej Wyrobów Medycznych POLMED do niedawna umieszczony na zleceniu rodzaj schorzenia podlegał kodowaniu zgodnie z klasyfikacją ICD-10. W ramach powyższego komunikatu Małopolski Oddział Wojewódzki NFZ wymagał, aby dane te zostały uzupełnione o „rozpoznanie bezpośrednie, uszczegółowione, uzasadniające zaopatrzenie”, a ponadto, aby w miejscu na dodatkowe uwagi zlecenie uzupełniać informacją pod nazwą „skutki i objawy choroby”. Organ do spraw ochrony danych osobowych podkreślił, że Ogólnopolska Izba Gospodarcza Wyrobów Medycznych POLMED stoi na stanowisku, iż działania takie stanowią nie tylko naruszenie przepisów art. 40³⁹³ ustawy z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty (Dz. U. z 2008 r. Nr 136, poz. 857 z późn. zm.), ale także zapisów art. 14 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. Nr 139, poz. 1141 z późn. zm.). W związku z powyższym Generalny Inspektor uznał, że wymagane przez Małopolski Oddział Wojewódzki NFZ działania związane są z udostępnianiem danych osobowych o stanie zdrowia osobom realizującym zlecenie na zaopatrzenie w określone wyroby medyczne. Podkreślił, że w świetle przepisów o ochronie danych osobowych dane takie posiadają status szczególnie chronionych (art. 27 ust. 1 tej ustawy), a ich przetwarzanie podlega wyjątkowemu reżimowi. Uznał również, że przy takiej realizacji zaleceń Małopolskiego Oddziału Wojewódzkiego NFZ dochodzić będzie do udostępniania danych osobowych szczególnie chronionych, a tym samym należących do sfery intymnej pacjentów, m.in. osobom realizującym zlecenie na zaopatrzenie, co nie zostało przewidziane w przepisach prawa powszechnie

³⁹³ Art. 40. 1. Lekarz ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu. 2. Przepisu ust. 1 nie stosuje się, gdy: 1) tak stanowią ustawy; 2) badanie lekarskie zostało przeprowadzone na żądanie uprawnionych, na podstawie odrębnych ustaw, organów i instytucji; wówczas lekarz jest obowiązany poinformować o stanie zdrowia pacjenta wyłącznie te organy i instytucje; 3) zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób; 4) pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy, po uprzednim poinformowaniu o niekorzystnych dla pacjenta skutkach jej ujawnienia; 5) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie lekarzowi sądowemu; 6) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innemu lekarzowi lub uprawnionym osobom uczestniczącym w udzielaniu tych świadczeń. 2a. W sytuacjach, o których mowa w ust. 2, ujawnienie tajemnicy może nastąpić wyłącznie w niezbędnym zakresie. 3. Lekarz, z zastrzeżeniem sytuacji, o których mowa w ust. 2 pkt 1-5, jest związany tajemnicą również po śmierci pacjenta. 4. Lekarz nie może podać do publicznej wiadomości danych umożliwiających identyfikację pacjenta bez jego zgody.

obowiązujących. W świetle ww. wątpliwości Generalny Inspektor zwrócił się do Prezesa NFZ w celu wskazania podstaw prawnych legalizujących powyższe działania.

W odpowiedzi z dnia 10 lutego 2011 r. NFZ nie zgodził się z wątpliwościami Generalnego Inspektora Ochrony Danych Osobowych wskazując, że jego działania znajdują oparcie w obecnie obowiązujących przepisach prawa. Argumentacja NFZ wzbudziła jednak szereg wątpliwości organu do spraw ochrony danych osobowych, który skierował sprawę do Rzecznika Praw Pacjenta.

W piśmie z dnia 28 lutego 2011 r. skierowanym do Narodowego Funduszu Zdrowia Generalny Inspektor poruszył problematykę wniosku o wydanie europejskiej karty ubezpieczenia zdrowotnego.³⁹⁴ Pozyskał bowiem informację wskazującą na to, że za pomocą przedmiotowego wniosku dochodzi do gromadzenia danych osobowych w zbyt szerokim zakresie. Zauważył również, że brak jest przepisów, które określałyby wzór takiego wniosku i zakres danych pozyskiwanych za jego pomocą. Wskazał jednocześnie, że z art. 49 ust. 9 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t. j. Dz. U. z 2008 r. Nr 164, poz. 1027 z późn. zm.) wynika, iż Rada Ministrów zobowiązana jest określić w drodze rozporządzenia m.in. wzór wniosku o wydanie europejskiej karty ubezpieczenia zdrowotnego. Rozporządzenie takie nie zostało jednak wydane, a na dzień przedstawienia opinii przez Generalnego Inspektora Narodowy Fundusz Zdrowia posługiwał się wzorem wniosku o wydanie takiej karty, który nie ma podstawy prawnej w powszechnie obowiązujących przepisach prawa, godząc tym samym w regulacje objęte Konstytucją Rzeczypospolitej Polskiej³⁹⁵. Analizując przedmiotowy problem Generalny Inspektor powołał się na decyzję Nr S1 z dnia 12 czerwca 2009 r. dotyczącą europejskiej karty ubezpieczenia zdrowotnego (Dz. Urz. UE C.2010.106.23), która określa wzór takiej karty i wskazuje, jakie dane powinny się na niej znaleźć, natomiast w zakresie wniosku pozostawiając państwom członkowskim swobodę jego określenia. Zaznaczył również, że ustawa o ochronie danych osobowych wymaga, aby dane osobowe były adekwatne w stosunku do celów, dla jakich są przetwarzane (art. 26 ust. 1 pkt 3). Generalny Inspektor nie uznał za zasadne i celowe pozyskiwania w takim wniosku informacji o celu wyjazdu, kraju do którego się wyjeżdża, czy okresie trwania pobytu. Zgodnie bowiem ze wzorem europejskiej karty ubezpieczenia zdrowotnego takie informacje nie są zamieszczane na samej karcie. Art. 8 w/w decyzji stanowi, iż z europejskiej karty ubezpieczenia zdrowotnego, która obowiązuje w krajach UE, można korzystać we wszystkich przypadkach pobytu czasowego, podczas którego ubezpieczony potrzebuje świadczeń rzeczowych niezależnie od celu pobytu, który może mieć związek z turystyką, działalnością zawodową, nauką. Jedynym wyjątkiem

³⁹⁴ DOLiS-035-572/11/8418

³⁹⁵ Stosownie do art. 7 organy władzy publicznej działają na podstawie i w granicach prawa. Zgodnie z art. 31 ust. 3, ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

jest, iż europejskiej karty ubezpieczenia zdrowotnego nie można używać w przypadku, gdy celem pobytu czasowego jest poddanie się leczeniu. Generalny Inspektor wskazał, że brak jest podstaw do pozyskiwania informacji o celu podróży i kraju, do którego się wyjeżdża. Ponadto okres ważności europejskiej karty ubezpieczenia zdrowotnego powinien uwzględniać przewidywany czas trwania uprawnienia ubezpieczonego. Nie ma zatem mowy o czasie pobytu, lecz o przewidywanym czasie trwania uprawnienia ubezpieczonego. Wobec powyższego, Generalny Inspektor uznał za niezbędne ustanowienie odpowiednich przepisów prawa, które nie tylko wyeliminują problemy związane z zakresem danych pozyskiwanych za pomocą wzoru, ale także przyczynią się do ochrony praw osób, których dane dotyczą.

W odpowiedzi NFZ z dnia 23 marca 2011 r. przedstawiono argumentację wskazującą na przepisy, które mają uprawniać Fundusz do gromadzenia danych za pośrednictwem przedmiotowego kwestionariusza. Wskazano jednocześnie, że wszelkie ewentualne kwestie legislacyjne należą do kompetencji Ministra Zdrowia.

6.1.2. Przetwarzanie danych osobowych – wybrane problemy

Interesujące zagadnienie z punktu widzenia ochrony danych osobowych oraz w związku ze zbliżającymi się Europejskimi Mistrzostwami Piłki Nożnej Euro 2012 zawarte było w **pytaniu Polskiego Związku Piłki Nożnej (PZPN), dotyczącym przetwarzania danych kibiców w Centralnej Bazie Danych Kibiców i problemu informowania przez kluby piłkarskie kibiców, że dane do nich należące będą przetwarzane w ww. bazie przez PZPN**. W odpowiedzi³⁹⁶ Generalny Inspektor wskazał, iż – z uwagi na uwarunkowania wynikające z ustawy o ochronie danych osobowych – w świetle aktualnego brzmienia ustawy z dnia 20 marca 2009 roku o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 z późn. zm.), brak jest podstaw prawnych dla tworzenia przez Polski Związek Piłki Nożnej (PZPN), zintegrowanej bazy danych kibiców meczów piłki nożnej, czyli Centralnej Bazy Danych Kibiców, powoływanej dalej z zastosowaniem skrótu „CBDK”. W ocenie Generalnego Inspektora, zgodnie z określonymi w ustawie o ochronie danych osobowych zasadami ochrony tych danych, każdy podmiot zamierzający przetwarzać, w tym zbierać i przechowywać (art. 7 pkt 2 ustawy o ochronie danych osobowych), dane osobowe tzw. „zwykłe” winien legitymować się jedną z równoprawnych przesłanek wymienionych w art. 23 ust. 1 ww. ustawy. Generalny Inspektor zauważył, że w przypadku wskazanym w piśmie PZPN, biorąc pod uwagę charakter danych, które miałyby być przetwarzane, przesłanką taką powinien być przepis prawa nakazujący PZPN-owi przetwarzanie danych osobowych kibiców w określonym celu i zakresie (art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych). Generalny Inspektor zastrzegł przy tym, że przepis prawa, o którym

³⁹⁶ DOLiS-035-1439/11/ 23131

mowa wyżej, musi być przepisem powszechnie obowiązującym w rozumieniu art. 87 Konstytucji Rzeczypospolitej Polskiej. Przedmiotem przetwarzania mają być bowiem dane osobowe osób trzecich (kibiców), nienależących do PZPN, ani nienależących do klubów piłkarskich zrzeszonych w PZPN. Analiza uregulowań dotyczących zbierania i przechowywania danych osobowych kibiców prowadzi do wniosku, iż w chwili obecnej nie ma przepisu prawa przyznającego PZPN-owi uprawnienie do tworzenia zintegrowanej bazy danych kibiców meczów piłki nożnej, a spełniającego wymagania wskazane wyżej w niniejszym piśmie. Organ do spraw ochrony danych osobowych zauważył, że stanowiąca podstawę prawną utworzenia CBDK *Uchwała nr IV/51 z dnia 30 marca 2010 r. Zarządu Polskiego Związku Piłki Nożnej w sprawie identyfikacji osób uczestniczących w meczach piłki nożnej będących imprezami masowymi* jest dokumentem wewnętrznym i jako taki nie wywołuje skutków prawnych wobec kibiców, ani też nie może skutecznie zobowiązywać innych podmiotów prowadzących bazy danych kibiców w oparciu o przepisy ustawy o bezpieczeństwie imprez masowych do przekazywania tych baz danych PZPN-owi. Zaznaczył, że PZPN jest jednym z organizatorów meczów piłki nożnej w rozumieniu rozdziału 3 ustawy o bezpieczeństwie imprez masowych (w zakresie meczów reprezentacji narodowej oraz finału Pucharu Polski) i – w związku z powyższym – ciążą na nim przewidziane w tej ustawie obowiązki dotyczące zapewnienia bezpieczeństwa imprez masowych, a w szczególności meczów piłki nożnej. Na podstawie art. 13 ust. 1 ustawy o bezpieczeństwie imprez masowych jest on zatem zobligowany do zapewnienia identyfikacji osób uczestniczących w – organizowanym przez niego – meczu piłki nożnej oraz zobowiązany do przekazywania Komendantowi Głównemu Policji informacji dotyczących bezpieczeństwa imprez masowych w zakresie określonym w art. 40 pkt 3 – 5 i 9 w zw. z art. 39 pkt 2 i art. 41 ust. 2 pkt 3 ustawy o bezpieczeństwie imprez masowych. Jednakże - jak uznał Generalny Inspektor - w odniesieniu do wprowadzania na obiektach wykorzystywanych do organizacji meczów piłki nożnej elektronicznych systemów identyfikacji osób (kibiców), służących do sprzedaży biletów, kontroli przebywania w miejscu i w czasie trwania meczu piłki nożnej oraz kontroli dostępu do określonych miejsc, ustawodawca ograniczył rolę PZPN-u do uzgadniania z podmiotem zarządzającym rozgrywkami ligi zawodowej zasad tworzenia tych systemów (art. 13 ust. 2 i 3 ustawy o bezpieczeństwie imprez masowych). Generalny Inspektor wskazał, że z woli ustawodawcy tworzenie baz danych kibiców piłki nożnej jest kompetencją podmiotu (podmiotów) zarządzającego (zarządzających) rozgrywkami ligi zawodowej, nie zaś PZPN-u. W związku z udziałem w pracach legislacyjnych dotyczących projektu ustawy o zapewnieniu bezpieczeństwa w związku z organizacją Turnieju Finałowego UEFA EURO 2012 oraz o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks wykroczeń oraz niektórych innych ustaw, organowi do spraw ochrony danych osobowych wiadomym jest, iż powyższy pogląd został podtrzymany. Generalny Inspektor zwrócił też uwagę, że w najnowszej wersji (z dnia

10.05.2011 r.) powołanego wyżej projektu ustawy, usunięte zostały bowiem projektowane unormowania dotyczące prowadzenia przez PZPN bazy danych uczestników meczów piłki nożnej. Reasumując Generalny Inspektor uznał, że tworzenie przez PZPN CBDK nie może być uznane za działanie zgodne z przepisami o ochronie danych osobowych.

Nieprawidłowości w przetwarzaniu danych osobowych odnotowano również w związku z przeprowadzaniem **rekrutacji chętnych do udziału w egzaminach wstępnych na aplikacje prawnicze, a dokładnie w związku z wypełnianiem kwestionariusza osobowego przygotowanego przez Ministerstwo Sprawiedliwości przez kandydatów na przedmiotowe egzaminy**. W piśmie z dnia 3 lutego 2011 r.³⁹⁷ Generalny Inspektor wskazał potrzebę uregulowania zakresu danych pozyskiwanych od kandydatów na aplikację gromadzonych za pomocą przedmiotowego formularza wskazanych w art. 75c ust. 2 pkt 2 ustawy z dnia 26 maja 1982 o adwokaturze (t. j. Dz. U. 2009 r. Nr 146 poz. 1188 z późn. zm.), w art. 71d § 2 pkt 2 ustawy z dnia 14 lutego 1991 o notariacie (t. j. Dz. U. 2008 r. Nr 189 poz. 1158 z późn. zm.) oraz w art. 33³ ust. 2 pkt 2 ustawy z dnia 6 lipca 1982 o radcach prawnych (t. j. Dz. U. 2010 r. Nr 10 poz. 65 z późn. zm.). Generalny Inspektor Ochrony Danych Osobowych zauważył, że zgodnie z treścią wyżej wskazanych przepisów, osoby chcące wziąć udział w egzaminach wstępnych na aplikację notarialną, radcowską i adwokacką są zobowiązane do złożenia w odpowiednim terminie szeregu dokumentów, w tym kwestionariusza osobowego, którego kształtu nie regulują żadne obowiązujące przepisy prawa. Wymagania dotyczące kandydatów ubiegających się o miejsce na poszczególnej aplikacji nie są identyczne, a co za tym idzie kwestionariusze osobowe odpowiednie dla każdej aplikacji powinny uwzględniać zakres danych adekwatnych do prawidłowego przeprowadzenia postępowania kwalifikacyjnego dla konkretnej aplikacji. Mimo, iż przepisy poszczególnych ustaw wskazują kryteria, jakie spełniać powinni poszczególni kandydaci na konkretne aplikacje, to jednak brak jasnych regulacji wskazujących zamknięty katalog danych udostępnianych przez kandydatów na aplikację i gromadzonych przez Ministerstwo Sprawiedliwości za pośrednictwem kwestionariuszy, może prowadzić do przetwarzania tych danych w zakresie szerszym niż jest to konieczne do przeprowadzania postępowania kwalifikującego do przystąpienia do egzaminu na wskazane aplikacje. Generalny Inspektor podniósł, że składanie przez kandydatów określonych formularzy zawierających dane osobowe prowadzi do przetwarzania danych osobowych w rozumieniu ustawy o ochronie danych osobowych³⁹⁸. Odnosił się również do zasad przetwarzania danych

³⁹⁷ DOLiS-035-277/11/ 4535

³⁹⁸ Zgodnie z art. 6 ust. 1, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (ust. 2). Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań (ust. 3). Przetwarzanie danych osobowych natomiast zgodnie z treścią art. 7 pkt 2 ustawy o ochronie danych osobowych rozumiane jest jako jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

osobowych wynikających z norm przewidzianych w art. 26 ustawy o ochronie danych osobowych, zaznaczając jednocześnie, że przepis ten jest odzwierciedleniem art. 6 ust. 1 lit. c implementowanej do polskiego porządku prawnego Dyrektywy nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. W podsumowaniu Generalny Inspektor wyraził potrzebę stworzenia odrębnych kwestionariuszy uwzględniających różnice w wymaganiach, jakie spełniać powinna osoba ubiegająca się o miejsce na konkretnej aplikacji.

W odpowiedzi³⁹⁹ na w/w stanowisko Generalnego Inspektora wskazano, że Minister Sprawiedliwości nie jest co prawda właściwy do uregulowania kwestii związanych z opisanym kwestionariuszem, niemniej jednak przyznaje słuszność organowi do spraw ochrony danych osobowych i podejmie stosowną analizę prawną odnośnie celowości przetwarzania danych osobowych zawartych w przedmiotowym kwestionariuszu.

Istotne stanowisko Generalnego Inspektora z punktu widzenia ochrony danych osobowych, a także szeroko pojętego prawa do prywatności zawarto w **piśmie z dnia 11 lutego 2011 r. do Dyrektora Zakładu Karnego w Chełmie, dotyczące braku zabezpieczania danych osobowych osób przesyłających skazanemu przesyłki pocztowe.**⁴⁰⁰ Oprócz regulacji wynikających z ustawy o ochronie danych osobowych, Generalny Inspektor zwrócił również uwagę na przepisy ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. 2010 r. Nr 79, poz. 523 z późn. zm.), ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz. U. 1997 r. Nr 90, poz. 557 z późn. zm.) oraz akty wykonawcze wydane na podstawie ustawy Kodeks karny wykonawczy, w szczególności rozporządzenie Ministra Sprawiedliwości z dnia 25 sierpnia 2003 r. w sprawie regulaminu organizacyjno-porządkowego wykonywania kary pozbawienia wolności (Dz. U. 2003 r. Nr 152, poz. 1493), pełniące szczególną rolę w związku z przetwarzaniem danych osobowych skazanych. Podniósł, iż przepisy te wskazują tryb i zasady postępowania z paczką żywnościową, która kierowana jest do skazanego osadzonego w Zakładzie. Po weryfikacji zawartości takiej paczki w obecności skazanego, jest ona następnie wydawana adresatowi. Brak jest natomiast w przepisach szczególnych wskazania sposobu postępowania z opakowaniem pozostającym po paczce żywnościowej. W ocenie Generalnego Inspektora, na opakowaniu po paczce żywnościowej znajdują się dane osobowe oraz adresowe nie tylko skazanego, ale i nadawcy przesyłki. Za bezpieczeństwo oraz tajemnicę korespondencji odpowiadać powinien administrator danych w taki sposób, żeby dane adresowe znajdujące się na opakowaniu paczki żywnościowej nie były dostępne ogółowi osadzonych w Zakładzie. Organ do spraw ochrony danych osobowych uznał więc za konieczne podjęcie rozwiązań zmierzających do zachowania tychże informacji adresowych w poufności poprzez np. opracowanie i wdrożenie w wewnętrznym

³⁹⁹ DOLiS-035-277/11/8987

⁴⁰⁰ DOLiS-035-382/11/5990

regulaminie organizacyjno-porządkowym Zakładu stosownych postanowień dotyczących postępowania z opakowaniami po paczkach żywnościowych. Dyrektor Zakładu, jako administrator danych osobowych, na mocy przepisów ustawy o ochronie danych osobowych, w szczególności osób osadzonych w tym Zakładzie, jest bowiem zobowiązany do właściwego zabezpieczenia przedmiotowych danych osobowych przed ich udostępnianiem osobom nieupoważnionym.⁴⁰¹ Generalny Inspektor w/w zmiany i rozwiązania uznał za konieczne, ponieważ z informacji powziętych przez organ ds. ochrony danych osobowych wynika, iż skazani osadzeni w Zakładzie mieli, bądź mają nieustannie dostęp do pudełek kartonowych „po paczkach żywnościowych które rodziny przysłały skazanym”. Jak wynikało z informacji otrzymanych przez Generalnego Inspektora Ochrony Danych Osobowych, na każdym z tych kartonów naklejony był druk z danymi osoby nadającej paczkę i odbierającej paczkę. Z informacji powziętych przez Generalnego Inspektora Ochrony Danych Osobowych wynika także, że „jeden ze skazanych przeglądał te dane”, a następnie „bezceremonialnie wyjął kartkę papieru i przepisał dane rodziny z adresem (...) człowieka”, który „doniósł” na skazanego utrwalającego dane w ww. sposób. W świetle przedstawionych powyżej informacji, Generalny Inspektor zwrócił się o podjęcie stosownych czynności, mających na celu wyjaśnienie i ewentualne wyeliminowanie wskazanych w niniejszym piśmie nieprawidłowości.

W odpowiedzi na powyższe stanowisko, szczegółowo opisane zostały działania jakie podjęto w Zakładzie Karnym w celu wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych.⁴⁰²

Istotne z punktu widzenia ochrony danych osobowych było **stanowisko Generalnego Inspektora wypracowane w kwestii, czy proponowana zmiana ustawy Prawo o aktach stanu cywilnego nie narusza przepisów ustawy o ochronie danych osobowych w związku z propozycją, aby każdorazowo Urząd Stanu Cywilnego przysyłał odpis aktu urodzenia dziecka przez małoletnią matkę do sądu opiekuńczego celem ustanowienia opieki.**⁴⁰³ O ocenie organu do spraw ochrony danych osobowych zaproponowane unormowanie art. 52a ustawy z dnia 29 września 1986 r. – Prawo o aktach stanu cywilnego (t. j. Dz. U. z 2004 r. Nr 161, poz. 1688 z późn. zm.), wydało się nie być zgodne z obowiązującymi przepisami dotyczącymi ustanawiania opieki nad małoletnimi. Generalny Inspektor podniósł, że zgodnie z art. 94 § 3 ustawy z dnia 25 lutego 1964 roku – Kodeks rodzinny i opiekuńczy (Dz. U. Nr 9, poz. 59 z późn. zm.), opiekę dla małoletniego ustanawia się tylko

⁴⁰¹ Zgodnie z brzmieniem art. 36 ust. 1 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1 (art. 36 ust. 2 ustawy). Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności (art. 36 ust. 3 ustawy). W myśl art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

⁴⁰² DOLiS-035-382/11/9865

⁴⁰³ DOLiS-035-792/11/32118

w przypadku, jeżeli żadnemu z jego rodziców nie przysługuje władza rodzicielska albo jeżeli rodzice małoletniego są nieznani. Biorąc zatem pod uwagę, że w sprawie opiekuńczej sąd opiekuńczy może wszcząć postępowanie z urzędu (art. 570 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, Dz. U. Nr 43, poz. 296 z późn. zm.), zaś na urzędach stanu cywilnego ciąży obowiązek zawiadomienia o zdarzeniu uzasadniającym wszczęcie postępowania z urzędu (art. 572 § 2 w zw. z § 1 ustawy – Kodeks postępowania cywilnego), Generalny Inspektor wskazał, że projektowana regulacja, przewidująca przesyłanie przez kierownika urzędu stanu cywilnego odpisu aktu urodzenia dziecka przez małoletnią niepozostającą w związku małżeńskim (a więc – nieposiadającą pełnej zdolności do czynności prawnych – patrz art. 10 § 2 zdanie pierwsze w zw. z art. 11 ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny – Dz. U. Nr 16, poz. 93 z późn. zm.), byłaby zasadna w sytuacji, gdy ojciec dziecka nie był znany albo sam był osobą małoletnią. W przypadku, jak zauważył Generalny Inspektor, jeżeli ojciec dziecka jest znany oraz pełnoletni (a informacja o tym fakcie znajduje się w akcie urodzenia), to z mocy art. 94 §1 zdanie pierwsze ustawy – Kodeks rodzinny i opiekuńczy, przysługuje mu władza rodzicielska nad dzieckiem małoletniej (o ile nie został jej pozbawiony w trybie określonym w przepisach odrębnych), brak jest podstaw prawnych dla ustanawiania opieki w takiej sytuacji. W tym stanie faktycznym przesyłanie przez kierownika urzędu stanu cywilnego odpisu aktu urodzenia dziecka przez małoletnią stanowiłoby naruszenie – chronionego przepisami Konstytucji Rzeczypospolitej Polskiej (art. 47) – prawa do prywatności rodziców dziecka.

Kolejne istotne stanowisko przedstawiono **w piśmie stanowiącym odpowiedź na pytanie dotyczące problemu związanego z udostępnianiem danych osobowych gromadzonych przez właściwych komendantów Policji w zakresie bezpieczeństwa masowych imprez sportowych, w szczególności meczów piłki nożnej, na potrzeby organizatorów, w tym klubów sportowych.**⁴⁰⁴ Generalny Inspektor zauważył, że wątpliwości wyrażone w piśmie znajdują bezpośrednie rozstrzygnięcie w ustawie z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 z późn. zm.). Organ do spraw ochrony danych osobowych zaznaczył, że powołany akt prawny w rozdziale 7 (art. 40) reguluje w sposób wyczerpujący problematykę zbierania i udostępniania informacji dotyczących bezpieczeństwa imprez masowych.⁴⁰⁵ Przetwarzanie (w tym gromadzenie

⁴⁰⁴ DOLiS-035-1688/11/26592

⁴⁰⁵ Art. 40. Zakres gromadzonych i przetwarzanych informacji dotyczących bezpieczeństwa masowych imprez sportowych, w tym meczów piłki nożnej, zawiera dane: 1) o osobach, przeciwko którym toczy się postępowanie karne lub przeciwko którym skierowano wnioski o ukaranie za czyn popełniony w związku z masową imprezą sportową, w tym meczem piłki nożnej, obejmujące: a) imię i nazwisko, używane pseudonimy, b) datę i miejsce urodzenia, c) numer PESEL lub serię i numer dokumentu potwierdzającego tożsamość osoby, d) adres zamieszkania lub stałego pobytu, e) adres korespondencyjny, f) informację o karalności, g) przynależność do klubów kibica oraz charakterystykę zachowania podczas i w związku z masowymi imprezami sportowymi, w tym meczami piłki nożnej; 2) o osobach, co do których zapadł prawomocny wyrok lub prawomocne orzeczenie o ukaraniu za przestępstwo albo wykroczenie, popełnione w związku z masową imprezą sportową, w tym meczem piłki nożnej, obejmujące: a) imię i nazwisko, używane pseudonimy, b) datę i miejsce urodzenia, c) numer PESEL lub serię i numer dokumentu potwierdzającego tożsamość osoby, d) adres zamieszkania lub stałego pobytu, e) adres korespondencyjny, f) informację o karalności, g) informacje o zastosowaniu środka karnego zakazu wstępu na imprezę masową lub środka karnego, o którym mowa w art. 15 ust. 3 pkt 1 lit. b, h) przynależność do klubów kibica oraz charakterystykę zachowania podczas i w związku z masowymi imprezami sportowymi, w tym meczami piłki nożnej; 3) o klubach, organizacjach, stowarzyszeniach skupiających kibiców, obejmujące: a) ich nazwę, b) imię i nazwisko osoby działającej w imieniu osób zrzeszonych,

i udostępnianie) – wskazanych wyżej – informacji dotyczących bezpieczeństwa masowych imprez sportowych (w tym meczów piłki nożnej) należy do zadań Komendanta Głównego Policji (art. 36 ust. 1 ustawy o bezpieczeństwie imprez masowych), zaś w zakresie dotyczącym masowych imprez sportowych organizowanych na obszarze ich działania – komendanci wojewódzcy (Komendant Stołeczny) Policji i komendanci powiatowi (rejonowi, miejscy) Policji mogą takie informacje otrzymywać i udostępniać (art. 36 ust. 3 i 4 w zw. z art. 40 ustawy o bezpieczeństwie imprez masowych). W myśl zaś art. 38 ust. 1 pkt 13 i 14 ustawy o bezpieczeństwie imprez masowych kluby sportowe oraz organizatorzy masowych imprez sportowych (w tym meczów piłki nożnej) są podmiotami uprawnionymi w zakresie swoich kompetencji do otrzymywania od Komendanta Głównego Policji informacji dotyczących bezpieczeństwa imprez masowych [w konsekwencji także – do otrzymywania od komendantów wojewódzkich (Komendanta Stołecznego) Policji i komendantów powiatowych (rejonowych, miejskich) Policji informacji dotyczących bezpieczeństwa imprez masowych organizowanych na obszarze działania tych komendantów – art. 36 ust. 4 w zw. ust. 3 i art. 38 ust. 1 pkt 13 i 14 ustawy o bezpieczeństwie imprez masowych]. Kluby sportowe i inni organizatorzy masowych imprez sportowych (w tym meczów piłki nożnej) w celu uzyskania informacji dotyczących bezpieczeństwa imprez masowych kierują do Komendanta Głównego Policji [odpowiednio: komendantów wojewódzkich (Komendanta Stołecznego) Policji, komendantów powiatowych (rejonowych, miejskich) Policji] zapytania, wraz z uzasadnieniem, na kartach zapytania (art. 42 ust. 3 ustawy o bezpieczeństwie imprez masowych). Generalny Inspektor zauważył, że wzór karty zapytania określa załącznik nr 12 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 2 marca 2010 r. w sprawie przekazywania informacji dotyczących bezpieczeństwa imprez masowych (Dz. U. Nr 54, poz. 329). Organ do spraw ochrony danych osobowych wskazał, że w oparciu o informacje zamieszczone przez klub sportowy (innego organizatora masowej imprezy sportowej) w karcie zapytania Komendant Główny Policji [odpowiednio: komendant wojewódzki (Komendant Stołeczny)

c) liczbę członków, d) miejsce spotkań oraz charakterystykę zachowań i metod działania osób, o których mowa w lit. c, oraz elementy charakterystyczne, w szczególności oznakowanie ubrania, e) informacje o czynach noszących znamiona przestępstwa albo wykroczenia o charakterze chuligańskim z udziałem osób, o których mowa w lit. c, f) informacje o wzajemnych relacjach pomiędzy poszczególnymi klubami, organizacjami i stowarzyszeniami; 4) o zaistniałych w związku z organizowanymi imprezami masowymi zbiorowych naruszeniach porządku i bezpieczeństwa publicznego oraz chuligańskich zachowaniach, obejmujące: a) datę i miejsce zdarzenia, b) informacje o rodzaju imprezy, w związku z którą doszło do zdarzenia, c) skutki zdarzenia, d) informacje o działaniach i podjętych środkach zaradczych; 5) o związkach i klubach sportowych, obejmujące: a) nazwę związku lub klubu sportowego oraz skład ich władz, b) adres siedziby, c) informacje o rodzaju rozgrywek, w których związek lub klub uczestniczył, uczestniczy oraz do jakich się zakwalifikował, d) informacje o obiektach sportowych, z których związek lub klub stale korzysta; 6) o terminarzu rozgrywek meczów piłki nożnej lub terminarzu innych masowych imprez sportowych z podaniem orientacyjnej liczby uczestników; 7) o obiektach, na terenie których są organizowane masowe imprezy sportowe, w tym mecze piłki nożnej, obejmujące: a) rodzaj obiektu i jego nazwę, b) informacje dotyczące dopuszczenia obiektu do użytkowania, c) informacje dotyczące usytuowania obiektu wraz z planem i jego opisem, d) informacje o pojemności obiektu, e) informacje dotyczące służby porządkowej i służby informacyjnej; 8) o przemieszczaniu się osób uczestniczących w masowych imprezach sportowych, w tym meczach piłki nożnej, i ich pobycie w miejscach organizowania tych imprez oraz informacje o środkach transportu, z jakich korzystają, miejscach zbiórek, trasach przejazdów oraz o liczebności grup uczestników; 9) o organizatorach masowych imprez sportowych, w tym meczów piłki nożnej, i organizatorach przejazdu osób uczestniczących w masowych imprezach sportowych, w tym meczach piłki nożnej, obejmujące: a) nazwę lub imię i nazwisko organizatora wraz z jego siedzibą oraz adresem, b) określenie masowej imprezy sportowej, w tym meczu piłki nożnej, w związku z którą organizowany jest przejazd; 10) o zakazach zagranicznych oraz instytucjach zagranicznych właściwych do współpracy, w tym ich nazwę, siedzibę oraz adres.

Policji, komendant powiatowy (rejonowy, miejski) Policji] decyduje o udostępnieniu (ewentualnie o odmowie udostępnienia) wnioskowanej informacji dotyczącej bezpieczeństwa imprez masowych i zakresie udostępnionych danych. Przy podejmowaniu decyzji w tej kwestii – wskazany wyżej – komendant Policji winien się w szczególności kierować wskazanymi przez podmiot uprawniony w uzasadnieniu zapytania powodami wystąpienia z zapytaniem (art. 43 ust. 1 zdanie drugie ustawy o bezpieczeństwie imprez masowych).

W niniejszym opracowaniu warto również zamieścić **odpowiedź Generalnego Inspektora Ochrony Danych Osobowych na pytanie, czy Prokuratura Apelacyjna jest uprawniona do utworzenia i prowadzenia elektronicznej bazy biegłych występujących w postępowaniach karnych.**⁴⁰⁶ W pierwszej kolejności organ do spraw ochrony danych osobowych powołał się na regulacje wynikające z art. 7 Konstytucji Rzeczypospolitej Polskiej, nakładające na organy władzy publicznej – do których to organów, w świetle jednoznacznego brzmienia art. 1 ust. 3 ustawy z dnia 20 czerwca 1985 r. o prokuraturze (t. j. Dz. U. z 2008 r. Nr 7, poz. 39 z późn. zm.), należy prokuratura – obowiązek działania na podstawie i w granicach prawa. Takie brzmienie unormowań Konstytucji Rzeczypospolitej Polskiej przesądza, iż – odmiennie aniżeli ma to miejsce w odniesieniu do podmiotów sektora prywatnego – organy władzy publicznej nie mogą podejmować działań, na które prawo im w sposób jednoznaczny nie zezwala. Skoro zatem brak jest regulacji uprawniających Prokuraturę Apelacyjną w Warszawie (czy szerzej prokuratury apelacyjne) do prowadzenia bazy danych biegłych występujących w postępowaniach karnych, to – w ocenie Generalnego Inspektora Ochrony Danych Osobowych – baza taka nie powinna być przez Prokuraturę Apelacyjną w Warszawie tworzona. Przenosząc bowiem dotychczasowe rozważania na grunt ustawy o ochronie danych osobowych trudno byłoby wskazać przesłankę – w rozumieniu art. 23 ust. 1 tejże ustawy – uprawniającą do takiego przetwarzania danych osobowych biegłych przez Prokuraturę Apelacyjną w Warszawie. Za zaprezentowanym wyżej stanowiskiem organu do spraw ochrony danych osobowych przemawiała dodatkowo okoliczność, że ustawodawca w rozporządzeniu Ministra Sprawiedliwości z dnia 24 stycznia 2005 r. w sprawie biegłych sądowych (Dz. U. Nr 15, poz. 133) przewidział zasady prowadzenia baz danych biegłych – zwanych w tym akcie prawnym listami biegłych sądowych - zaś w § 8 ust. 3 zdanie drugie przedmiotowego rozporządzenia zapewnił organom prowadzącym postępowanie przygotowawcze w sprawach karnych (a więc także prokuraturze) możliwość dostępu do tych list. Nie było zatem uzasadnienia dla dublowania przez Prokuraturę Apelacyjną w Warszawie istniejącego rozwiązania w kwestii prowadzenia bazy danych biegłych.

Interesująca była również **odpowiedź Generalnego Inspektora w przedmiocie prawidłowości sposobu zabezpieczenia danych osób ubiegających się o wizę za pośrednictwem usługodawcy**

⁴⁰⁶ DOLiS-035-2716/11/53393

zewnętrznego, o którym mowa w art. 43 Wspólnotowego Kodeksu Wizowego w polskich przedstawicielstwach dyplomatycznych.⁴⁰⁷ Generalny Inspektor wskazał, że zasady współpracy między przedstawicielstwami konsularnymi (wydziałami konsularnymi przedstawicielstw dyplomatycznych) państw strefy Schengen a usługodawcami zewnętrznymi z państw, w których znajdują się te przedstawicielstwa, reguluje rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz. Urz. UE L 243 z 15.09.2009, s. 1 z późn. zm.). Generalny Inspektor przypomniał, że ten sam akt prawny (patrz w szczególności art. 43 i 44 oraz załącznik X) normuje również kwestię ochrony danych osobowych przetwarzanych podczas takiej współpracy. Uwzględniając, iż rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) jest stosowane bezpośrednio w należących do strefy Schengen państwach członkowskich Unii Europejskiej (art. 288 zdanie trzecie Traktatu o funkcjonowaniu Unii Europejskiej – Dz. U. z 2004 r. Nr 90, poz. 864/2 z późn. zm. oraz wyjątki zawarte w motywach 36 i 37 kodeksu wizowego), jedynie w zakresie nieuregulowanym w kodeksie wizowym do ochrony danych osobowych przetwarzanych w ramach współpracy między konsulatami Rzeczypospolitej Polskiej (Wydziałem Konsularnym Ambasady Rzeczypospolitej Polskiej w Federacji Rosyjskiej) a usługodawcą zewnętrznym w Federacji Rosyjskiej znajdują zastosowanie przepisy ustawy o ochronie danych osobowych. Organ do spraw ochrony danych osobowych zauważył, że z pisma przewodnika wynika, że polskie przedstawicielstwa konsularne w Federacji Rosyjskiej (w tym Wydział Konsularny Ambasady Rzeczypospolitej Polskiej w Federacji Rosyjskiej) zamierzają nałożyć na wyłonięgo w odpowiednim trybie usługodawcę zewnętrznego obowiązek stosowania się do unormowań kodeksu wizowego dotyczących ochrony danych osobowych. Tym samym, jak wskazał organ do spraw ochrony danych osobowych, zaproponowany w piśmie sposób postępowania polskich przedstawicielstw konsularnych w Federacji Rosyjskiej uznać wypada za zgodny z przepisami o ochronie danych osobowych. Z punktu widzenia ochrony danych osobowych kwestię ewentualnego konfliktu z regulacjami rosyjskimi rozstrzyga art. 43 ust. 9 kodeksu wizowego. Zgodnie z tym przepisem na państwie członkowskim, w niniejszej sprawie – Rzeczypospolitej Polskiej, ciąży obowiązek zapewnienia ochrony danych osobowych ubiegających się o wizy, zaś wykonywanie czynności przez usługodawcę zewnętrznego pozostaje bez wpływu na odpowiedzialność Rzeczypospolitej Polskiej wobec osób, których dane będą przetwarzane, z tytułu uchybień w procedurze takiego przetwarzania. Ocena przesłanek takiej odpowiedzialności będzie dokonywana w oparciu o unormowania ustawy o ochronie danych osobowych, z uwzględnieniem przepisów kodeksu wizowego. Generalny Inspektor wskazał, że konstrukcja taka nie wyłącza potencjalnej odpowiedzialności usługodawcy zewnętrznego za naruszenie norm rosyjskich.

⁴⁰⁷ DOLiS-035-3551/11/62927

Interesującym było także pytanie Dyrektora Departamentu Dróg i Autostrad w Ministerstwie Transportu, Budownictwa i Gospodarki Morskiej, czy **przekazywanie numerów rejestracyjnych pojazdów użytkowników elektronicznego systemu poboru opłat Służbie Celnej podlega przepisom ustawy o ochronie danych osobowych**. W odpowiedzi⁴⁰⁸ Generalny Inspektor wskazał, że wyrażenie przez organ do spraw ochrony danych osobowych ostatecznego stanowiska w przedstawionej sprawie wymagałoby przeprowadzenia postępowania administracyjnego, w tym dokonania przez Generalnego Inspektora Ochrony Danych Osobowych ustaleń faktycznych w kwestii sposobu planowanego wykorzystania przez Służbę Celną danych o pojazdach, które to dane miałyby być pozyskiwane z Elektronicznego Systemu Poboru Opłat. Opierając się wszakże na informacjach zawartych w piśmie przewodnim, organ do spraw ochrony danych osobowych wskazał, że z dużą dozą prawdopodobieństwa można uznać, iż pozyskiwane przez Służbę Celną numery rejestracyjne pojazdów poruszających się po płatnych drogach krajowych mogłyby być potraktowane jako dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych.⁴⁰⁹ Generalny Inspektor zauważył, że o ile bowiem numer rejestracyjny pojazdu nie dotyczy wprost zidentyfikowanej osoby fizycznej, to może on stanowić daną osobową, jeśli pozwala na taką identyfikację połączenie lub powiązanie z innymi danymi czy cechami (art. 6 ust. 2 ustawy o ochronie danych osobowych). Organowi do spraw ochrony danych osobowych wiadomym zaś jest, że Służba Celna posiada dostęp do centralnej ewidencji pojazdów (art. 80 c ust. 1 pkt 8 ustawy z dnia 20 czerwca 1997 roku – Prawo o ruchu drogowym – t. j. Dz. U. z 2005 r. Nr 108, poz. 908 z późn. zm.), w której to ewidencji do numeru rejestracyjnego pojazdu przypisane są dane osobowe (imię, nazwisko, adres zamieszkania, nr PESEL) właściciela pojazdu (posiadacza pojazdu powierzonego podmiotowi polskiemu przez zagraniczną osobę fizyczną lub prawną) – art. 80b ust. 1 pkt 5 lit. a – c w zw. z ust. 1 pkt 1 lit. c ustawy – Prawo o ruchu drogowym. Generalny Inspektor stwierdził zatem, że w oparciu o aktualnie posiadane informacje nie można wykluczyć, iż Służba Celna będzie wykorzystywała numery rejestracyjne pozyskane z Elektronicznego Systemu Poboru Opłat do identyfikacji osób. Dlatego też – nie rozstrzygając ostatecznie sprawy – Generalny Inspektor Ochrony Danych Osobowych przychylił się do stanowiska, że udostępnianie Służbie Celnej z Elektronicznego Systemu Poboru Opłat numerów rejestracyjnych pojazdów poruszających się po płatnych drogach krajowych powinno odbywać się w trybie i na zasadach określonych w art. 7 ustawy z dnia 27 sierpnia 2009 roku o Służbie Celnej (Dz. U. Nr 168, poz. 1323 z późn. zm.).

⁴⁰⁸ DOLiS-035-3608/11/64548

⁴⁰⁹ Art. 6. 1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. 3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

6.1.3. Wystąpienia

Mocą art. 19a ustawy o ochronie danych osobowych, w celu realizacji zadań, o których mowa w art. 12 pkt 6, Generalny Inspektor Ochrony Danych Osobowych może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów, wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych (ust. 1). Generalny Inspektor może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych (ust. 2). Podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania (ust. 3).

W roku 2011 r. Generalny Inspektor skierował łącznie **10 wystąpień do podmiotów administracji rządowej** w celu dostosowania obecnie obowiązujących przepisów prawa do zasad prawidłowego przetwarzania danych osobowych. Najważniejsze z nich zostały omówione poniżej.

Wystąpienie do **Ministra Sprawiedliwości** z dnia 7 kwietnia 2011 r.⁴¹⁰ dotyczące **podjęcia prac legislacyjnych zmierzających do zmiany aktualnego stanu prawnego zezwalającego na ujawnianie danych osobowych członków zarządu fundacji, w zakresie ich prywatnych adresów zamieszkania, w celu jego dostosowania do przepisów ustawy o ochronie danych osobowych.**

W przedmiotowym wystąpieniu Generalny Inspektor Ochrony Danych Osobowych w pierwszej kolejności wskazał, że pismem z dnia 5 sierpnia 2009 r.⁴¹¹ sygnalizował już przedmiotowy problem Ministrowi Sprawiedliwości⁴¹² i otrzymał wtedy zapewnienie, że Ministerstwo podejmie prace legislacyjne nad nowelizacją rozporządzenia z dnia 8 maja 2001 r. w sprawie ramowego zakresu sprawozdania z działalności fundacji (Dz. U. z 2001 r. Nr 50, poz. 529 z późn. zm.).

Generalny Inspektor Ochrony Danych Osobowych ponownie wskazał zakres § 2 pkt 1 omawianego rozporządzenia⁴¹³ oraz zauważył, że składane corocznie właściwemu ministrowi sprawozdanie z działalności fundacji jest udostępnione do publicznej wiadomości (ust. 3 art. 12 ustawy o fundacjach). Nie negując zasadności zapewnienia transparentności działania fundacji, w tym weryfikowania jej działalności przez społeczeństwo, organ do spraw ochrony danych osobowych podniósł, iż w demokratycznym państwie prawnym konieczne jest także respektowanie prawa do

⁴¹⁰ DOLiS-035-1038/11/16010

⁴¹¹ sygn.: DL-P-II-4108-3/09

⁴¹² DOLiS-035-698/09/16785

⁴¹³ Zgodnie z § 2 pkt 1 sprawozdanie powinno zawierać nazwę fundacji, jej siedzibę i adres, datę wpisu w Krajowym Rejestrze Sądowym i numer KRS-u wraz ze statystycznym numerem identyfikacyjnym w systemie REGON, dane członków zarządu fundacji (imię i nazwisko według aktualnego wpisu w rejestrze sądowym i adres zamieszkania) oraz określenie celów statutowych fundacji.

prywatności i ochrony danych osobowych. Powołał tym samym regulacje zamieszczone w Konstytucji Rzeczypospolitej Polskiej⁴¹⁴ i europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie w dniu 4 listopada 1950 r.⁴¹⁵ Ponadto, Generalny Inspektor Ochrony Danych Osobowych powołał się na zasadę adekwatności danych w stosunku do celu ich przetwarzania określoną w ustawie o ochronie danych osobowych. W ocenie Generalnego Inspektora, ustanowienie wyczerpujących i adekwatnych przepisów prawa dotyczących publikowania danych członków zarządu fundacji nie tylko wyeliminuje wątpliwości w tym zakresie, ale przyczyni się także do ochrony praw osób, których dane te dotyczą.

W odpowiedzi z dnia 9 maja 2011 r.⁴¹⁶ Minister Sprawiedliwości zgodził się ze stanowiskiem Generalnego Inspektora informując jednocześnie o podjętych pracach nad nowelizacją rozporządzenia Ministra Sprawiedliwości w sprawie ramowego zakresu sprawozdania z działalności fundacji, w celu zapewnienia zgodności aktu normatywnego z ustawą o ochronie danych osobowych. Przedstawił również projekt rozporządzenia regulującego ww. kwestie, który ostatecznie został zaakceptowany przez Generalnego Inspektora⁴¹⁷.

Kolejne prezentowane wystąpienie miało na celu **kompleksowe uregulowanie problematyki przetwarzania danych osobowych przez gminne komisje rozwiązywania problemów alkoholowych** tworzonych na podstawie art. 4¹ ust. 3 ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (t. j. Dz. U. 2007 r. Nr 70 poz. 473 z późn. zm.).

W wystąpieniu z dnia 20 kwietnia 2011 r. kierowanym do **Ministra Zdrowia**⁴¹⁸ Generalny Inspektor zauważył, że mocą art. 4¹ ust. 1 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, prowadzenie działań związanych z profilaktyką i rozwiązywaniem problemów alkoholowych oraz integracji społecznej osób uzależnionych od alkoholu należy do zadań własnych gmin. Ponadto wskazał na treść art. 4 ust. 3 ustawy⁴¹⁹. W wystąpieniu tym Generalny Inspektor wyraził stanowisko, że działalność przedmiotowych komisji bez wątpienia wiąże się z przetwarzaniem danych osobowych szczególnie chronionych tzw. wrażliwych, wskazując tym samym na generalny zakaz przetwarzania danych osobowych wrażliwych oraz wyjątki od tej zasady wynikające z art. 27 ustawy

⁴¹⁴ Zgodnie z art. 47 Konstytucji RP, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu. Zgodnie z art. 51, nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

⁴¹⁵ Art. 8 ustanawia prawo do poszanowania życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

⁴¹⁶ DL-P-II-410-20/11

⁴¹⁷ DOLiS-033-126/11

⁴¹⁸ DOLiS-035-1187/11/18548

⁴¹⁹ Art. 4 ust. 3 stanowi, że wójtowie (burmistrzowie, prezydenci miast) powołują gminne komisje rozwiązywania problemów alkoholowych, w szczególności inicjujące działania w zakresie określonym w ust. 1 oraz podejmujące czynności zmierzające do orzeczenia o zastosowaniu wobec osoby uzależnionej od alkoholu obowiązku poddania się leczeniu w zakładzie leczenia odwykowego.

o ochronie danych osobowych. Zwrócił również uwagę na regulacje zawarte w prawie europejskim, w szczególności do Dyrektywy 95/46/WE⁴²⁰. Odwołując się do art. 27 ust. 2 pkt 2, zaznaczył, że tylko przepis zawarty w akcie normatywnym o randze ustawy może zezwolić na przetwarzanie danych wrażliwych. Przepis taki powinien jednoznacznie wskazywać, że uchyla generalny zakaz przetwarzania danych wrażliwych, określać rodzaj danych, których dotyczy oraz wskazywać, że przetwarzanie danych wrażliwych możliwe jest bez zgody podmiotu tych danych. Ponadto przepis taki powinien stwarzać pełne gwarancje ochrony danych, których dotyczy. Generalny Inspektor podniósł, że problem dotyczący informacji o uzależnieniach jest niezwykle istotny z punktu widzenia ochrony prywatności, bowiem bez wątpienia informacja taka powiązana jest z informacją o stanie zdrowia. Wskazał również, że działalność gminnych komisji rozwiązywania problemów alkoholowych, w zakresie przetwarzania danych osobowych osób korzystających z pomocy tych podmiotów wymaga szczególnego uregulowania na płaszczyźnie ustawowej. W ocenie organu do spraw ochrony danych osobowych istotnym jest bowiem wskazanie jednoznacznej podstawy legalizującej proces przetwarzania danych osobowych osób korzystających z pomocy przedmiotowych komisji, a także zakresu tych danych. Ponadto, ważne jest uregulowanie wszelkich kwestii dotyczących zasad przetwarzania tych danych osobowych, zwłaszcza trybu ich pozyskiwania i udostępniania, kategorii podmiotów, którym mogą być udostępniane. Generalny Inspektor zaznaczył, że harmonizacja reguł przetwarzania danych osobowych przez omawiane podmioty pozwoli na minimalizację ryzyka wystąpienia ewentualnych nieprawidłowości w procesie przetwarzania danych. Argumentując potrzebę szczegółowego uregulowania wyżej wskazanej problematyki organ do spraw ochrony danych osobowych odniósł się także do zasad przetwarzania danych osobowych wynikających z norm przewidzianych w art. 26 ustawy o ochronie danych osobowych określających zasady: legalizmu, związania celem oraz zasadę adekwatności. Organ do spraw ochrony danych osobowych podkreślił, że obowiązki ciążące na administratorze i wskazane w w/w artykule uważane są za jedne z podstawowych. Generalny Inspektor wskazał też, że zgodnie z zasadą legalizmu, administrator danych osobowych powinien zapewnić aby dane osobowe przetwarzane były zgodnie z prawem. Ustawodawca celowo posłużył się zwrotem „zgodnie z prawem” bowiem termin ten obejmuje wszystkie normy prawne obowiązujące zgodnie z przyjętą w Konstytucji hierarchią źródeł prawa. W analizowanym wystąpieniu organ do spraw ochrony danych osobowych powołał art. 47 i 51 ust. 1 Konstytucji RP i wskazał, że wszelka ingerencja instytucji publicznych bądź podmiotów wykonujących zadania publiczne w prywatność jednostki, nawet dla jej dobra, wymaga wyraźnego sprecyzowania granic tej ingerencji, a określenie jasnych

⁴²⁰ Zgodnie z art. 8 ust. 4, państwa członkowskie mogą dodatkowo ze względu na ważny interes publiczny, zapewniając odpowiednie gwarancje, ustanowić inne wyjątki od zakazu przetwarzania wrażliwych danych osobowych albo bezpośrednio w prawie krajowym, albo też na podstawie decyzji organu sprawującego nadzór nad ochroną danych osobowych.

i rzetelnych procedur regulujących proces przetwarzania danych osobowych pozwoli na ochronę prywatności tych osób i zapobiegnie powstawaniu niejasności w związku z ich udostępnianiem.

W odpowiedzi z dnia 17 maja 2011 r. **Minister Zdrowia poinformował Generalnego Inspektora o trwających pracach nad projektem ustawy o zmianie ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi oraz niektórych innych ustaw**, niemniej jednak nie odniósł się konkretnie do problematyki poruszonej przez Generalnego Inspektora. W związku z tym, pismem z dnia 6 czerwca 2011 r. Generalny Inspektor ponownie skierował prośbę o uregulowanie ww. kwestii. W związku z tym, że Prezes Rady Ministrów zwrócił Ministrowi Zdrowia przedmiotowy projekt, w piśmie z dnia 21 października 2011 r. GODO poinformowany został, że jego uwagi zostaną uwzględnione w przyszłych ewentualnych pracach nad ustawą o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.

Celem wystąpienia z dnia 27 kwietnia 2011 r. kierowanego **do Ministra Spraw Wewnętrznych i Administracji** było **podjęcie przez ten resort prac legislacyjnych zmierzających do zmiany zasad działania komisji rewizyjnych kontrolujących działalność jednostek samorządu terytorialnego, poprzez ich dostosowanie do przepisów ustawy o ochronie danych osobowych**.

Generalny Inspektor zwrócił uwagę na regulacje zawarte w art. 18a ust. 1 ustawy z dnia z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.)⁴²¹. W ocenie organu do spraw ochrony danych osobowych wprowadzie przepisy ustawy o samorządzie gminnym stwarzają podstawy do utworzenia w gminie komisji rewizyjnej, niemniej jednak nie stanowią one wprost, do jakich dokumentów i informacji (danych osobowych) mogą mieć dostęp członkowie komisji rewizyjnej przeprowadzający kontrolę, odsyłając w tym zakresie do statutu gminy, w którym powinny być uregulowane zasady i tryb działania komisji rewizyjnej rady gminy. Nie negując celowości powoływania komisji rewizyjnych, w tym określania zasad i trybu ich działania w drodze statutu, Generalny Inspektor uznał, że niezbędne jest sprecyzowanie w przepisach rangi ustawowej zasad przetwarzania przez przeprowadzających kontrolę członków tych komisji informacji obejmujących dane osobowe w rozumieniu art. 6⁴²² i ewentualnie art. 27 ust. 1⁴²³ ustawy o ochronie danych osobowych.

⁴²¹ Art. 18a ust. 1 stanowi, że rada gminy kontroluje działalność wójta, gminnych jednostek organizacyjnych oraz jednostek pomocniczych gminy; w tym celu powołuje komisję rewizyjną. Komisja rewizyjna wykonuje inne zadania zlecone przez radę w zakresie kontroli (art. 18a ust. 4 zd. 1 ustawy o samorządzie gminnym). Zasady i tryb działania komisji rewizyjnej określa statut gminy (art. 18a ust. 5 ustawy o samorządzie gminnym). Rada gminy kontroluje działalność wójta, gminnych jednostek organizacyjnych oraz jednostek pomocniczych gminy; w tym celu powołuje komisję rewizyjną. Komisja rewizyjna wykonuje inne zadania zlecone przez radę w zakresie kontroli (art. 18a ust. 4 zd. 1 ustawy o samorządzie gminnym). Zasady i tryb działania komisji rewizyjnej określa statut gminy (art. 18a ust. 5 ustawy o samorządzie gminnym).

⁴²² Zgodnie z art. 6, w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (ust. 1). Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub

W wystąpieniu tym Generalny Inspektor powołał również regulacje zawarte w art. 51 Konstytucji RP. Odwołał się również do zasady adekwatności przetwarzania danych osobowych w stosunku do celu ich przetwarzania. Zdaniem Generalnego Inspektora, ustanowienie odpowiednich przepisów prawa we wskazanym zakresie nie tylko wyeliminuje wątpliwości interpretacyjne, z którymi wielokrotnie spotyka się Generalny Inspektor, ale przede wszystkim przyczyni się do ochrony praw osób, których dane dotyczą.

W odpowiedzi z dnia 24 maja 2011 r. nie uwzględniono stanowiska Generalnego Inspektora z uwagi na wątpliwości, co do celowości dokonywania zmiany obowiązujących przepisów. Generalny Inspektor zdecydował w związku z tym o niepodjęciu dalszych działań w tej kwestii.

Adresatem kolejnych dwóch wystąpień Generalnego Inspektora Ochrony Danych Osobowych był Minister Spraw Wewnętrznych i Administracji. Jedno z nich, a mianowicie **wystąpienie z dnia 28 kwietnia 2011 r.⁴²⁴ dotyczyło ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie (t. j. Dz. U. z 2005 r. Nr 180, poz. 1493 z późn. zm.) i uregulowanej za jej pośrednictwem instytucji gminnych zespołów interdyscyplinarnych realizujących zadania gminy w zakresie przeciwdziałania przemocy w rodzinie.**

Organ do spraw ochrony danych osobowych zwrócił się do **Ministra Spraw Wewnętrznych i Administracji z prośbą o przekazanie organom reprezentującym gminy informacji o obowiązkach wynikających z przepisów ustawy o ochronie danych osobowych.** Generalny Inspektor podniósł bowiem, że każde przedsięwzięcie związane z przetwarzaniem danych osobowych powinno się odbywać z poszanowaniem zasad wynikających z powszechnie obowiązujących przepisów prawa, w szczególności przepisów ustawy o ochronie danych osobowych i wydanych na jej podstawie aktów wykonawczych, o ile przepisy innych aktów prawnych nie określają w sposób szczególny procesu przetwarzania danych osobowych. Zauważył również, że realizując zadania gminy z zakresu przeciwdziałania przemocy w rodzinie zespoły interdyscyplinarne zbierają i przetwarzają szeroki zakres danych osobowych, w tym danych szczególnie chronionych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych. Za konieczne uznał zapewnienie prawidłowego stosowania w pracy zespołów interdyscyplinarnych przepisów prawa, w tym przepisów ustawy o ochronie danych osobowych i przepisów wykonawczych do tejże ustawy. Powołał tym samym regulacje zawarte w art. 37⁴²⁵ i w art. 38⁴²⁶ ustawy o ochronie danych osobowych odwołujących się do

społeczne (ust. 2). Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań (ust. 3).

⁴²³ Zgodnie z art. 27 ust. 1 zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

⁴²⁴ DOLiS-035-1297/11/19860

⁴²⁵ Zgodnie z art. 37 do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

obowiązku nadawania upoważnień osobom dopuszczonym do przetwarzania danych osobowych. Zwrócił również uwagę na art. 39 ust. 1 pkt - pkt 3 ustawy⁴²⁷ oraz sposoby zabezpieczenia danych osobowych⁴²⁸. Generalny Inspektor nadmienił również, iż w przypadku przetwarzania danych osobowych w systemach informatycznych na administratorze danych ciąży obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024). Podniósł również, że administrator danych musi mieć na względzie wymogi bezpieczeństwa danych osobowych w związku z prowadzeniem wszelkiej dokumentacji, w tym dotyczącej również jej obsługi. Organ wskazał, że obowiązki w tym zakresie spoczywać będą na pracownikach zatrudnionych w ośrodku pomocy społecznej w celu obsługi organizacyjno-technicznej zespołu interdyscyplinarnego. Zauważył również, że skoro organ reprezentujący gminę (wójt, burmistrz, prezydent miasta) powołuje zespół interdyscyplinarny, to także w tym zakresie powinno być dokonane zgłoszenie zbioru do rejestracji przez podmiot upoważniony na mocy art. 40 ustawy o ochronie danych osobowych⁴²⁹. W wystąpieniu tym wskazano również, że wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi określa załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. Nr 229, poz. 1536). Uwzględniając powyższe Generalny Inspektor wystąpił o przekazania powyższych uwag wskazanym podmiotom, tak aby proces przetwarzania danych osobowych w celu realizacji zadań z zakresu przeciwdziałania przemocy w rodzinie przebiegał w zgodzie z obowiązującymi przepisami prawa.

W ostatecznej odpowiedzi z dnia 6 września 2011 r.⁴³⁰ Ministerstwo Spraw Wewnętrznych i Administracji poinformowało o przekazaniu stanowiska Generalnego Inspektora do wszystkich

⁴²⁶ Art. 38 stanowi, że administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

⁴²⁷ Zgodnie z art. 39 ust. 1 pkt - pkt 3 ustawy administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: imię i nazwisko osoby upoważnionej (pkt 10), datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych (pkt 2), identyfikator, jeżeli dane są przetwarzane w systemie informatycznym (pkt 4).

⁴²⁸ Art. 39 ust. 2 ustawy wskazuje, że osoby upoważnione do przetwarzania danych osobowych są obowiązane zachować w tajemnicy zarówno te dane, jak i sposoby ich zabezpieczenia.

⁴²⁹ Na mocy art. 40 ustawy o ochronie danych osobowych, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

⁴³⁰ DOLIS-035-1279/11/43729

województw z prośbą o dalsze przekazywanie określonych wytycznych podmiotom, których działalność wiąże się z problematyką poruszoną w przedmiotowym wystąpieniu.

Natomiast w wystąpieniu z dnia 31 maja 2011 r.⁴³¹ dotyczącym **przepisów prawa w związku z procedurą nadawania orderów i odznaczeń** uregulowanych w art. 29 ust. 1 i 2 ustawy z dnia 16 października 1992 r. o orderach i odznaczeniach (t. j. Dz. U. z 1992 r. Nr 90, poz. 450, z późn. zm.), GİODO – powołując się na treść art. 30 ust. 1 i ust. 3, art. 31a oraz art. 31 ust. 4⁴³² - wskazał Ministrowi Spraw Wewnętrznych i Administracji na istnienie dużych rozbieżności dotyczących oceny uprawnień i będących ich wynikiem faktycznych działań podmiotów uprawnionych do kierowania do prezydenta RP wniosków o nadanie odznaczeń.

Wymienione w art. 2 ust. 3 ustawy o orderach i odznaczeniach organy przedstawiają Prezydentowi RP wnioski o nadanie odznaczeń za zasługi w dziedzinach objętych zakresem ich działania. O nadanie odznaczeń osobom związanym z obszarem województwa, miejscem zamieszkania, pracy lub działalności mogą występować wojewodowie, np. w przypadku Medalu za Długoletnie Pożycie Małżeńskie. Z powziętych przez Generalnego Inspektora informacji wynika natomiast, iż zdarzają się przypadki, w których wojewodowie wymagają od organów gmin wypełnienia takich wniosków, co wiąże się z pozyskaniem z Krajowego Rejestru Karnego tzw. danych szczególnie chronionych w rozumieniu ustawy o ochronie danych osobowych. W innych zaś przypadkach organy gminy niejako z własnej inicjatywy podejmują takie działania (przygotowują wniosek w całości) mimo braku kompetencji w tym zakresie - przysługującej wyłącznie wojewodom, jednakże za ich wyraźną aprobatą. Co istotne także, realizacja przez organy uprawnione obowiązku określonego w art. 30 ust. 3⁴³³ powoduje, iż zgłaszającym inicjatywę podawane są informacje pozyskane z Krajowego Rejestru Karnego jako uzasadniające nieprzedstawienie Prezydentowi RP stosownego wniosku. W rezultacie zgłaszający inicjatywę i tak stają się dysponentami przedmiotowych danych osobowych. W związku z powyższym Generalny Inspektor podniósł, iż istniejąca praktyka przesyłania przez organy samorządu terytorialnego wypełnionych wniosków (obejmujących więc dane szczególnie chronione), zważywszy na liczbę wniosków wpływających do wojewodów w tym zakresie, znacznie skraca czas oczekiwania na ich załatwienie, a w efekcie otrzymania Medalu przez jubilatów. Mając zaś na uwadze charakter tego odznaczenia ma to bardzo duże znaczenie. Generalny Inspektor podkreślił, że

⁴³¹ DOLiS-035-1587/11/25412

⁴³² Organ uprawniony występuje do Prezydenta RP z wnioskiem o nadanie orderu lub odznaczenia z własnej inicjatywy lub z inicjatywy jednostek organizacyjnych im podległych, organów samorządowych, organizacji społecznych i zawodowych (art. 30 ust. 1). Wniosek o nadanie orderu lub odznaczenia powinien zawierać informację o karalności osoby, której dotyczy (art. 31a ustawy). Zgodnie z kolei z art. 31 ust. 4 komentowanego aktu prawnego, wnioski o nadanie Medalu za Długoletnie Pożycie Małżeńskie przedstawiają Prezydentowi RP wojewodowie. Nieprzedstawienie Prezydentowi RP wniosku o nadanie orderu lub odznaczenia przez organ uprawniony wymaga zawiadomienia i podania przyczyny zgłaszającemu inicjatywę (art. 30 ust. 3).

⁴³³ Zgodnie z art. 30 ust. 2 nieprzedstawienie Prezydentowi wniosku o nadanie orderu lub odznaczenia przez organ uprawniony, wymaga zawiadomienia i podania przyczyny zgłaszającemu inicjatywę.

określone organy uprawnione są do występowania z wnioskiem o nadanie orderu lub odznaczenia, i tylko tym organom przepisy prawa nadają uprawnione do pozyskania informacji o karalności osoby, której procedura nadania orderu lub odznaczenia dotyczy. Takimi podmiotami nie są zaś jednostki samorządu terytorialnego, organizacje społeczne i zawodowe, z inicjatywy których może być podejmowana procedura nadania orderu lub odznaczenia. Niemniej jednak organ do spraw ochrony danych osobowych zauważył, że stają się one i tak dysponentami takich danych w późniejszym etapie, skoro uzyskują informację o przyczynach niewystąpienia z wnioskiem do Prezydenta RP. Generalny Inspektor poddał zatem pod rozagę Ministrowi Spraw Wewnętrznych i Administracji sposób rozwiązania istniejącego problemu, czy to w drodze odpowiedniej nowelizacji ustawy o orderach i odznaczeniach zmierzającej do przyznania podmiotom występującym z inicjatywą kompetencji przetwarzania informacji stanowiących dane szczególnie chronione w rozumieniu ustawy, bądź też wyraźnego określenia roli ww. z wyłączeniem ich z takich działań, i ograniczeniu obowiązku, o którym mowa w art. 30 ust. 3 ustawy jedynie do powiadomienia zgłaszającemu inicjatywę o nienadaniu tej inicjatywie dalszego biegu. W przedmiotowej bowiem sprawie, jak zwrócił uwagę Generalny Inspektor, istniejące normy kompetencyjne wydają się nie uwzględniać w pełni interesu obywateli. Z jednej strony ich konstrukcja może wydłużać czas oczekiwania na przyznanie odznaczenia, z drugiej jednak przyjęcie rozwiązania powierzającego organom gminy kompetencje w zakresie przetwarzania danych osobowych dotyczących karalności jubilatów, może niekiedy skutkować obawami o naruszenie ich wizerunku w podmiocie zgłaszającym inicjatywę w sytuacji, gdy informacje te nie zostaną odpowiednio zabezpieczone (lub np. gdy krąg osób upoważnionych do ich przetwarzania będzie zbyt rozległy). Argumentując swoje stanowisko odnośnie potrzeby wprowadzenia odpowiednich zmian w przepisach, organ do spraw ochrony danych osobowych odniósł się do zasad wyrażonych w art. 7 Konstytucji RP, który nakazuje, by wszelkie działania organów władzy publicznej były oparte na wyraźnie określonych normach kompetencyjnych. Generalny Inspektor zwrócił również uwagę na brzmienie art. 37a omawianej ustawy⁴³⁴, który odnosi się do nieobowiązującego już art. 28 ustawy o ochronie danych osobowych. Wątpliwości Generalnego Inspektora wzbudziło sformułowanie „przechowywanie (...) danych, nie wymaga zgody osoby, której dane dotyczą”, a właściwie wyraz „przechowywanie”. Odwołał się zatem do art. 7 ust. 2 ustawy o ochronie danych osobowych oraz art. 23 ust.1 i 27 ust. 2 ustawy (w zależności od ich rodzaju) i wskazał, iż każdorazowo dotyczą one przetwarzania w rozumieniu jakichkolwiek operacji, nie zaś jedynie ich przechowywania. Podkreślił, że ograniczenia braku konieczności uzyskiwania zgody osób, których dane dotyczą jedynie do sytuacji przechowywania danych jest wysoce niezrozumiałe, zwłaszcza biorąc pod uwagę fakt, iż przesłanki

⁴³⁴ Przechowywanie zawartych we wnioskach o nadanie orderu, odznaczenia lub tytułu honorowego albo we wnioskach o pozbawienie orderu, odznaczenia lub tytułu honorowego danych osobowych, o których mowa w art. 27 ust. 1 i art. 28 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych nie wymaga zgody osoby, której te dane dotyczą.

legalności przetwarzania danych osobowych są, co do zasady, równoprawne. Istnienie więc przesłanki, o której mowa w art. 23 ust. 1 pkt 2 lub w art. 27 ust. 2 pkt 2 ustawy (przepisów prawa) powoduje, iż pozyskiwanie zgód osób, których dane dotyczą na przetwarzanie (nie tylko przechowywanie) ich danych jest zbędne. Co więcej, istniejący w tym względzie przepis wprowadza w błąd podmioty uczestniczące w procedurze nadawania orderu lub odznaczenia, co do konieczności pozyskiwania zgód osób, których dane dotyczą, na przetwarzanie - w znaczeniu art. 7 pkt 2 ustawy - ich danych. W ocenie organu do spraw ochrony danych osobowych stało się celowe znowelizowanie ustawy o orderach i odznaczeniach, które zdecydowałoby o skreśleniu postanowień jej art. 37a. Generalny Inspektor oczekuje na ustosunkowanie się Ministra Spraw Wewnętrznych i Administracji do tego wystąpienia.

W dniu 29 grudnia 2011 r. Generalny Inspektor został poinformowany przez Ministerstwo Spraw Wewnętrznych o przekazaniu sprawy do Ministerstwa Administracji i Cyfryzacji.

Z kolei wystąpienie z dnia 29 lipca 2011 r. skierowane do **Minister Pracy i Polityki Społecznej**⁴³⁵ dotyczyło rozważenia zainicjowania przez ten podmiot **prac legislacyjnych mających na celu unormowanie w przepisach rangi ustawowej zasad pozyskiwania oraz określenie zakresu danych osobowych przetwarzanych przy rekrutacji do żłobków dzieci w wieku do lat 3.**

Organ do spraw ochrony danych osobowych pozyskał bowiem szereg informacji wskazujących na rozszerzanie przez rady gmin zakresu danych osobowych rodziców (np. dane zawarte w kopii deklaracji podatkowej PIT, czy w zaświadczeniu o zarobkach), pozyskiwanych w toku w/w rekrutacji, w sposób nie wynikający wprost z przepisów ustawy o opiece nad dziećmi oraz wydanych na jej podstawie aktów wykonawczych. Zdaniem organu do spraw ochrony danych osobowych nie ma wątpliwości, że samorząd terytorialny uczestniczy w sprawowaniu władzy publicznej przysługującej mu mocą powszechnie obowiązujących przepisów prawa. Istotną część zadań publicznych powierzonych tymi przepisami samorząd terytorialny wykonuje w imieniu własnym i na własną odpowiedzialność. Bez wątpienia źródłem powszechnie obowiązującego prawa Rzeczypospolitej Polskiej na obszarze działania organów, które je ustanowiły, są również akty prawa miejscowego. Tym niemniej sama Konstytucja RP, przyjmując konstrukcję aktu prawa miejscowego, stanowi, że organy samorządu terytorialnego ustanawiają akty prawa miejscowego obowiązujące na obszarze działania tych organów na podstawie i w granicach upoważnień zawartych w ustawie. Konstytucja również stanowi, że szczególny rodzaj danych, jakie stanowią dane osobowe, może być regulowany jedynie w szczególnym rodzaju aktu powszechnie obowiązującego jakim jest ustawa. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób.

⁴³⁵ DOLiS-035-2170/11/ 36105

Generalny Inspektor podkreślił również, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a zasady i tryb gromadzenia oraz udostępniania informacji określa również ustawa. Generalny Inspektor uznał, że aktami prawnymi, które w pierwszym rzędzie należy brać pod uwagę w omawianej sprawie są: ustawa o ochronie danych osobowych oraz ustawa z dnia 4 lutego 2011 r. o opiece nad dziećmi w wieku do lat 3 (t. j. Dz. U. z 2011 r. Nr 45, poz. 235 z późn. zm.). Zaznaczył, że regulacja zawarta w w/w przepisach nie może być rozszerzana poza ramy ustawowe w drodze uchwały rady gminy, czy miasta (a i z takimi przypadkami mamy do czynienia). Podniósł również, że ustawa o ochronie danych osobowych dopuszcza przetwarzanie danych osobowych po spełnieniu jednej z przesłanek legalizujących dokonywanie jakichkolwiek operacji na danych osobowych, które określone zostały w art. 23 ust. 1 pkt 1 - pkt 5⁴³⁶ ustawy o ochronie danych osobowych i/lub w art. 27 ust. 2 pkt 1 - pkt 10 ustawy o ochronie danych osobowych (w odniesieniu do danych szczególnie chronionych, o których mowa jest w art. 27 ust. 1 ww. ustawy). W szczególności przetwarzanie danych osobowych jest dopuszczalne m.in. gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy) i / lub przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony (art. 27 ust. 2 pkt 2 ustawy). Organ do spraw ochrony danych osobowych zauważył jednak, że aktualnie obowiązujące przepisy ustawy o opiece nad dziećmi w wieku do lat 3 nie regulują zasad rekrutacji dzieci do żłobków, w tym, nie określają katalogu danych osobowych koniecznych dla realizacji celu rekrutacji. O ile zatem dla procesu rekrutacji za niezbędne uznawane są dane z dokumentów (tj. o których mowa na początku pisma, jak kopii deklaracji podatkowej PIT, czy też kopii zaświadczenia o zarobkach) dotyczące rodziców dzieci przyjmowanych do żłobków, to kwestię tę należy uregulować mocą przepisów powszechnie obowiązujących. Ustanowienie odpowiednich przepisów prawa we wskazanym zakresie nie tylko wyeliminuje wątpliwości interpretacyjne, z którymi wielokrotnie spotyka się Generalny Inspektor Ochrony Danych Osobowych, ale przede wszystkim przyczyni się do ochrony praw osób, których dane dotyczą i zapobiegnie dalszej arbitralności i dobrowolności w rozstrzyganiu przez wskazane wcześniej podmioty w przedmiocie dokumentów niezbędnych w procesie rekrutacji do żłobków dzieci w wieku do lat 3. Generalny Inspektor zauważył też, iż ustawa o ochronie danych osobowych wymaga, aby dane osobowe były adekwatne w stosunku do celów, dla jakich są

⁴³⁶ Art. 23. 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

przetwarzane (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych⁴³⁷) i aby swym rodzajem i treścią nie wykraczały poza potrzeby wynikające z celu ich przetwarzania. Jednostki samorządu terytorialnego, jako administratorzy danych⁴³⁸, przy rekrutacji do żłobków mogą zatem przetwarzać jedynie takie dane, które są niezbędne do realizacji ustawowo określonego celu.

W odpowiedzi z dnia 30 sierpnia 2011 r.⁴³⁹ Minister Pracy i Polityki Społecznej zgodziła się z całością argumentacji organu do spraw ochrony danych osobowych uznając jednocześnie za niezbędne podjęcie prac legislacyjnych w zasygnalizowanym zakresie. Generalny Inspektor oczekuje zatem, na przedłożenie projektu zawierającego nowe przepisy, w celu wydania stosownej opinii na temat zgodności przyszłych regulacji z ustawą o ochronie danych osobowych, co wyraził w zreferowanym wyżej wystąpieniu.

W tym miejscu warto również zwrócić uwagę na działania podjęte przez organ do spraw ochrony danych osobowych w roku 2010, w podobnej sprawie dotyczącej rekrutowania dzieci do przedszkoli. Generalny Inspektor skierował w przedmiotowej sprawie wystąpienie do Ministra Edukacji Narodowej, Ministra Spraw Wewnętrznych i Administracji oraz Prezesa Rady Ministrów. Na dzień sporządzenia poniższego podsumowania sprawa wciąż jest monitorowana i stanowi przedmiot szczególnego zainteresowania organu do spraw ochrony danych osobowych.

Wystąpienie z dnia 25 sierpnia 2011 r. również skierowane **do Minister Pracy i Polityki Społecznej**⁴⁴⁰ dotyczyło **potrzeby zmiany obowiązującego wzoru załącznika nr 1 część C do rozporządzenia Ministra Gospodarki i Pracy z dnia 26 listopada 2004 r. w sprawie rejestracji bezrobotnych i poszukujących pracy (Dz. U. z 2004 r. Nr 262, poz 2607 z późn. zm.), poprzez usunięcie z jego treści klauzuli zgody na przetwarzanie danych osobowych.**

Wątpliwości organu do spraw ochrony danych osobowych, wzbudził wzór oświadczenia bezrobotnego, w załączniku nr 1 część C do przedmiotowego rozporządzenia, zawierający klauzulę o treści: „Wyrażam zgodę na przetwarzanie, w rozumieniu przepisów o ochronie danych osobowych, moich danych osobowych dla celów wynikających z ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. Nr 99, poz. 1001)”. Oświadczenie należy podpisać w obecności pracownika powiatowego urzędu pracy. Generalny Inspektor podniósł, że legalność przetwarzania, w tym udostępniania danych osobowych, uzależniona jest od spełnienia jednej z przesłanek wymienionych w art. 23 ust. 1 pkt 1-5 ustawy o ochronie danych osobowych i/lub art. 27 ust. 2, w przypadku przetwarzania danych szczególnie chronionych, w rozumieniu art. 27 ust. 1

⁴³⁷ Art. 26. 1. 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 merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

⁴³⁸ Art. 7 pkt 4 ustawy o ochronie danych osobowych stanowi, że ilekroć w ustawie jest mowa o administratorze danych rozumie się organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.

⁴³⁹ DOLiS-035-2170/11/41896

⁴⁴⁰ DOLiS-035-2427/11/ 40291

ustawy. Podkreślił, że przesłanki legalizujące przetwarzanie danych osobowych mają charakter autonomiczny oraz rozłączny i co do zasady są równoprawne, dlatego też spełnienie jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych. Z punktu widzenia przepisów ustawy o ochronie danych osobowych przetwarzanie danych osobowych jest dopuszczalne m.in. wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy). Tym samym ustawa o ochronie danych osobowych odsyła do przepisów szczególnych, regulujących działalność określonych podmiotów i instytucji, wskazujących w jakich przypadkach i w jakim zakresie mogą one przetwarzać dane osobowe, aby obowiązki i uprawnienia nałożone na nie mocą tych przepisów mogły być realizowane. W tym miejscu Generalny Inspektor wskazał na § 3 ust. 1-5 rozporządzenia Ministra Gospodarki i Pracy w sprawie bezrobotnych i poszukujących pracy⁴⁴¹ i uznał, że o ile przetwarzanie danych osobowych niezbędne jest dla realizacji uprawnień, czy też spełnienia obowiązków wynikających z ustawy o promocji zatrudnienia i instytucjach rynku pracy, to należy uznać, że pozyskiwanie odrębnej zgody na takie przetwarzanie danych osobowych jest zbędne oraz może wprowadzać osoby rejestrujące się w błąd, jako że ww. ustawa daje uprawnienie do przetwarzania danych osobowych m.in. w zakresie niezbędnym do dokonania rejestracji w urzędzie pracy. Podkreślił przy tym, że zgoda jest jednym z możliwych, ale nie jedynym warunkiem legalizującym przetwarzanie danych. Nie jest zatem konieczne jej pozyskiwanie, gdy spełniony jest jeden z pozostałych warunków z art. 23 ust. 1 ustawy, zwłaszcza gdy przetwarzanie danych osobowych znajduje podstawę w stosownych przepisach prawa. Jak zauważył Generalny Inspektor, istnienie komentowanych rozwiązań (w postaci zgody na przetwarzanie danych osobowych w załączniku do rozporządzenia) powoduje, że dopuszczalne jest nieudzielenie zgody na przetwarzanie danych osobowych, co pozostaje w konflikcie z istniejącymi przepisami prawa, z mocy których – a zatem bez odrębnej zgody – przetwarzanie danych osobowych jest dopuszczalne.

W odpowiedzi z dnia 9 września 2011 r.⁴⁴² Minister Pracy i Polityki Społecznej poinformowała Generalnego Inspektora Ochrony Danych Osobowych o trwających pracach nad nowym rozporządzeniem w sprawie rejestracji bezrobotnych i poszukujących pracy, w którym przewidziano odstępianie od w/w klauzuli zgody. Generalny Inspektor zwrócił się natomiast z prośbą o przekazanie dokładniejszych informacji na temat obecnie trwających prac nad treścią przedmiotowego aktu

⁴⁴¹ § 3. 1. Osoba rejestrująca się przedkłada do wglądu pracownikowi powiatowego urzędu pracy dokonującemu rejestracji: 1) dowód osobisty lub inny dokument tożsamości; 2) dyplom, świadectwo ukończenia szkoły lub świadectwo szkolne albo zaświadczenie o ukończeniu kursu lub szkolenia; 3) świadectwa pracy oraz inne dokumenty niezbędne do ustalenia jej uprawnień; 4) dokument stwierdzający przeciwwskazania do wykonywania określonych prac, jeżeli taki dokument posiada. 2. Osoba niepełnosprawna, oprócz dokumentów, o których mowa w ust. 1, przedkłada dokument potwierdzający stopień niepełnosprawności. 3. Powiatowy urząd pracy może sporządzać kserokopie dokumentów, o których mowa w ust. 1 pkt 2 i 3, oraz notatki z dokumentów, o których mowa w ust. 1 pkt 1, 4 i ust. 2, w zakresie niezbędnym do ustalenia uprawnień. 4. Rejestracji nie dokonuje się w przypadku nieprzedłożenia dokumentów, o których mowa w ust. 1 pkt 1-3 i ust. 2, lub odmowy złożenia podpisu na karcie rejestracyjnej przez osobę rejestrującą się. 5. W szczególnie uzasadnionych przypadkach starosta może wyrazić zgodę na rejestrację osoby nieposiadającej kompletu dokumentów.

⁴⁴² DOLiS-035-2725/11/48006

wykonawczego⁴⁴³. Wyraził również przekonanie, że projekt rozporządzenia zostanie przedłożony Generalnemu Inspektorowi celem zaopiniowania jego treści pod względem zgodności z ustawą o ochronie danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych w wystąpieniu z dnia 30 sierpnia 2011 r.⁴⁴⁴ skierowanym do **Minister Zdrowia** sygnalizował potrzebę **podjęcia prac legislacyjnych mających na celu wprowadzenie podstaw prawnych dla zlecania informatycznej obsługi procesu przetwarzania danych osobowych przez administratorów danych przetwarzających dane osobowe pacjentów, w związku z udzielaniem świadczeń zdrowotnych innym wyspecjalizowanym w tym zakresie podmiotom.**

Generalny Inspektor Ochrony Danych Osobowych wskazał, że problem braku odpowiedniej podstawy prawnej korzystania przez podmioty udzielające świadczeń zdrowotnych ze specjalistycznych usług w modelu tzw. outsourcingu, w praktyce wzbudza wiele wątpliwości i było przedmiotem wielu pytań kierowanych do organu ochrony danych osobowych. Ze względu na szczególny charakter kategorii danych, do jakiej należą dane o stanie zdrowia, ustawa o ochronie danych osobowych zapewnia wysoki reżim ich ochrony. Generalny Inspektor przypomniał również, że zgodnie z art. 27 ustawy, przetwarzanie powyższych danych jest co do zasady zabronione. Zasada ta doznaje wyjątków jedynie w przypadkach enumeratywnie wyliczonych w art. 27 ust. 2 ustawy. Nadmienił, że wobec jednoznacznej dyspozycji art. 27 ust. 2 pkt 2 ustawy, gdyby podstawę dla przetwarzania danych sensytywnych miałby stanowić przepis ustawy, musiałby on spełniać określone w tym punkcie kryteria.⁴⁴⁵ Generalny Inspektor podniósł, że w obecnym stanie prawnym dopuszczalność przekazywania przez podmioty sektora ochrony zdrowia danych osobowych pacjentów wyspecjalizowanym podmiotom w celu obsługi procesu przetwarzania danych w systemach informatycznych budzi zastrzeżenia przede wszystkim ze względu na istnienie tajemnicy zawodowej określonej w art. 13⁴⁴⁶ i 14⁴⁴⁷ ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t. j. Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.). Wskazał również, że obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku

⁴⁴³ DOLiS-035-2427/11/46978

⁴⁴⁴ DOLiS-035-2464/11/41153

⁴⁴⁵ Art. 27 ust. 2 pkt 2, przetwarzanie danych szczególnie chronionych, do jakich należą dane o stanie zdrowia, jest dopuszczalne, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

⁴⁴⁶ Art. 13. Pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego.

⁴⁴⁷ Art. 14. 1. W celu realizacji prawa, o którym mowa w art. 13, osoby wykonujące zawód medyczny są obowiązane zachować w tajemnicy informacje związane z pacjentem, w szczególności ze stanem zdrowia pacjenta. 2. Przepisu ust. 1 nie stosuje się, w przypadku gdy: 1) tak stanowią przepisy odrębnych ustaw; 2) zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób; 3) pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy; 4) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu tych świadczeń. 3. Osoby wykonujące zawód medyczny, udzielające świadczeń zdrowotnych, z wyjątkiem przypadków, o których mowa w ust. 2 pkt 1-3, są związane tajemnicą również po śmierci pacjenta.

z wykonywaniem zawodu wynika również m.in. z przepisów ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (t. j. Dz. U. 2008 r. Nr 136 poz. 857 z późn. zm.), ustawy z dnia 5 lipca 1996 r. o zawodach pielęgniarki i położnej (t. j. Dz. U. z 2009 r. Nr 151 poz. 1217 z późn. zm.), ustawy z dnia 20 lipca 1950 r. o zawodzie felczera (t. j. z Dz. U. 2004 r. Nr 53 poz. 531 z późn. zm.). Zdaniem organu do spraw ochrony danych osobowych, przyjęte w przytoczonych przepisach gwarancje ochrony prywatności pacjentów są niewątpliwie niezbędne i uzasadnione. Jednakże powyższy sposób ukształtowania ochrony prywatności pacjentów nie uwzględnia niezwykle istotnego problemu, jakim jest obsługa procesu przetwarzania danych w systemach informatycznych, czy specjalistycznego sprzętu diagnostycznego rejestrującego dane osobowe na rzecz podmiotów świadczących usługi zdrowotne. Delegowanie powyższych zadań na zewnątrz pozwalające m.in. na korzystanie ze specjalistycznej wiedzy przy znacznej redukcji kosztów jest szczególnie powszechne wśród małych i średnich podmiotów świadczących usługi lecznicze. Generalny Inspektor zaznaczył, że aby przekazywanie danych osobowych przez administratorów danych przetwarzających dane osobowe pacjentów w związku z udzielaniem świadczeń zdrowotnych innym wyspecjalizowanym w tym zakresie podmiotom było zgodne z prawem, konieczne jest istnienie odpowiedniej dla takiego działania podstawy prawnej. Argumentując swoje stanowisko wskazał, że ustawa o ochronie danych osobowych przewiduje możliwość powierzenia przetwarzania danych osobowych w art. 31⁴⁴⁸. Zaznaczył również, że w przepisach ustawy nie ma przy tym żadnych zastrzeżeń co do możliwości powierzenia do przetwarzania także danych szczególnie chronionych, do których zalicza się dane o stanie zdrowia. Generalny Inspektor podkreślił, że przedmiotem powierzenia przetwarzania danych osobowych może być przy tym zarówno kompleksowa obsługa procesu przetwarzania danych dla określonego celu, jak i jedynie tylko niektóre operacje na danych, jak np. ich przechowywanie czy usuwanie. W ocenie GODO należy mieć również świadomość, że umowa powierzenia przetwarzania danych jest często prawną podstawą dostępu do danych osobowych dla zapewnienia konserwacji i naprawy oprogramowania i sprzętu informatycznego lub diagnostycznego. Generalny Inspektor zaznaczył również, że stosowanie instytucji powierzenia danych może jednak budzić wątpliwości w odniesieniu do informacji, w tym danych osobowych, objętych zakresem ustawowych tajemnic wynikających z przepisów dotyczących wykonywania zawodów medycznych. Wynika to ze wzajemnego stosunku przepisów ustawy o ochronie danych osobowych i ustaw do niej szczególnych, który oceniać należy na

⁴⁴⁸ Art. 31. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. 2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. 3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych. 4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. 5. Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.

gruncie art. 5 ustawy o ochronie danych osobowych.⁴⁴⁹ Powierzenie przetwarzania danych osobowych następuje bez konieczności uzyskiwania zgody osób, których dane dotyczą. Jednakże w razie związania tajemnicą zawodową, każdy przypadek posłużenia się podwykonawcą w związku z przetwarzaniem danych wymaga istnienia przepisu rangi ustawy, który na takie działanie wprost zezwala. Organ do spraw ochrony danych osobowych zaznaczył, że analogiczna relacja zachodzi pomiędzy przepisami ustawy o ochronie danych osobowych a innymi regulacjami sektorowymi uwzględniającymi szczególne zagrożenia dla sfery prywatności i wprowadzającymi tajemnice zawodowe, np. ustawie z dnia 29 sierpnia 1997 r. Prawo bankowe (t. j. Dz. U. 2002 r. Nr 72 poz. 665 z późn. zm.), ustawie z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. Nr 11, poz. 66), ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t. j. Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.). Na gruncie wymienionych przepisów Generalny Inspektor zauważył, iż przewidziano możliwość przekazywania danych niezbędnych do prowadzenia odpowiednio: działalności bankowej, ubezpieczeniowej czy telekomunikacyjnej innym podmiotom przez podmioty prowadzące ww. rodzaje działalności oraz jednocześnie rozciągnięto na powyższe podmioty współpracujące obowiązek zachowania ustawowej tajemnicy. Niemniej jednak uchwalone w ostatnim czasie: ustawa o działalności leczniczej, mająca zastąpić ustawę z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (t. j. Dz. U. 2007 r. Nr 14 poz. 89 z późn. zm.) oraz ustawa o systemie informacji w ochronie zdrowia, nie przewidują rozwiązań dotyczących omawianego problemu. Do powierzenia zadań publicznych oraz zapewnienia dostępu do danych zgromadzonych w rejestrach publicznych w zakresie zadań realizowanych m.in. przez samodzielne publiczne zakłady opieki zdrowotnej, odnoszą się przepisy ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t. j. Dz. U. Nr 64, poz. 565 z późn. zm.). Analizując przedmiotowy problem Generalny Inspektor wskazał art. 2⁴⁵⁰ oraz 15⁴⁵¹ w/w ustawy oraz art. 13 i 14 ustawy z dnia

⁴⁴⁹ Art. 5. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

⁴⁵⁰ Art. 2. 1. Z zastrzeżeniem ust. 2-4, przepisy ustawy stosuje się do realizujących zadania publiczne określone przez ustawy: 1) organów administracji rządowej, organów kontroli państwowej i ochrony prawa, sądów, jednostek organizacyjnych prokuratury, a także jednostek samorządu terytorialnego i ich organów, 2) jednostek budżetowych i samorządowych zakładów budżetowych, 3) funduszy celowych, 4) samodzielnych publicznych zakładów opieki zdrowotnej oraz spółek wykonujących działalność leczniczą w rozumieniu przepisów o działalności leczniczej, 5) Zakładu Ubezpieczeń Społecznych, Kasy Rolniczego Ubezpieczenia Społecznego, 6) Narodowego Funduszu Zdrowia, 7) państwowych lub samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw w celu realizacji zadań publicznych - zwanych dalej „podmiotami publicznymi”. 2. Przepis art. 13 ust. 2 pkt 1 stosuje się również do podmiotu, któremu podmiot publiczny powierzył lub zlecił realizację zadania publicznego, jeżeli w związku z realizacją tego zadania istnieje obowiązek przekazywania informacji do lub od podmiotów niebędących organami administracji rządowej. 3. Przepisów ustawy nie stosuje się do przedsiębiorstw państwowych, spółek handlowych, służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154), Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej oraz Narodowego Banku Polskiego, poza przypadkami gdy w związku z realizacją zadań przez te podmioty istnieje obowiązek przekazywania informacji do i od podmiotów niebędących organami administracji rządowej; w takich przypadkach stosuje się art. 13 ust. 2 pkt 1 niniejszej ustawy. 4. Przepisów rozdziału 4 nie stosuje się do jednostek badawczo-rozwojowych, uczelni publicznych, Polskiej Akademii Nauk i tworzonych przez nią jednostek organizacyjnych, Rzecznika Praw Obywatelskich, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii

6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Uznał tym samym, że żaden z przepisów ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne nie odnosi się w sposób bezpośredni do informacji dotyczących pacjentów objętych tajemnicą na podstawie przepisów szczególnych. W konsekwencji uznał, że przepisy te nie stanowią wyjątku od zasady przyjętej w art. 14 ust. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, tj. zasady zobowiązującej do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające pacjentowi świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego. Organ do spraw ochrony Danych Osobowych podniósł, że prawidłowo skonstruowana podstawa prawna dla przekazywania danych pacjenta objętych tajemnicą zawodową powinna w sposób wyraźny określać krąg podmiotów uprawnionych do dostępu do informacji objętych tajemnicą, a ponadto cel i zakres tego udostępnienia. W ocenie Generalnego Inspektora, niezbędne jest wprowadzenie dodatkowego przepisu rozciągającego obowiązek zachowania powyższej tajemnicy na podmioty, którym informacje te będą powierzane. Jedynie w ten sposób zapewnione zostałyby gwarancje ochrony prywatności pacjentów i zachowania tajemnicy informacji uzyskiwanych w związku z wykonywaniem zawodu medycznego.

W odpowiedzi z dnia 5 października 2011 r. Minister Zdrowia wyraziła zdanie przeciwne wobec stanowiska Generalnego Inspektora Ochrony Danych Osobowych. Wskazała, że nieadekwatne w stanowisku Generalnego Inspektora były przykłady zaczerpnięte z prawa bankowego oraz innych ustaw. Zdaniem Minister Zdrowia powierzenie przetwarzania danych osobowych pacjentów przez podmioty udzielające świadczeń zdrowotnych dotyczy jedynie przechowywania dokumentacji medycznej sporządzonej w postaci elektronicznej. Konkludując, zdaniem Minister, przepisy ustawy o ochronie danych osobowych stanowią wystarczającą podstawę do zawierania przedmiotowych umów powierzenia. Mimo tego, organ do spraw ochrony danych osobowych przedstawił w/w problem nowemu Ministrowi Zdrowia pismem z dnia 13 grudnia 2011 r. i oczekuje na jego odpowiedź.

Wśród przedstawionych sygnalizacji na uwagę zasługuje także wystąpienie Generalnego Inspektora Ochrony Danych Osobowych do **Komendanta Powiatowego Policji w Żarach** z dnia 21 grudnia 2011 r. **Dotyczyło ono upublicznienia w Internecie nagrania telefonicznej prośby**

i Telewizji, Krajowego Biura Wyborczego, Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Generalnego Inspektora Ochrony Danych Osobowych, Komisji Nadzoru Finansowego oraz Generalnego Inspektora Informacji Finansowej.

⁴⁵¹ Art. 15. 1. Podmiot prowadzący rejestr publiczny zapewnia podmiotowi publicznemu albo podmiotowi niebędącemu podmiotem publicznym, realizującym zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny ich realizacji, nieodpłatny dostęp do danych zgromadzonych w prowadzonym rejestrze, w zakresie niezbędnym do realizacji tych zadań. 2. Dane, o których mowa w ust. 1, powinny być udostępniane za pomocą środków komunikacji elektronicznej i mogą być wykorzystane wyłącznie do realizacji zadań publicznych. 3. Rada Ministrów określi, w drodze rozporządzenia, sposób, zakres i tryb udostępniania danych, o których mowa w ust. 1, mając na uwadze potrzebę usprawnienia realizacji zadań publicznych, zapewnienia szybkiego i bezpiecznego dostępu do danych oraz zabezpieczenia wykorzystania danych do celów realizacji zadań publicznych.

o interwencję skierowanej do Powiatowej Komendy, co przypuszczalnie było skutkiem nieprawidłowego zabezpieczenia danych osobowych przez administratora. Nagranie to zawierało dane osobowe osoby kontaktującej się z komendą.

W przedmiotowym wystąpieniu Generalny Inspektor wskazał, że każdej osobie przysługuje prawo do ochrony jej życia prywatnego. Zwrócił również uwagę na treść rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i administracyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). Ponadto Generalny Inspektor wskazał zasady wynikające z art. 26 ustawy o ochronie danych osobowych oraz obowiązki administratora danych określone w art. 36 i 37 ustawy. Zaznaczył, że ujawnianie przez funkcjonariuszy Policji danych osobowych osobom nieuprawnionym prowadzi nie tylko do naruszenia zasady bezpieczeństwa danych osobowych wynikającej z ustawy, ale może również stanowić naruszenie przepisów ustawy z dnia 6 kwietnia 1990 r. o Policji (t. j. Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.). W ocenie organu do spraw ochrony danych osobowych nieprawidłowości, których dotyczyło wystąpienie zwracają uwagę także w kontekście naruszenia zaufania, jakim jest obdarzona w systemie państwa i w samym społeczeństwie instytucja Policji. Generalny Inspektor podkreślił, że zadaniem Policji jest ochrona porządku publicznego i zabezpieczenie przestrzegania przepisów prawa, a w sytuacji ich naruszenia – ściganie takich czynów. Wobec tego, zachowania mogące stanowić naruszenie przepisów prawa, w tym ustawy o ochronie danych osobowych, nie powinny mieć miejsca ze strony Policji.

W odpowiedzi z dnia 30 grudnia 2011, Komendant Powiatowy Policji poinformował, iż powiadomił o przedmiotowym incydencie Biuro Spraw Wewnętrznych Komendy Głównej w Warszawie. Komendant wyjaśnił również, że sprawa stała się przedmiotem postępowania Prokuratury Rejonowej w Żaganiu a on sam podejmie odpowiednie postępowanie dyscyplinarne po tym jak zostanie zakończone śledztwo prokuratorskie. Komendant wyraził również przekonanie, że przedmiotowa sprawa nie powtórzy się w przyszłości.

W październiku 2011 r. Generalny Inspektor został poinformowany przez Prezesa Polskiej Izby Informatyki i Telekomunikacji, że w ramach Grupy Internet działającej przy Ministrze Kultury i Dziedzictwa Narodowego przygotowano *„Porozumienie o współpracy i wzajemnej pomocy w sprawie ochrony praw własności intelektualnej w środowisku cyfrowym”*. Kształt tego porozumienia wyłożonego do podpisu 6 października 2011 r. zaniepokoił Izbę na tyle, że postanowiła zwrócić się do GIODO o przyjrzenie się dokumentowi zanim zaczną doń przystępować sygnatariusze. Porozumienia takie jak przekazane przez Izbę, stanowią zdaniem GIODO wypełnienie norm wynikających z art. 27 ust. 3 Umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA), która w tym samym czasie przygotowana była do

podpisania przez Radę Unii Europejskiej (w której Polska sprawowała przewodnictwo) oraz przez państwa członkowskie UE.

W powiązaniu z normą z art. 27 ust. 4 przekazane GİODO Porozumienie może prowadzić do stworzenia alternatywnej metody wymiany danych osobowych pomiędzy podmiotami będącymi sygnatariuszami Porozumienia. Art. 4 Porozumienia wskazuje bowiem, że „sygnatariusze będą przekazywali sobie wzajemnie informacje o ujawnionych faktach naruszeń praw własności intelektualnej”. Art. 3 tego samego Porozumienia stwierdza, że uprawniony może monitorować środowisko cyfrowe w celu identyfikacji oraz rozpoznawania naruszeń praw własności intelektualnej. Jednocześnie Porozumienie przewiduje nakładanie na usługodawców obowiązków, których nie przewiduje dzisiejsze prawo polskie. Przykładem jest obowiązek wprowadzenia stosownych warunków i procedur, które doprowadzą do zabezpieczenia posiadanych informacji niezbędnych do identyfikacji użytkownika, który dopuścił się naruszeń przy jednoczesnym stwierdzeniu, że zasady korzystania z informacji uzyskanych w ten sposób zostaną uregulowane przez sygnatariuszy – jak rozumiem w kolejnych Porozumieniach (art. 9 i 11 Porozumienia).

W piśmie skierowanym do Pana Prezesa Polskiej Izby Informatyki i Telekomunikacji dra Wacława Iszkowskiego z dnia 9 listopada 2011 r. Generalny Inspektor Ochrony Danych Osobowych stwierdził m.in.:

„Bardzo niekonkretnie sformułowania użyte w porozumieniu oraz zdawkowy opis systemu służącego do przekazywania informacji (lub czystych danych) pomiędzy stronami porozumienia zdaje się sugerować, że tekst tego dokumentu nie był przygotowywany przez osoby posiadające wystarczającą zakresu zasad ochrony prywatności i ochrony danych osobowych w prawie polskim i europejskim. Nie sądzę więc by prawnicy Ministerstwa Kultury i Dziedzictwa Narodowego – których wiedzę bardzo cenię – uczestniczyli w przygotowaniu tego dokumentu.”

Ponieważ dalsze zdarzenia sugerowały jednak, że urzędnicy Ministerstwa Kultury i Dziedzictwa Narodowego byli jednak zaangażowani w te prace, Generalny Inspektor uznał, że *Porozumienie* jest de facto wypełnieniem normy wynikającej z art. 27 ust. 3 planowanej do podpisania Umowy ACTA, jako że stanowi „wsparcie wspólnych wysiłków przedsiębiorców na rzecz skutecznego zwalczania naruszeń praw związanych ze znakami towarowymi, praw autorskich lub praw pokrewnych”.

W tej sytuacji Generalny Inspektor zwrócił się do Ministra Kultury i Dziedzictwa Narodowego z wystąpieniem w którym zwrócił uwagę na fakt, że Biuro GİODO nie miało wcześniej okazji uczestniczenia w żadnych pracach nad tym dokumentem. GİODO uznał, że nie ma żadnych wątpliwości, że dane, o których mowa w *Porozumieniu* m.in. jako o „informacjach o przypadkach naruszeń praw własności intelektualnej” (art. 7 Porozumienia) mogą stanowić dane osobowe w rozumieniu art. 6 ust. 1 ustawy o ochronie danych osobowych. Opisane bardzo ogólnie w dokumencie procesy przetwarzania tych danych są niewątpliwie operacjami przetwarzania danych, o których mówi ustawa. Generalny Inspektor Ochrony Danych Osobowych, ma nie tylko prawo, ale też obowiązek podejmowania działań mających na celu stanie na straży praworządności w

Rzeczypospolitej Polskiej w zakresie uprawnień, których sposoby realizacji zostały określone w ustawie o ochronie danych osobowych. Stąd też Porozumienie stało się przedmiotem zainteresowania GODO.

Ponieważ Konstytucja Rzeczypospolitej Polskiej w art. 47 gwarantuje wszystkim osobom znajdującym się pod władzą Rzeczypospolitej Polskiej prawo do ochrony życia prywatnego, a w myśl postanowień zawartych w art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób, administrator danych osobowych, stosując w swej działalności zasady ochrony danych osobowych, powinien dopełniać obowiązku dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt 1-4 ustawy o ochronie danych osobowych). Brak natomiast spełnienia przesłanki legalności przetwarzania danych osobowych rodzić po stronie administratora danych m.in. odpowiedzialność karną.

Generalny Inspektor podkreślił, że z zasady popiera idee dążące do samoregulacji rynku, a kwestie ochrony praw własności intelektualnej są dla jego prac bardzo istotne. Jednak proponowane *Porozumienie* należy uznać za rozwiązanie chybione. Rozwiązanie to może prowadzić do stworzenia systemu informacyjnego, który nie znajduje podstaw prawnych, a którego istnienie jest ingerencją w konstytucyjne prawa osób fizycznych nieadekwatną dla planowanego celu. W kilka dni po przesłaniu stanowiska GODO Ministerstwo Kultury i Dziedzictwa Narodowego poinformowało o wstrzymaniu prac nad „*Porozumieniem o współpracy i wzajemnej pomocy w sprawie ochrony praw własności intelektualnej w środowisku cyfrowym*”. Problem powrócił w 2012 r. podczas dyskusji nad podpisaniem i ratyfikacją przez Polskę umowy ACTA.

6.2. Działalność informacyjna

W celu upowszechniania wiedzy z zakresu ochrony danych osobowych, Generalny Inspektor w 2011 r., 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.godo.gov.pl) będącej jednocześnie Biuletynem Informacji Publicznej. W grudniu 2011 r. uruchomił zaś newsletter, dostarczany wszystkim,

wyrażającym chęć jego otrzymywania poprzez zarejestrowanie się za pośrednictwem strony internetowej GIODO.

Informacje do pojedynczych odbiorców trafiały zarówno w formie pism, jak i ustnych wyjaśnień udzielanych za pośrednictwem, działającego w godzinach pracy Biura, telefonu informacyjnego oraz indywidualnych spotkań interesantów 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.

6.2.1 Współpraca ze środkami masowego przekazu

1. Stałe kontakty z mediami

W celu upowszechniania wiedzy o ochronie danych osobowych, GIODO – wzorem lat ubiegłych – w roku 2011 kontynuował stałą współpracę z mediami polegającą na przekazywaniu do publikacji opracowanych przez GIODO materiałów informacyjno-edukacyjnych. Taka 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”, „Wspólnotą” oraz portalami będącymi zarówno odpowiednikami prasy drukowanej, jak i innymi, jak np. Dziennik Internautów, gazeta.pl. czy lex.pl. Dodatkową formą upowszechniania wiedzy z zakresu ochrony danych osobowych była publikacja wyjaśnień GIODO w czasopismach kobiecych, przede wszystkim w „Twoim Imperium” czy „Tinie”. W 2011 r. GIODO zainicjował ponadto stałe kontakty m.in. z „Pulsem Biznesu”, Serwisem Samorządowym PAP, miesięcznikami „IT w Administracji” oraz „Kadra Kierownicza w Administracji” oraz tygodnikiem „Uważam Rze”, co zaowocowało regularnym upowszechnianiem w tych mediach problematyki z zakresu ochrony danych osobowych.

Dzięki stałej współpracy z wymienionymi wyżej mediami, w 2011 r. zostało opublikowanych lub wyemitowanych około **150 materiałów prasowych** poświęconych tej tematyce. Większość z nich jest dostępna na stronie internetowej GIODO.

2. Odpowiedzi na indywidualne pytania dziennikarzy

Stałą formą kontaktów GIODO z dziennikarzami było udzielanie im odpowiedzi na przesłane pytania dotyczące ochrony danych osobowych. W 2011 r. GIODO udzielił – pisemnie lub telefonicznie – około **260** takich odpowiedzi. Wśród problemów, z którymi najczęściej zgłaszali się przedstawiciele mediów, były m.in.:

- przetwarzanie danych osobowych z wykorzystaniem nowoczesnych technologii, zwłaszcza modelu *cloud computing*,
- funkcjonowanie portali społecznościowych,
- tworzenie nowych rejestrów publicznych, zwłaszcza w sektorze edukacji i ochrony zdrowia, w tym zakres danych osobowych w nich gromadzonych i ich zabezpieczenie,
- zasady przetwarzania danych osobowych dłużników,
- wykorzystywanie danych osobowych na potrzeby marketingu,
- ochrona danych osobowych w procesie rekrutacji i zatrudnienia,
- dopuszczalność przetwarzania przez pracodawców danych biometrycznych pracowników,
- wycieki danych osobowych zarówno z instytucji publicznych, jak i prywatnych,
- zabezpieczanie danych osobowych, jako główny problem w związku ze stosowaniem nowych technologii,
- zasady przetwarzania danych osobowych przez kościoły i związki wyznaniowe,
- warunki świadczenia usługi *Google Street View*,
- zasady przetwarzania danych osobowych przedsiębiorców,
- upublicznianie przez jednostki samorządu terytorialnego danych osobowych zarówno w BIP, jak i w uchwałach czy decyzjach,
- podawanie do publicznej wiadomości wykazu osób, którym udzielono ulg, odroczone, umorzono bądź rozłożono na raty spłatę podatków lub opłat lokalnych,
- możliwość stosowania monitoringu wizyjnego przez podmioty inne niż ustawowo upoważnione,
- przetwarzanie danych osobowych na potrzeby kampanii wyborczej.

3. Wywiady i wystąpienia

Jedną z form działalności edukacyjno-informacyjnej były wywiady radiowe i telewizyjne, których w 2011 r. GIODO udzielił blisko **260**. 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

marketingowym, mieszkalnictwa, oświaty i służby zdrowia. Wiele wywiadów i wypowiedzi GODO 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 przeglądarek internetowych, jak np. Google. Wśród innych tematów rozmów związanych z wykorzystaniem nowoczesnych technologii wymienić można: wyłudzenie bądź wykradanie danych osobowych, monitorowanie pracowników czy tworzenie profili osobowych.

Zmiany w przepisach dotyczących funkcjonowania systemu informacji oświatowej oraz tworzenie systemu informacji w ochronie zdrowia to kolejny temat częstych wystąpień medialnych GODO w 2011 r.

Duże zainteresowanie mediów budziła także kwestia zmian prawa regulującego ochronę danych osobowych, zarówno tych wprowadzonych wchodzącą w życie 7 marca 2011 r. nowelizacją ustawy o ochronie danych osobowych, jak i tych planowanych na poziomie Unii Europejskiej.

Ponadto GODO niejednokrotnie udzielał wywiadów poświęconych wyciekom danych osobowych, bezpiecznemu korzystaniu z Internetu, zasadom przetwarzania danych osobowych w chmurach obliczeniowych, a także tworzenia przez przedsiębiorców profili osobowych klientów.

a) **Konferencje i spotkania prasowe**

W związku z potrzebą nagłośnienia niektórych wydarzeń lub upublicznienia stanowiska GODO w istotnych sprawach, GODO w 2011 r. zorganizował 14 konferencji prasowych. Poświęcone one były:

- obchodom V Dnia Ochrony Danych Osobowych, zarówno wydarzeniom mającym miejsce w Brukseli (26 stycznia 2011 r.), jak i w Polsce (31 stycznia 2011 r. w Warszawie),
- kontroli zabezpieczenia danych osobowych przetwarzanych na potrzeby przeprowadzenia Narodowego Spisu Powszechnego Ludności i Mieszkań w 2011 r. Organizacja tej konferencji wywołana była m.in. doniesieniami medialnymi dotyczącymi np. możliwości podszycia się pod inną osobę przy wypełnianiu formularza internetowego na potrzeby spisu powszechnego oraz pozyskania danych osób fizycznych przez osoby do tego niepowołane (7 kwietnia 2011 r.),
- ochronie danych osobowych w dobie rozwoju nowoczesnych technologii, który wymusza dokonanie zmian obecnie obowiązujących przepisów prawa dotyczących ochrony prywatności i danych osobowych, które tworzone były w latach dziewięćdziesiątych XX wieku. Zarówno unijne, jak i polskie przepisy odnoszą się do zupełnie innej rzeczywistości, stąd zachodzi konieczność ich zmian (16 maja 2011 r.),
- przekazaniu informacji o skierowaniu przez GODO pierwszego wystąpienia w trybie art. 19a ustawy o ochronie danych osobowych mającego na celu ochronę prywatności członków

zarządów fundacji oraz o otrzymanej na nie odpowiedzi.. GIODO zwrócił się bowiem do Ministra Sprawiedliwości o dokonanie takich zmian w przepisach, aby w zamieszczanych w Internecie sprawozdaniach z działalności fundacji nie widniały prywatne adresy zamieszkania członków ich zarządów. Minister Sprawiedliwości podzielił stanowisko GIODO i poinformował o rozpoczęciu stosownych prac legislacyjnych (24 maja 2011 r.),

- dopuszczalności tworzenia profili osobowych, ale dopiero po spełnieniu określonych warunków. Takie działanie musi być zasadne, prowadzone na określonej podstawie prawnej, a osoby, których dane są w ten sposób przetwarzane, muszą mieć tego świadomość (25 maja 2011 r.),
- przedstawieniu wyników kontroli GIODO w sprawie zabezpieczenia danych osobowych przetwarzanych na potrzeby Narodowego Spisu Powszechnego Ludności i Mieszkań w 2011 r. (30 maja 2011 r.),
- upowszechnieniu efektów programu „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”. Program był realizowany przez Gliwicki Ośrodek Metodyczny we współpracy z Generalnym Inspektorem Ochrony Danych Osobowych. Jego efektem jest m.in. opracowanie modelowych scenariuszy lekcji oraz przeszkolenie grupy nauczycieli - trenerów, których rolą jest teraz przekazywanie tej wiedzy innym (2 czerwca 2011 r.),
- omówieniu zagadnień związanych ze stosowaniem wiążących reguł korporacyjnych, w tym postulowanego uproszczenia procedury ich zatwierdzania. W opinii GIODO, przedsiębiorstwom o zasięgu międzynarodowym, które wdrożą europejskie normy ochrony danych osobowych, trzeba ułatwić przesyłanie danych wewnątrz korporacji (14 czerwca 2011 r.),
- przetwarzaniu danych osobowych kibiców - konferencja ta została zorganizowana w związku z docierającymi do GIODO sygnałami o nieprawidłowościach w przetwarzaniu danych osobowych kibiców klubów piłkarskich oraz trwającą sektorową kontrolą GIODO potwierdzającą te sygnały, a także dobiegającymi końca pracami parlamentarnymi nad nowelizacją ustawy o bezpieczeństwie imprez masowych. GIODO w czasie jej trwania wyjaśniał, że kibice muszą przekazywać klubom piłkarskim tylko te dane osobowe, które służą ich identyfikacji niezbędnej dla zapewnienia bezpieczeństwa. Pozostałe dane osobowe kluby mogą zbierać jedynie za zgodą kibiców i to wyrażoną świadomie i dobrowolnie (17 sierpnia 2011 r.),
- przetwarzaniu danych osobowych wyborców - konferencja ta została zorganizowana w związku z opracowaniem przez GIODO poradnika dotyczącego zasad wykorzystywania danych

osobowych na potrzeby przeprowadzenia wyborów, w tym kampanii wyborczej (19 sierpnia 2011 r.),

- zasadom ochrony danych osobowych w placówkach oświatowych - konferencja ta została zorganizowana w związku z udziałem GIODO w odbywającej się 18 i 19 października 2011 r. w Łodzi XIII Krajowej Konferencji Dyrektorów Szkół i Przedszkoli. GIODO poinformował media m.in., że szkoły, gromadząc wiele informacji o uczniach, ich rodzicach bądź opiekunach oraz o nauczycielach, są zobowiązane do właściwej ochrony tych danych (18 października 2011 r.),
- przetwarzaniu danych osobowych studentów, absolwentów oraz pracowników naukowych uczelni wyższych - konferencja ta została zorganizowana, by zwrócić uwagę opinii publicznej na zasady, jakich uczelnie wyższe powinny przestrzegać przy przetwarzaniu danych osobowych studentów, absolwentów oraz pracowników naukowych uczelni wyższych. Podczas jej trwania GIODO wskazywał, że uczelnie wyższe na potrzeby monitorowania karier zawodowych absolwentów mogą pozyskiwać ich dane osobowe jedynie na podstawie dobrowolnej zgody (27 października 2011 r.),
- zaprezentowaniu stanowiska GIODO dotyczącego konieczności zmiany przepisów regulujących upublicznianie danych osobowych podatników, którym w zakresie podatków lub opłat udzielono ulg, odroczeń, umorzeń lub rozłożono spłatę na raty, o zmianę których GIODO wystąpił do Ministra Finansów (15 grudnia 2011 r.).

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

b) 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 2011 r. w ten właśnie sposób rozpropagowane zostały obchody V Dnia Ochrony Danych Osobowych.

W 2011 r. miały one szczególny charakter, gdyż w tym właśnie roku 28 stycznia minęło 30 lat od uchwalenia Konwencji 108 Rady Europy 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 28 stycznia 2011 r. w Brukseli odbyła się konferencja zorganizowana przez Komisję Europejską i Radę Europy pt. „Ochrona danych (30 lat później): od europejskich do międzynarodowych standardów”, zaś GIODO był moderatorem jednego z dwóch paneli pt. „Od europejskich do międzynarodowych standardów ochrony danych”.

Podobnie jak w latach ubiegłych w Brukseli odbyło się spotkanie GIODO z eurodeputowanymi (26 stycznia 2011 r.). Zorganizowano je we współpracy z europosem Jackiem Protasiewiczem, członkiem Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych PE, a jego tematem była kwestia reformy ochrony prywatności. Natomiast w uroczystościach w siedzibie Stałego Przedstawicielstwa Rzeczypospolitej Polskiej przy Unii Europejskiej (27 stycznia 2011 r.) zorganizowanych we współpracy z polskim ambasadorem przy Unii Europejskiej, Janem Tombińskim, uczestniczyli polscy posłowie do Parlamentu Europejskiego, europejscy rzecznicy ochrony danych osobowych z Peterem Hustinxem, Europejskim Rzecznikiem Ochrony Danych Osobowych na czele, przedstawiciele Komisji Europejskiej oraz innych polskich i unijnych instytucji mających siedzibę w Brukseli.

W 2011 r. główne obchody Dnia Ochrony Danych Osobowych w Polsce miały miejsce 31 stycznia. Tematem przewodnim Dnia była kwestia wypracowania nowego podejścia do ochrony prywatności, a także sposób wdrożenia tzw. dyrektywy retencyjnej. Tego dnia w Biurze GIODO zorganizowano Dzień Otwarty, na który złożyły się:

- panel dyskusyjny „Retencja danych w demokratycznym państwie prawnym” z udziałem Rzecznika Praw Obywatelskich, przedstawicieli Ministerstwa Infrastruktury, Urzędu Komunikacji Elektronicznej, Prokuratury Generalnej, Komedy Głównej Policji, a także reprezentantów organizacji pozarządowych działających na rzecz bezpieczeństwa i praw obywateli w sieci,
- wykłady ekspertów, w tym pracowników Biura GIODO, poświęcone bezpiecznemu korzystaniu z Internetu,
- bezpłatne porady i konsultacje ekspertów Biura GIODO.

Obchody Dnia Ochrony Danych Osobowych były też okazją do organizacji, wzorem lat ubiegłych, przez GIODO oraz redakcję „Dziennika Gazety Prawnej” panelu dyskusyjnego „Retencja danych”. Odbył się on 19 stycznia 2011 r. w siedzibie redakcji, zaś publikacja jego zapisu miała miejsce 31 stycznia 2011 r.

Z kolei 2 lutego 2011 r. odbył się zorganizowany w redakcji portalu Wirtualna Polska wideoczat z GIODO pt. „Ochrona danych osobowych w świetle nowoczesnych technologii”. Umożliwił on internautom bezpośredni kontakt z GIODO i szybkie uzyskanie odpowiedzi na najbardziej nurtujące ich problemy z zakresu prawa do prywatności i ochrony danych osobowych.

Częścią obchodów Dnia Ochrony Danych Osobowych było śniadanie naukowe „Stosowanie przez pracodawcę nowoczesnych technologii nadzoru nad zatrudnionymi” zorganizowane 17 lutego 2011 r. w Warszawie, w Akademii Leona Koźmińskiego.

Informacje o wszystkich tych wydarzeniach były również przekazywane do mediów. Akcja informacyjna dotycząca Dnia Ochrony Danych Osobowych zaowocowała publikacją licznych artykułów prasowych i internetowych związanych z jego tematem przewodnim.

6.2.2 Publikacje

W 2011 r. GODO kontynuował wydawanie broszur informacyjnych z serii „ABC ochrony danych osobowych”, których publikację rozpoczął w 2008 r.

W analizowanym 2011 r. ukazały się:

- Poradnik „Ochrona danych osobowych w trakcie prowadzenia kampanii wyborczej”, zawierający zestaw wytycznych dla komitetów wyborczych, partii politycznych, kandydatów, wyborców oraz stowarzyszeń i organizacji społecznych, jak zorganizować kampanię wyborczą z poszanowaniem przepisów o ochronie danych osobowych i prawa do prywatności;
- Poradnik ochrony danych osobowych w kościele prawosławnym, ogłoszony jako wspólna deklaracja Metropolity Sawy i GODO na wzór opracowanej we wrześniu 2009 r. przez ówczesnego Generalnego Inspektora Ochrony Danych Osobowych i Sekretarza Generalnego Konferencji Episkopatu Polski Instrukcji „Ochrona danych osobowych w działalności Kościoła Katolickiego w Polsce”.
- „Wybrane zagadnienia z zakresu ochrony danych. Przewodnik dla przedsiębiorców”, będący efektem współpracy międzynarodowej GODO z Biurem Ochrony Danych z Czech oraz z Rzecznikiem Ochrony Danych i Wolności Informacji z Węgier. Przewodnik dla przedsiębiorców przygotowany został w czterech językach – polskim, angielskim, czeskim i węgierskim. Publikacja ta powstała w ramach Projektu Partnerskiego Leonardo da Vinci „Podnoszenie świadomości w zakresie ochrony danych wśród przedsiębiorców działających na terytorium UE”.

Dodatkowo w związku z wejściem w życie 7 marca 2011 r. nowelizacji ustawy o ochronie danych osobowych GODO opracował i we współpracy z Wydawnictwem Sejmowym wydał broszurę „Wykaz zmian w ustawie o ochronie danych osobowych wprowadzonych nowelizacją z 29 października 2010 r.”, która jest erratą do serii „ABC ochrony danych osobowych”. Jednocześnie rozpoczęte zostały prace nad aktualizacją wszystkich broszur wydanych z tej serii.

6.2.3 Szkolenia

- **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.

W 2011 r. Generalny Inspektor Ochrony Danych Osobowych i jego przedstawiciele przeprowadzili szkolenia m.in.: nowo powołanych dyrektorów warszawskich placówek szkolnych i przedszkoli, a także doradców i konsultantów ośrodków doskonalenia zawodowego nauczycieli z Rybnika, Jasła, Częstochowy i Gliwic, którzy zgłosili swój udział w ogólnopolskim Programie edukacyjnym „*Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli*”. Konwencję szkolenia przybrała również wideokonferencja nt. prawa do prywatności i ochrony danych osobowych w Internecie, zorganizowana dla nauczycieli i uczniów Zespołu Szkół Sportowych im. Olimpijczyków Śląskich w Mysłowicach.

Wśród podmiotów szkolonych w 2011 r. znalazły się: Rada Organizacji Pozarządowych Województwa Łódzkiego oraz inne organizacje pozarządowe, jak np. Fundacja Dzieci Niczyich, a także Stowarzyszenie Notariuszy RP, kadra zarządzająca Urzędu Ochrony Konkurencji i Konsumentów, Narodowego Funduszu Zdrowia i Mazowieckiego Zarządu Dróg Wojewódzkich w Warszawie. Szkoleniem objęci też zostali przedstawiciele Rady Dyrektorów Biur Kancelarii Sejmików Województw RP, pracownicy Naczelnej Dyrekcji Archiwów Państwowych, Centrum Projektów Europejskich, Generalnej Dyrekcji Ochrony Środowiska, Wojewódzkiego Funduszu Ochrony Środowiska i Gospodarki Wodnej w Rzeszowie oraz Głównego Inspektoratu Pracy i Państwowej Inspekcji Pracy.

Ponadto w szkoleniach przeprowadzonych przez GIODO w 2011 r. udział wzięły urzędy administracji samorządowej, Urząd m.st. Warszawy, Urząd Miasta Wrocław, Sąd Okręgowy Warszawa Praga, Prokuratura Okręgowa w Płocku oraz przedstawiciele służb mundurowych, jak Straż Graniczna oraz Straż Miejska i Gminna zrzeszona w Krajowej Radzie Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej w Częstochowie. Na liście przeszkolonych przez Generalnego Inspektora Ochrony Danych Osobowych pracowników ministerstw znalazły się Ministerstwa: Spraw Zagranicznych (Centrum Rozwoju Zawodowego), Zdrowia, Pracy i Polityki Społecznej, Finansów (Departament Izby Celnej) oraz Spraw Wewnętrznych i Administracji (Centrum Projektów Informatycznych). W szkoleniach z zakresu ochrony danych osobowych brali też udział pracownicy Kancelarii Prezydenta RP.

W sumie w 2011 r. przeprowadzonych zostało **55** szkoleń z zakresu ochrony danych osobowych dla podmiotów zewnętrznych. Ich wykaz znajduje się w załączniku nr 6.

W tym miejscu należy podkreślić, że wykaz ten zawiera nie tylko szkolenia *sensu stricte*, ale także spotkania, seminaria, warsztaty i konferencje o charakterze dydaktycznym czy popularnonaukowym, propagującym idee ochrony danych osobowych. Przykładem może być udział przedstawiciela GIODO

w warsztatach dla służb prawnych statystyki publicznej zorganizowanych przez Główny Urząd Statystyczny, seminarium „Ochrona danych osobowych w agencjach zatrudnienia”, którego organizatorem był Związek Pracodawców – Ogólnopolski Konwent Agencji Pracy, czy spotkanie Zespołu Krajowego Mechanizmu Prewencji Biura Rzecznika Praw Obywatelskich z przedstawicielami „Porozumienia na rzecz wprowadzenia OPCAT”, podczas którego przeprowadzone zostało szkolenie poświęcone anonimizacji danych osobowych. Za propagowanie idei ochrony danych osobowych, które przybrało formę szkolenia, można również uznać wykład dla studentów Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego wygłoszony w 2011 r. przez przedstawiciela GODO.

- **Szkolenia wewnętrzne pracowników Biura GODO**

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 eduGODO”, status GODO 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.

- **Udział pracowników Biura GODO w szkoleniach organizowanych przez jednostki zewnętrzne**

Pracownicy Biura GODO korzystali ze szkoleń informatycznych, które miały na celu podnoszenie ich kompetencji w zakresie zarządzania i administrowania posiadaną infrastrukturą informatyczną, usprawnieniem sposobu dokumentowania przebiegu załatwiania spraw w związku z wdrażaniem nowej elektronicznej wersji instrukcji kancelaryjnej oraz systemów Elektronicznego Zarządzania Dokumentacją, a także uczestniczyli w prelekcji na temat postępowania z dokumentacją archiwalną, wygłoszonej przez przedstawiciela Departamentu Kształtowania Narodowego Zasobu Archiwalnego Naczelnej Dyrekcji Archiwów Państwowych.

Brali też udział w szkoleniach organizowanych przez Komendę Główną Policji w związku z udziałem Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, a także w systemie szkoleń z zakresu Oceny Skutków Regulacji organizowanych przez Ministerstwo Gospodarki w ramach projektu systemowego „Reforma procesu stanowienia prawa i uproszczenie obowiązujących przepisów”, współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Ponadto w związku z przygotowaniem polskiej administracji do Prezydencji w Radzie Unii Europejskiej, przedstawiciele Biura Generalnego Inspektora Ochrony Danych Osobowych brali udział

w szkoleniu z zakresu wiedzy ogólnej na temat europejskiego systemu prawnego, porządku instytucjonalnego oraz procesu decyzyjnego UE, przeprowadzonym przez przedstawiciela Departamentu Prawa Unii Europejskiej Ministerstwa Spraw Zagranicznych.

W analizowanym roku sprawozdawczym pracownicy Biura uczestniczyli również w szkoleniu pt. „Współpraca w zespole”, którego organizatorem było Warszawskie Centrum Innowacji Edukacyjnych i Szkoleń, samorządowa placówka doskonalenia nauczycieli. Zasadniczym celem tego szkolenia było doskonalenie kompetencji społecznych związanych z podniesieniem jakości współpracy w grupie poprzez trening umiejętności istotnych w pracy zespołowej.

6.2.4 Konkursy

W analizowanym 2011 r. Generalny Inspektor Ochrony Danych Osobowych był zarówno organizatorem, patronem, jak i laureatem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

- **Wzmocnienie umiejętności pracowników Biura GODO** to tytuł projektu realizowanego w Biurze Generalnego Inspektora Ochrony Danych Osobowych w latach 2009 - 2010, który został wyróżniony decyzją kapituły konkursu EDUinspiracje 2011.

Celem wyróżnionego projektu było umożliwienie pracownikom Biura GODO wymiany wiedzy i doświadczeń w zakresie stosowania prawa z zakresu ochrony danych osobowych z innymi organami zajmującymi się podobną problematyką w krajach partnerskich. Uczestnicy mieli szansę skonfrontowania swojej wiedzy oraz pozyskania nowych informacji i doświadczeń w wybranych obszarach ochrony danych osobowych, zgodnie z zakresem zadań wykonywanych przez poszczególnych pracowników urzędu na danych stanowiskach pracy. Projekt adresowany był do wybranej grupy pracowników merytorycznych, którzy zajmowali się zadaniami obejmującymi działalność edukacyjno-szkoleniową, kontrolę przetwarzania danych oraz rejestrację zbiorów danych osobowych.

Konkurs ogłoszony był przez Narodową Agencję programu „Uczenie się przez całe życie” i polegał na wyborze najlepszego projektu w zakresie mobilności. Projekt ten został wyróżniony w kategorii instytucjonalnej.

- **„Zastosowanie przepisów o ochronie danych osobowych w celu stworzenia portalu społecznościowego do wymiany informacji między kibicami piłki nożnej”** – to tytuł konkursu dla studentów wydziałów prawa zorganizowanego w 2011 r. przez Generalnego Inspektora Ochrony Danych Osobowych, przy wsparciu merytorycznym Kancelarii CMS Cameron Mc Kenna. Przedmiotem Konkursu było przygotowanie eseju, w którym uczestnicy mieli okazję wykazać się wiedzą na temat zastosowania przepisów prawa o ochronie danych osobowych do sytuacji opisanej w kazusie. Na konkurs nadesłanych zostało 14 prac. Oprócz nagród przyznanych autorom prac za

zajęcie trzech pierwszych miejsc, wszystkim wyróżnionym przyznane zostały nagrody specjalne w postaci miesięcznych praktyk zawodowych w Biurze GIODO. Uroczystość wręczenia nagród miała miejsce podczas międzynarodowego seminarium pt. „*Wiążące Reguły Korporacyjne – pojęcie, stosowanie, doświadczenia praktyczne*”, które odbyło się w dniu 14 czerwca 2011 r. w siedzibie Generalnego Inspektora Ochrony Danych Osobowych w Warszawie.

- W ramach obchodów V Dnia Ochrony Danych Osobowych 2011 r., GIODO objął patronatem **konkurs „Logotyp DODO”** zorganizowany przez Fundację Dzieci Niczyje.

Zadaniem konkursu było stworzenie logo (symbolu graficznego) Dnia Ochrony Danych Osobowych. Konkurs ogłoszony został przez serwis Sieciaki.pl i przeznaczony był tylko dla zarejestrowanych użytkowników tego serwisu. Rezultatem konkursu było 115 prac nadesłanych przez użytkowników portalu Sieciaki.pl. Oprócz zwycięzców trzech pierwszych miejsc, autorom sześciu nadesłanych prac przyznane zostały wyróżnienia.

6.2.5 Projekty i programy

W roku sprawozdawczym 2011, 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 projekty partnerskie. Drugim rodzajem był krajowy projekt edukacyjny, realizowany pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka.

I. Unijne projekty partnerskie

- a) W 2011 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 powstała publikacja **„Wybrane**

zagadnienia z zakresu ochrony danych. Przewodnik dla przedsiębiorców”. Omówione w niej zostały zagadnienia ochrony danych w kontekście prowadzenia działalności gospodarczej oraz dokonano przeglądu 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. W przewodniku tym poruszono też 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.

- b) W 2011 r. Biuro GODO kontynuowało realizację rozpoczętego w 2010 r. kolejnego projektu partnerskiego finansowanego ze środków Unii Europejskiej w ramach Programu Leonardo da Vinci **„Postrzeganie zagadnień związanych z ochroną danych i prywatnością przez dzieci i młodzież”** (Perception of the data protection and privacy issues by children and youth”). Projekt realizowany będzie w latach 2010-2012 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 analizowanym roku sprawozdawczym odbyły się dwa spotkania konsorcjum partnerskiego realizującego ww. projekt: 30-31 marca 2011 r. w siedzibie GODO w Warszawie i 11-12 października 2011 w Zadarze. Podczas spotkań omawiane były zagadnienia metodologiczne związane z prowadzeniem badań na dzieciach i młodzieży, w tym konstrukcji narzędzia badawczego. Efektem tych spotkań było wyznaczenie kierunku dalszego działania oraz przygotowane zostały podstawy do realizacji badania ankietowego. W rezultacie tego projektu powstanie raport podsumowujący badania wraz z oceną tego zjawiska w trzech krajach członkowskich Unii Europejskiej. Realizacja projektu umożliwi diagnozę poziomu świadomości dzieci i młodzieży na temat prawa do prywatności i ochrony danych osobowych, porównanie wyników badań między krajami biorącymi udział w projekcie, przygotowanie rekomendacji w oparciu o wyniki badań, upowszechnianie wyników badań na poziomie krajowym i międzynarodowym, wzmocnienie roli organów ochrony danych państw uczestniczących w projekcie w celu upowszechnienia informacji w grupach docelowych, zintensyfikowanie współpracy między organami ochrony danych w różnych krajach członkowskich UE. Wiedza pozyskana w toku realizacji projektu umożliwi lepsze ukierunkowanie działań informacyjnych w kraju i na świecie w kwestii sposobów ochrony danych osobowych i prywatności dzieci i młodzieży.

II. Krajowy program edukacyjny

W 2011 r. kontynuowany był również **ogólnopolski program edukacyjny „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli”**. Przedsięwzięcie to jest wynikiem zawartych przez GIODO z Gliwickim Ośrodkiem Metodycznym oraz Samorządowym Ośrodkiem Doradztwa Metodycznego i Doskonalenia Nauczycieli w Kielcach, porozumień o współpracy w obszarze działań edukacyjnych na rzecz podnoszenia poziomu świadomości w zakresie prawa do prywatności i ochrony danych osobowych. Podstawowym celem programu jest poszerzenie oferty edukacyjnej szkół o treści związane z ochroną danych osobowych i prawem każdego człowieka do prywatności poprzez zwiększenie wiedzy nauczycieli, pedagogów szkolnych i uczniów szkół gimnazjalnych o zagadnienia związane z tą tematyką. Podobnie jak w latach poprzednich program ten objęty został honorowym patronatem Minister Edukacji Narodowej i Rzecznika Praw Dziecka. W jego ramach nauczyciele mogą korzystać z bezpłatnych szkoleń, konsultacji, materiałów dydaktycznych oraz wymiany doświadczeń. W ramach programu przygotowane zostały pakiety edukacyjne dla 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.

Program ten spotkał się z dużym zainteresowaniem metodyków, nauczycieli oraz uczniów, co jest dowodem na istniejącą potrzebę realizacji tego typu inicjatyw edukacyjnych. Mając na uwadze pozytywne doświadczenia związane z realizacją programu w okresie, gdy był on skierowany wyłącznie do szkół gimnazjalnych na terenie kraju, podjęta została decyzja nie tylko o jego kontynuacji na rok szkolny 2011/2012, ale także o rozszerzeniu obszaru działań tego programu na szkoły podstawowe.

6.2.6 Konferencje, seminaria, spotkania

W roku sprawozdawczym 2011, Generalny Inspektor Ochrony Danych Osobowych organizował konferencje i seminaria, jak również brał aktywny udział w konferencjach zorganizowanych przez inne podmioty. Patronował i aktywnie uczestniczył w wielu wydarzeniach organizowanych cyklicznie, jak chociażby Dzień Bezpiecznego Internetu, organizowany od 2005 r. przez Fundację Dzieci Niczyje oraz Naukową i Akademicką Sieć Komputerową (NASK) – realizatorów unijnego programu „Safer Internet”, czy obchody Światowego Dnia Społeczeństwa Informacyjnego, który w 2011 r. przebiegał pod hasłem „Przeciwdziałanie wykluczeniu cyfrowemu na terenach mało zurbanizowanych”. Wykaz patronatów Generalnego Inspektora Ochrony Danych Osobowych udzielonych różnym wydarzeniom zorganizowanym w 2011 r. znaleźć można w załączniku nr 7.

Poniżej przedstawiony zostały najważniejsze wydarzenia krajowe o charakterze ogólnopolskim lub międzynarodowym z udziałem Generalnego Inspektora bądź przedstawicieli jego Biura. Ich pełny wykaz zawiera załącznik nr 8.

1. V Dzień Ochrony Danych Osobowych – 28 stycznia 2011 r.

W dniu 28 stycznia 2011 r. Generalny Inspektor Ochrony Danych Osobowych już po raz piąty 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. Wydarzenia związane z Dniem odbywały się zarówno w Brukseli, jak i we wszystkich stolicach państw członkowskich Unii Europejskiej. Tegoroczne obchody połączone były z 30-tą rocznicą przyjęcia Konwencji 108.

Z tej okazji 31 stycznia 2011 r. zorganizowany został w Biurze GIODO Dzień Otwarty, w ramach którego uczestnicy mieli okazję uzyskać informacje na temat ochrony danych osobowych oraz porady prawne i konsultacje. W ramach obchodów Dnia zorganizowany został panel dyskusyjny „Retencja danych w demokratycznym państwie prawnym” oraz cykl zajęć pod hasłem „Bezpieczeństwo dzieci i młodzieży w Internecie” wraz z konkursem wiedzy dla dzieci i młodzieży.

W kalendarz wydarzeń związanych z organizacją tego święta w Polsce wpisać należy seminarium dotyczące ochrony danych osobowych dla organizacji pozarządowych, które odbyło się w Łodzi 20 stycznia 2011 r. oraz Śniadanie naukowe „Stosowanie przez pracodawcę nowoczesnych technologii nadzoru nad zatrudnionymi”, które miało miejsce w Akademii Leona Koźmińskiego w Warszawie w dniu 17 lutego 2011 r. zaś 2 lutego 2011 r. – czat z GIODO na wp.pl, którego tematem była „Ochrona danych osobowych w świetle nowoczesnych technologii”.

Z kolei 12 lutego 2011 r. Andrzej Lewiński, zastępca GIODO, uczestniczył w inauguracji studiów podyplomowych z zakresu IT w Wyższej Szkole Biznesu w Dąbrowie Górniczej, podczas których wygłosił wykład pt. „Prawo do prywatności w świetle rozwoju cywilizacyjnego społeczeństw”. Charakter uroczystości, zakres tematyczny studiów podyplomowych oraz specyfika projektu, który jest dofinansowany z Europejskiego Funduszu Społecznego, doskonale wpisywał się w obchody V Europejskiego Dnia Ochrony Danych Osobowych.

Ponadto w okresie styczeń-luty 2011 r., podczas zajęć świetlicowych na półkoloniach w czasie ferii zimowych dla uczniów gliwickich szkół podstawowych, odbywały się zajęcia oraz konkursy pod hasłem „Bezpieczeństwo w sieci”.

Jak już o tym była mowa, wydarzenia, jakie towarzyszą obchodom Europejskiego Dnia Ochrony Danych Osobowych tradycyjnie od pięciu lat odbywają się również w Brukseli. Z tej okazji 24 stycznia 2011 r. Generalny Inspektor Ochrony Danych Osobowych uczestniczył w warsztatach pt. „Zgłoszenia

naruszeń ochrony danych w Europie – perspektywa na przyszłość” zorganizowanych przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), 26 stycznia 2011 r. - spotkał się z polskimi europosłami w siedzibie Parlamentu Europejskiego w Brukseli, zaś następnego dnia, do grona uczestników spotkania z Generalnym Inspektorem w siedzibie Stałego Przedstawicielstwa RP przy UE dołączyli także przedstawiciele Komisji Europejskiej oraz innych polskich i unijnych instytucji.

Natomiast 28 stycznia 2011 r. odbyła się w Brukseli konferencja pt. „Ochrona danych (30 lat później): od europejskich do międzynarodowych standardów”, zorganizowana przez Komisję Europejską i Radę Europy. Wojciech Rafał Wiewiórowski (GIODO) był moderatorem jednego z 2 paneli konferencji, zatytułowanego „Od europejskich do międzynarodowych standardów ochrony danych”, w którym udział wzięli m.in. Pani Jennifer Stoddart - Komisarz ds. prywatności w Kanadzie oraz przedstawiciele organów ochrony danych osobowych w USA i Meksyku.

2. Ogólnopolskie Forum Dyrektorów Urzędów Pracy (Warszawa, 3 lutego 2011 r.)

Podczas spotkania, zastępca Generalnego Inspektora Ochrony Danych Osobowych wystąpił z prelekcją z zakresu ochrony danych osobowych pt. „Dyrektor Urzędu Pracy jako Administrator Danych Osobowych”.

3. Ogólnopolskie Forum Operatorów Kablowych FORTEL 2011 (Wisła, 8 marca 2011 r.)

Celem Ogólnopolskiego Forum Operatorów Kablowych FORTEL 2011, zorganizowanego przez Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM oraz Fundację Wspierania Nowych Technologii Telekomunikacyjnych PROTELKO, było przybliżenie uczestnikom spotkania obowiązków wynikających z ustawy o ochronie danych osobowych. Referat na ten temat wygłosił zastępca Generalnego Inspektora Ochrony Danych Osobowych.

4. Konwersatorium nt. ochrony informacji w urzędach administracji samorządowej (Rynia, 09 marca 2011 r.)

Konwersatorium, którego organizatorem było Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, nawiązywało do uchwalonej nowelizacji ustawy o ochronie informacji niejawnych i ustawy o ochronie danych osobowych i miało na celu zapoznanie nowo wybranych samorządowców z zasadami bezpieczeństwa informacji, ochrony danych osobowych, prawa do prywatności i zapobiegania przestępczości zorganizowanej. Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Ochrona danych osobowych w administracji samorządowej a dostęp do referencyjnych danych rejestrowych”.

5. Ogólnopolska Konferencja Dyrektorów Szkół Katolickich (Częstochowa, 16 marca 2011 r.)

GIODO spotkał się z dyrektorami katolickich placówek szkolnych, by przypomnieć im podstawowe zasady pozyskiwania i wykorzystywania danych osobowych, a także omówić najważniejsze problemy wiążące się z przetwarzaniem tych danych w systemach informatycznych szkół. Podczas Konferencji

zorganizowanej przez Radę Szkół Katolickich GIODO wygłosił referat pt. „Zasady ochrony prywatności w praktyce działania szkół katolickich”.

6. Spotkanie GIODO z przedstawicielami Amerykańskiej Izby Handlowej (Warszawa, 17 marca 2011 r.)

Spotkanie dra Wojciecha R. Wiewiórowskiego, GIODO, z przedstawicielami Amerykańskiej Izby Handlowej poświęcone było reformie europejskich przepisów o ochronie prywatności w kontekście nadchodzącej Prezydencji RP w Radzie UE. Na zaproszenie Amerykańskiej Izby Handlowej, GIODO omówił aktualne problemy związane ze stosowaniem obowiązujących przepisów o ochronie danych osobowych, w tym kwestie rejestracji zbiorów danych i potrzebę ujednolicenia pojęcia danych wrażliwych. Dyskutowano nad nowymi rozwiązaniami w dziedzinie ochrony prywatności i możliwości ich zastosowania, takie jak „privacy by design” (uwzględnienie ochrony prywatności w fazie projektowania), czy też prawo do bycia zapomnianym. Przedstawiając swoje działania na forum europejskim, Generalny Inspektor wskazał również na potrzebę promocji nowych rozwiązań, jak np. Wiążące Reguły Korporacyjne.

7. Konferencja „Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym” (Warszawa, 21 marca 2011 r.)

Organizatorami tej ogólnopolskiej konferencji był Wydział Prawa i Administracji Uniwersytetu Warszawskiego. Tematyka Konferencji skupiała się na zagadnieniach związanych z ochroną danych osobowych i prawem do prywatności w ramach prowadzonej działalności gospodarczej przez różne podmioty, zarówno w kraju, jak i za granicą. Omówione zostały kierunki zmian w ustawodawstwie dotyczącym ochrony danych osobowych, w szczególności w kontekście odwoływalności zgody na przetwarzanie danych osobowych i jej znaczenia dla praktyki gospodarczej. Podczas Konferencji Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład pt. „Profilowanie osób na podstawie ogólnodostępnych danych”.

8. Konferencja naukowa pt. „Zabezpieczenie danych osobowych – aktualny stan prawny a rzeczywiste potrzeby” (Warszawa, 28 marca 2011 r.)

Konferencja, zorganizowana przez Stowarzyszenie Administratorów Bezpieczeństwa Informacji oraz Wydział Zarządzania Politechniki Warszawskiej, była elementem ogólnopolskiej debaty na temat projektowanych zmian w przepisach o ochronie danych osobowych. Jej podstawowym celem była ocena aktualnego stanu i potrzeb w zakresie prawnych wymogów zabezpieczenia organizacyjnego i technicznego danych osobowych. Dlatego głównym przedmiotem zainteresowania były przepisy rozdziału 5 ustawy o ochronie danych osobowych wraz z przepisami wykonawczymi. Omówione zostały konieczne zmiany w ww. przepisach prawa, a także w unijnej Dyrektywie 95/46/WE stanowiącej pierwowzór polskich przepisów. Odrębny blok poświęcono funkcjonowaniu administratora bezpieczeństwa informacji. Dr Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych

Osobowych, objął konferencję patronatem oraz wygłosił wykład inauguracyjny pt. Prawna regulacja zasad zabezpieczania systemów teleinformatycznych, zaś Andrzej Kaczmarek, Dyrektor Departamentu Informatyki Biura GODO, w swoim wystąpieniu mówił o koniecznych zmianach w przepisach rozporządzenia do ustawy o ochronie danych osobowych.

9. Seminarium „Bezpieczeństwo i ochrona danych w modelu cloud computing” (Warszawa, 30 marca 2011 r.)

Centrum Promocji Informatyki było organizatorem seminarium poświęconemu zagadnieniom związanym z usługą przetwarzania danych w chmurze, w tym w szczególności zagrożeniom dla prywatności i kwestii odpowiedzialności za dane. Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład inauguracyjny pt. „Prawne aspekty przetwarzania danych w chmurze obliczeniowej – rekomendacje i regulacje Unii Europejskiej”.

10. Śniadanie naukowe „Zmiany do ustawy o ochronie danych osobowych w dobie rozwoju nowoczesnych technologii” (Warszawa, 07 kwietnia 2011 r.)

Spotkanie, które przybrało konwencję Śniadania naukowego, zgromadziło przedstawicieli instytucji finansowych, którym GODO przedstawił zakres najnowszych i planowanych zmian w ustawie o ochronie danych osobowych. Wskazywał, że zmiany, których należy dokonać, muszą być znacznie szersze niż dostosowanie się do nowych technologii. Zmiany wymagają także zapisy dotyczące m.in. zakresu danych wrażliwych czy rejestracji zbiorów danych osobowych. Dyskutowano też o innych kwestiach istotnych z punktu widzenia działalności sektora finansowego, takich jak wykorzystywanie danych biometrycznych czy ochrona genomu.

11. Konferencja naukowa „Ochrona danych osobowych w prawie pracy i w prawie ubezpieczeń społecznych – stan obecny i perspektywy zmian” (Warszawa, 14 kwietnia 2011 r.)

Wymianie poglądów na temat kierunków zmian w prawie pracy i w prawie ubezpieczeń społecznych w obszarze prawa do prywatności i ochrony danych osobowych pomiędzy środowiskiem naukowym i biznesowym, poświęcona została konferencja naukowa „Ochrona danych osobowych w prawie pracy i w prawie ubezpieczeń społecznych - stan obecny i perspektywy zmian” zorganizowana przez Kolegium Prawa Akademii Leona Koźmińskiego w Warszawie oraz Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego pod honorowym patronatem Generalnego Inspektora Ochrony Danych Osobowych. Podczas Konferencji dr Wojciech R. Wiewiórowski, GODO, wygłosił wykład pt. „Prawna ochrona danych biometrycznych w systemach teleinformatycznych pracodawcy. Cele przetwarzania a zakres ochrony”.

12. Spotkanie z przedstawicielami Amerykańskiej Izby Handlowej nt. harmonizacji przepisów dotyczących ochrony danych osobowych (Warszawa, 11 maja 2011 r.)

Przedmiotem dyskusji była problematyka różnic prawnych w zakresie ochrony danych osobowych w krajach Unii Europejskiej i Stanach Zjednoczonych oraz wynikające z nich ograniczenia dla firm

amerykańskich przesyłających dane osobowe z Polski do USA. Podkreślając różnice w filozofii ochrony danych osobowych pomiędzy tymi dwoma systemami prawnymi, GIODO wyraził pogląd, że istnieje szansa na zharmonizowanie tych systemów w przyszłości dzięki staraniom wielu amerykańskich senatorów zabiegających o wprowadzenie prawa o ochronie danych osobowych na poziomie rządu federalnego USA.

13. Konferencja pt. „Nie daj się złapać w sieć!” (Lublin, 16 maja 2011 r.)

Organizatorem konferencji, która pod patronatem GIODO odbyła się na Wydziale Prawa i Administracji Uniwersytetu Marii Curie-Skłodowskiej w Lublinie, było Europejskie Stowarzyszenie Studentów Prawa ELSA Lublin. Tematem przewodnim tego wydarzenia była kwestia zapewnienia bezpieczeństwa osób korzystających z Internetu poprzez omówienie regulacji prawnych normujących zachowania w sieci. Z ramienia GIODO referat pt. „Bezpieczeństwo przetwarzania danych osobowych w Internecie” wygłosiła Monika Krasieńska, Dyrektor DOLiS Biura GIODO.

14. Śniadanie prasowe (Warszawa, 17 maja 2011 r.)

Omówieniu kwestii związanych z szybkim rozwojem nowoczesnych technologii, który rodzi nowe wyzwania dla ochrony danych osobowych poświęcone było Śniadanie prasowe zorganizowane 17 maja 2011 r. podczas Światowego Dnia Społeczeństwa Informacyjnego, przez Krajowe Stowarzyszenie Ochrony Informacji Niejawnych i Grupę BOSSG. Podczas spotkania Andrzej Lewiński, Zastępca Generalnego Inspektora Ochrony Danych Osobowych zwrócił uwagę m.in. na postępującą globalizację prowadzącą do wielu istotnych zmian w funkcjonowaniu społeczeństw. Dla GIODO oznacza to nowe wyzwania związane z ochroną prywatności i danych osobowych. Andrzej Lewiński mówił o nich w kontekście koniecznych zmian prawa, które planowane są zarówno w Unii Europejskiej, jak i w Polsce. Jako przykład zagadnienia, które wymaga uregulowania w przepisach, podał radiową transmisję danych (RFID). Tematem technologii RFID zajmują się zarówno GIODO, jak i polski rząd, który został zobowiązany, by do końca maja 2011 r., przedłożyć KE informacje o wdrażaniu tej technologii pod kątem bezpieczeństwa ochrony danych i prywatności.

15. Międzynarodowa konferencja szkoleniowa „Miasto monitorowane – personel, aspekty prawne i technika systemów CCTV” (Częstochowa, 19 maja 2011 r.)

Techniczne możliwości przetwarzania danych wizyjnych i tworzenia zbiorów danych w cyfrowych systemach CCTV, wzrost technicznych możliwości zautomatyzowanego łączenia danych wizyjnych z danymi pozyskanymi z innych źródeł, a także propozycje rozwiązań w zakresie wzrastających możliwości tych systemów w kontekście europejskich standardów wykorzystywania miejskich systemów monitoringu wizyjnego – to główne tematy wystąpienia dra Wojciecha Wiewiórowskiego, GIOGO, podczas konferencji w Częstochowie. Organizatorami tego wydarzenia byli: Prezydent Miasta Częstochowy, Związek Miast Polskich i Krajowa Rada Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej.

16. Konferencja naukowa pt. „Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli” (Warszawa, 21 maja 2011 r.)

Naczelna Rada Adwokacka była organizatorem konferencji z udziałem Generalnego Inspektora Ochrony Danych Osobowych, poświęconej zagadnieniom retencji danych osobowych zbieranych przez służby specjalne, implementacji dyrektywy retencyjnej do polskiego porządku prawnego, a także trudnościom kontroli konstytucyjnej przepisów regulujących retencję danych telekomunikacyjnych. Dr Wojciech R. Wiewiórowski, GODO, wygłosił wykład pt. „Granice ingerencji w swobodę komunikacji w 10 lat po World Trade Center”.

17. Konferencja „Ochrona danych osobowych na rynku finansowym (Warszawa, 25 maja 2011 r.)

Mechanizmy ochrony danych osobowych w bankach wraz z analizą obowiązujących regulacji prawnych, obowiązki prawne firm inwestycyjnych w zakresie ochrony danych osobowych klientów, a także zasady anonimowości obrotu na giełdowym rynku regulowanym (jako element ochrony prywatności finansowej), to tylko kilka przykładów tematów poruszonych na konferencji zorganizowanej przez Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Wykład Generalnego Inspektora Ochrony Danych Osobowych poświęcony wyzwaniom związanym z przekazywaniem danych osobowych instytucjom finansowym, wskazał na nowe obszary identyfikowania tego jakże ważnego i zarazem do tej pory mało rozpoznanego zagadnienia, jakim jest ochrona danych osobowych na rynku finansowym.

18. VII Kongres ochrony informacji niejawnych, biznesowych i danych osobowych (Spała, 25-27 maja 2011 r.)

Omówieniu nowych przepisów dotyczących ochrony informacji niejawnych oraz ochrony danych osobowych, a także kwestii tajemnic prawnie chronionych poświęcony był VII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych, któremu patronował Generalny Inspektor Ochrony Danych Osobowych. Uczestnicy spotkania dzielili się swoimi doświadczeniami w zakresie organizacji i funkcjonowania pionów ochrony, stosowania kompleksowych rozwiązań systemowych bezpieczeństwa informacji, zmian unormowań dotyczących postępowań sprawdzających, bezpieczeństwa fizycznego, teleinformatycznego i przemysłowego oraz prowadzenia cyklicznych szkoleń. Omawiano je m.in. w kontekście bezpieczeństwa państwa. Osobną sesję poświęcono aktualnym problemom ochrony prywatności i danych osobowych. Tematykę tę zaprezentował goszczący na Kongresie Andrzej Lewiński, zastępca Generalnego Inspektora Ochrony Danych Osobowych. Tradycyjnie podczas Kongresu ogłoszono wyniki Konkursu „**Lider ochrony informacji niejawnych, biznesowych i danych osobowych**”. Nagrodą Grand Prix oraz szablą w dowód uznania szczególnych zasług na rzecz ochrony informacji niejawnych uhonorowany został Andrzej Lewiński, zastępca GODO. Organizatorami VII Kongresu było Krajowe Stowarzyszenie Ochrony Informacji

Niejawnych (KSOIN) oraz Podyplomowe Studium Ochrony Informacji Niejawnych na Uniwersytecie Śląskim.

19. Konferencja naukowa nt. „Twoje dane – twoja sprawa. Ochrona danych osobowych w szkołach” (Warszawa, 02 czerwca 2011 r.)

Podstawowym zadaniem Konferencji, której organizatorem był Generalny Inspektor Ochrony Danych Osobowych, było podsumowanie trwającego ponad dwa lata ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli”. W programie konferencji omówione były m.in. zmiany ustawodawcze w systemie oświaty, działania informacyjno-edukacyjne GODO – w szczególności w kontekście uczestnictwa dzieci i młodzieży w portalach społecznościowych – dzielenie się dobrymi praktykami przez przedstawicieli ośrodków doskonalenia nauczycieli w zakresie programów nauczania o ochronie danych osobowych, którzy uczestniczyli w programie „Twoje dane – twoja sprawa”, a także prezentacja działań Gliwickiego Ośrodka Metodycznego oraz Fundacji Dzieci Niczyje. Konferencja stanowiła niezwykle ważne forum wymiany poglądów i doświadczeń, stając się ważnym głosem w dyskusji na temat prywatności i ochrony danych osobowych najmłodszych członków społeczeństwa.

20. Konferencja naukowa „Bezpieczeństwo w Internecie” (Warszawa, 08-09 czerwca 2011 r.)

O tym, jak w dobie powszechnego wykorzystywania nowoczesnych rozwiązań technologicznych zapewnić naszym danym osobowym należyta ochronę, debatowali uczestnicy konferencji naukowej „Bezpieczeństwo w Internecie” odbywającej się na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Konferencję zorganizowali Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Naukowa i Akademicka Sieć Komputerowa oraz Naukowe Centrum Prawno-Informatyczne. Patronat honorowy nad nią sprawowali zaś Rzecznik Praw Obywatelskich, Generalny Inspektor Ochrony Danych Osobowych, Szef Agencji Bezpieczeństwa Wewnętrznego, Prezes Urzędu Komunikacji Elektronicznej.

21. X FORUM ADO/ABI „Aktualne problemy bezpieczeństwa technicznego i organizacyjnego danych osobowych” (Warszawa, 09 czerwca 2011 r.)

Temat jubileuszowego X Forum ADO/ABI dotyczył techniczno-organizacyjnych aspektów zabezpieczenia danych osobowych, wśród których omówione zostały m.in. normy ISO w ochronie danych osobowych, archiwizacja danych i tworzenia kopii zapasowych, wykonywania zadań ABI oraz procedura upoważniania do przetwarzania danych osobowych. Wykład wprowadzający pt. „Podstawowe zagrożenia i wyzwania technologiczne dla ochrony danych osobowych” wygłosił dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych.

22. V Międzynarodowa Konferencja „Bezpieczeństwo dzieci i młodzieży w Internecie” (Warszawa, 20-21 września 2011 r.)

Organizatorami Konferencji są Polskie Centrum Programu Safer Internet (PCPSI), które tworzą Naukowa i Akademicka Sieć Komputerowa (NASK) i Fundacja Dzieci Niczyje (FDN) oraz partnerski projekt na rzecz bezpieczeństwa w Internecie – klicksafe. Wydarzenie to organizowane było w ramach programu Komisji Europejskiej „Safer Internet”. Konferencja została objęta patronatem polskiej Prezydencji w Radzie UE. Konferencja poświęcona była szerokiemu spektrum zagadnień związanych z bezpieczeństwem dzieci i młodzieży w Internecie. Jej adresatami byli przedstawiciele sektora edukacyjnego, organizacji pozarządowych, wymiaru sprawiedliwości i organów ścigania oraz dostawców usług i treści internetowych. Celem Konferencji było przekazanie najnowszej wiedzy zarówno w zakresie działań edukacyjnych, jak również zwalczania nielegalnych treści w sieci.

23. Spotkanie ze Stowarzyszeniem Marketingu Bezpośredniego nt. ochrony danych osobowych
(Warszawa, 23 listopada 2011 r.)

W ramach Porozumienia zawartego w 2008 r. o wspólnym działaniu na rzecz poprawy poziomu ochrony danych osobowych i prawa do prywatności w działalności marketingowej oraz stosowaniu Kodeksu Dobrych Praktyk, dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, spotkał się z reprezentatami Stowarzyszenia Marketingu Bezpośredniego (SMB). W trakcie spotkania GODO przedstawił sytuację dotyczącą ochrony danych w Polsce i Europie, komentarz do obecnej ustawy oraz kierunki zmian/nowelizacji, jakie planuje GODO i Komisja Europejska. Dyskusja skupiła się również na ochronie danych w kontekście realiów biznesowych w dzisiejszej Polsce w świetle rozwoju nowoczesnych technologii.

24. Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z przedstawicielami instytucji sektora finansowego nt. profilowania klientów (Warszawa, 24 listopada 2011 r.)

Dr Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, wyjaśniał, dlaczego tworzenie profili klientów, czyli pozyskiwanie informacji o nich z różnych źródeł i ich łączenie, coraz częściej wykorzystywane przez sektor finansowy czy ubezpieczeniowy, wymaga wiedzy i zgody osób, których dane są w ten sposób przetwarzane. Przypomniwał, że jeśli dane, które zostały zebrane w określonym celu, np. na potrzeby zawarcia i realizacji umowy, firmy zestawiają z innymi danymi i na tej podstawie tworzą profil osobowy klienta, to tym samym zmieniają cel przetwarzania. GODO podkreślał, że każdy, kto dokonuje profilowania, ma obowiązek poinformowania o tym osoby profilowanej.

25. Konferencja „E-zdrowie – bezpieczeństwo i jakość informacji medycznej oraz szerokie zastosowanie technologii telemedycznych dla UE w ramach Europy Cyfrowej” (Warszawa, 28-29 listopada 2011 r.)

Konferencję zorganizowało Centrum Systemów Informacyjnych Ochrony Zdrowia w ramach Polskiej Prezydencji w Radzie Unii Europejskiej. Temat konferencji odnosił się do jednego z jej priorytetów, tj. wspierania i rozwoju dostępu do danych i usług medycznych on-line. Podstawowymi zagadnieniami

poruszonymi na tym spotkaniu było bezpieczeństwo i jakość informacji medycznej oraz szerokie zastosowanie technologii telemedycznych dla obywateli UE w ramach Europy Cyfrowej. Podczas Konferencji wykład na temat „E-zdrowie a ochrona danych osobowych w kontekście europejskim” wygłosił Piotr Drobek, zastępca Dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej Biura GODO.

26. Konferencja naukowo-branżowa „Bezpieczny hotel – oczekiwania i wyzwania wobec EURO 2012 (Warszawa, 30 listopada 2011 r.)

Celem Konferencji było przekazanie uczestnikom niezbędnej wiedzy na temat rozwiązań organizacyjnych i technicznych, jakie należy zastosować w obiekcie hotelarskim, by osiągnąć pożądany poziom bezpieczeństwa gości przy jednoczesnym poszanowaniu prawa do prywatności i ochrony danych osobowych. Organizatorami Konferencji byli: Komenda Główna Policji, Biuro Ochrony Rządu, Izba Gospodarcza Hotelarstwa Polskiego, Instytut Wiedzy i Umiejętności w Warszawie oraz Wyższa Szkoła Hotelarstwa, Gastronomii i Turystyki w Warszawie. Z ramienia Generalnego Inspektora Ochrony Danych Osobowych wykład nt. ochrony danych osobowych w praktyce hotelarskiej – podstawowe standardy bezpieczeństwa, wygłosiła Monika Krasieńska, Dyrektor DOLiS Biura GODO.

27. Konferencja Naukowa „Medycyna personalizowana. Genom – etyka – prawo” (Lublin, 02 grudnia 2011 r.)

Konferencja, której organizatorem był Uniwersytet Medyczny w Lublinie, stanowiła arenę interdyscyplinarnej dyskusji nad problemami etycznymi, filozoficznymi, społecznymi i prawnymi związanymi z dynamicznym rozwojem współczesnej genetyki i ideą personalizacji medycyny. W szczególności zaś poruszała ważne kwestie związane z prawami pacjenta w związku z badaniami genetycznymi, równością dostępu do świadczeń z zakresu genetyki, ryzykiem dyskryminacji ze względu na dziedzictwo genetyczne czy patentowania i komercjalizacji wyników badań w dziedzinie genetyki. Podczas Konferencji Monika Krasieńska, Dyrektor Departamentu Orzecznictwa, Legislacji i Skarg Biura GODO, wygłosiła referat pt. „Ochrona danych osobowych a informacja genetyczna”.

28. VIII Konferencja „Wyzwania w zakresie badań nad bezpieczeństwem wewnętrznym – nowa perspektywa finansowa UE 2013 – 2020” (Będlewo k/Poznań, 6-7 grudnia 2011 r.)

Tematem VIII Konferencji zorganizowanej przez Polską Platformę Bezpieczeństwa Wewnętrznego były kwestie związane z wykorzystywaniem nowoczesnych technologii przez służby odpowiedzialne za bezpieczeństwo państwa i jego obywateli. Przedstawione zostały nowe narzędzia informatyczne będące na etapie wdrażania w wymienionych służbach oraz omówiono kierunki przyszłych badań nad bezpieczeństwem wewnętrznym w perspektywie lat 2013 – 2020. Stanowisko GODO w sprawie poszanowania prawa do prywatności i ochrony danych osobowych w działalności służb

odpowiedzialnych za bezpieczeństwo wewnętrzne, zaprezentowała Monika Kasińska, Dyrektor Departamentu Orzecznictwa, Legislacji i Skarg Biura GODO.

29. Konferencja naukowa „Bezpieczeństwo technologii biometrycznych – ochrona danych biometrycznych (Warszawa, 09 grudnia 2011 r.)

Biometria a prawa człowieka, ochrona danych biometrycznych i procesów ich przetwarzania, wykorzystanie i zabezpieczenie identyfikacji biometrycznej w administracji publicznej, bankowości, spółkach IT oraz w innych podmiotach sektora prywatnego oraz biometria w stosunkach pracy to bloki tematyczne konferencji, która odbyła się 9 grudnia 2011 r. na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Generalny Inspektor Ochrony Danych Osobowych, wspólnie z Rzecznikiem Praw Obywatelskich oraz Szefem Agencji Bezpieczeństwa Wewnętrznego objął nad konferencją patronat honorowy. Podczas konferencji dr Wojciech R. Wiewiórowski, GODO, wygłosił wykład pt. „Prawna regulacja ochrony danych biometrycznych a swoboda badań naukowych”.

6.2.7 Internet

W roku 2011 przeprowadzonych zostało szereg modyfikacji i poprawek systemu e-GODO zarówno pod względem funkcjonalnym jak i poprawności jego działania, uporządkowano usługi przekazywania pism i wniosków udostępnionych na ePUAP⁴⁵², a także wykonano szereg prac w ramach modyfikacji serwisu informacyjnego Biura GODO, systemu Rejestru Zbiorów Danych Osobowych i udoskonalenia funkcjonalności elektronicznego obiegu dokumentów eSOD:VENTUS.

W grudniu 2011 r. zakończono prace instalacyjne i wdrożeniowe systemu Doręczyciel GODO zapewniającego funkcjonalności wymagane dla zapewnienia zobowiązań Biura GODO w zakresie elektronicznej formy doręczania pism urzędowych dla podmiotów nie będących podmiotami administracji publicznej wynikających ze zmian w K.p.a. wprowadzonymi ustawą z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. z 2010 r. Nr 40, poz. 230). Wykonano również niezbędne testy systemu i przygotowano system do rozpoczęcia pracy, która nastąpi na początku 2012 r.

Ponadto w 2011 r. utworzony został serwis „Newsletter” dystrybuujący w formie korespondencji e-maile do zainteresowanych osób. „Newsletter” zawiera informacje o nowych wydarzeniach w zakresie ochrony danych osobowych i pracy Biura GODO przygotowane przez Zespół Prasowy Biura Generalnego Inspektora Ochrony Danych Osobowych.

6.2.8 Porozumienia o współpracy

⁴⁵² Wykonanie korekty było niezbędne ze względu na zmianę interfejsu systemu ePUAP oraz zmianach w kartach opisu usług dotyczących komunikacji z GODO wprowadzonych przez MSWiA w pierwszym kwartale 2011 r.

a) Porozumienie o współpracy GIODO z Warszawskim Centrum Innowacji Edukacyjno-Społecznych i Szkoleń, 10.03.2011 r.

W dniu 10 marca 2011 r. Dyrektor Biura Generalnego Inspektora Ochrony Danych Osobowych i Dyrektor Warszawskiego Centrum Innowacji Edukacyjno-Społecznych i Szkoleń podpisali porozumienie na rzecz podwyższania poziomu wiedzy zawodowej i profesjonalnych umiejętności praktycznych. Współpraca obejmować będzie organizację wzajemnych szkoleń oraz innego typu działań edukacyjno-informacyjnych.

b) Porozumienie o współpracy GIODO z Wyższą Szkołą Biznesu w Dąbrowie Górniczej, 05.10.2011 r.

W dniu 5 października 2011 r. w Dąbrowie Górniczej Z-ca Generalnego Inspektora Ochrony Danych Osobowych Pan Andrzej Lewiński podpisał porozumienie o współpracy z JM Rektorem WSB prof. Zdzisławą Dacko-Pikiewicz. To już kolejne porozumienie, jakie zawiera GIODO ze szkołą wyższą w celu uruchomienia studiów podyplomowych. Studia *„Ochrona danych osobowych i informacji prawnie chronionych w administracji i biznesie”* rozpoczęły się Wyższej Szkole Biznesu w Dąbrowie Górniczej już w październiku 2011 roku. Porozumienie przewiduje również współpracę naukowo-badawczą, edukacyjną, wydawniczą oraz realizację wspólnych projektów.

c) Porozumienie w sprawie współpracy GIODO z Akademią Obrony Narodowej, 21.10.2011 r.

W dniu 21 października 2011 r. w Warszawie, w Sali Tradycji Klubu Akademii Obrony Narodowej (AON), dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, podpisał z gen. dyw. dr inż. Romualdem Ratajczakiem, Rektorem – Komendantem AON, porozumienie w sprawie współpracy. Podczas uroczystości obecni byli także Pan Andrzej Lewiński, Z-ca GIODO oraz Prorektor ds. Naukowych dr hab. Andrzej Glen. Przedmiotem porozumienia jest określenie obszarów, zasad i warunków współpracy pomiędzy tymi instytucjami, która przebiegać będzie zarówno w obszarze edukacji, jak i działalności naukowo-dydaktycznej, promocyjnej, wydawniczej i organizacyjnej

d) Porozumienie o współpracy GIODO z Uniwersytetem Łódzkim, 08.12.2011 r.

Porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych podpisane zostało przez Generalnego Inspektora Ochrony Danych Osobowych z prof. zw. dr hab. Włodzimierzem Nykielem w dniu 08 grudnia 2012 r. W tym dniu na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego w Łodzi odbyło się uroczyste spotkanie z władzami uczelni i studentami, podczas którego Andrzej Lewiński, Zastępca GIODO, wygłosił wykład „Ochrona danych osobowych w związku z wykorzystaniem nowych technologii w stosunkach pracy”. Obszar współpracy Generalnego

Inspektora Ochrony Danych Osobowych z Uniwersytetem Łódzkim obejmować będzie działalność naukowo-nadawczą, edukacyjną, wydawniczą promocyjną i organizacyjną.

e) Porozumienie w sprawie zasad współpracy GODO z Najwyższą Izbą Kontroli, 12.12.2011 r.

W dniu 12 grudnia 2011 r. w Warszawie, dr Wojciech R. Wiewiórowski, GODO i Jacek Jezierski, Prezes NIK podpisali porozumienie w sprawie zasad współpracy Najwyższej Izby Kontroli i Biura Generalnego Inspektora Ochrony Danych Osobowych. Współpraca obejmować będzie przekazywanie – z zachowaniem przepisów o tajemnicach ustawowo chronionych – zbiorczych informacji z wyników przeprowadzonych kontroli z zakresu ochrony danych osobowych, udział w kursach i szkoleniach organizowanych przez Strony, spotkaniach informacyjno-szkoleniowych, wzajemną wymianę doświadczeń, wspólne prowadzenie kontroli w uzgodnionym zakresie tematycznym i konsultacje w odniesieniu do metodyki prowadzenia kontroli.

6.2.9 Inne informacje

a) Zalecenia dla Kościoła prawosławnego

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 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.

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

Podobnie, jak w latach poprzednich, również w 2011 r. przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych aktywnie uczestniczył w pracach Komitetu Technicznego nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych przy Polskim Komitecie Normalizacyjnym (PKN). Działalność GODO była zwrócona szczególnie na prace podejmowane przez Komitet JTC/SC27 w ramach grupy roboczej WG 5 - Identity Management and Privacy Technologies. W roku 2011 w ramach ww. Komitetu Technologicznego KT-182 przygotowanych zostało 97 projektów norm.

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.

Z ramienia Rzeczypospolitej Polskiej Generalny Inspektor Ochrony Danych Osobowych uczestniczy w pracach Komitetu Konsultacyjnego ds. Konwencji 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (T-PD). Prace Komitetu T-PD koncentrują się obecnie na modernizacji Konwencji 108 z dnia 28 stycznia 1981 r., która ma na celu zagwarantowanie, na terytorium każdej ze Stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowanie jej praw i podstawowych wolności, w szczególności prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych.

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 odbywających się cyklicznie raz w roku spotkaniach Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji (tzw. Grupa Berlińska).

W omawianym roku sprawozdawczym 2011, podobnie jak w latach poprzednich, na szczególne podkreślenie zasługuje 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.

W tym miejscu warto przypomnieć, że w minionym roku sprawozdawczym, podczas I posiedzenia GR Art. 29, które odbyło się 15-16 lutego 2010 r., przyjęty został Program prac na lata 2010-2011 (WP 170)⁴⁵³. Podkreślono w nim, że celem Grupy Roboczej będzie przede wszystkim zapewnienie spójnego i prawidłowego stosowania istniejących ram prawnych w zakresie ochrony danych osobowych. Grupa w swoich pracach koncentrować się będzie na wyzwaniach związanych z rozwojem nowych technologii, globalizacją i zmianami instytucjonalnymi wynikającymi z wejścia w życie Traktatu 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 oraz inne kwestie sektorowe (np. dane osobowe podróżnych, czy przekazywanie danych w kontekście transferów finansowych).

W roku sprawozdawczym 2011 Generalny Inspektor Ochrony Danych Osobowych uczestniczył we wszystkich czterech posiedzeniach wspomnianej Grupy. Podczas 79 posiedzenia europejskie organy ochrony danych zrzeszone w ramach Grupy Roboczej Art. 29 przyjęły Opinię 9/2011 w sprawie ram oceny wpływu na ochronę danych dla aplikacji RFID. Uznano, że identyfikacja za pomocą fal radiowych (RFID) wskazuje na nowy kierunek w społeczeństwie informacyjnym, w którym mamy coraz więcej przedmiotów wyposażonych w elementy mikroelektroniczne zdolne do automatycznego przetwarzania danych o swoich użytkownikach. Ponadto, w posiedzeniu tym uczestniczył Przewodniczący Komitetu Konsultacyjnego Konwencji 108 Rady w celu przedstawienia i omówienia zakresu prac nad zmianą Konwencji 108 planowanych przez Radę Europy. Celem tej zmiany nie będzie preredagowywanie tekstu, ponieważ podstawowe zasady nadal pozostają w mocy, lecz modernizacja Konwencji oraz wzmocnienie mechanizmów z niej wynikających.

W takcie kolejnych posiedzeń Grupy przyjęta została Opinia 10/2011 w sprawie wniosku Komisji Europejskiej dotyczącego utworzenia systemu PNR UE. Dokument ten odwoływał się do dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania,

⁴⁵³ 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

prowadzenia dochodzeń i ścigania sprawców. W ramach tego systemu linie lotnicze byłyby zobowiązane do wymiany informacji dotyczących pasażerów ze służbami bezpieczeństwa w celu zapobiegania, wykrywania, prowadzenia dochodzeń i ścigania sprawców działań terrorystycznych i poważnej przestępczości. W opinii GR Art. 29 niedostatecznie udowodniono konieczność utworzenia proponowanego systemu. Ponadto przedstawione środki nie były zgodne z zasadą proporcjonalności, ponieważ wniosek przewidywał gromadzenie wszystkich danych od wszystkich pasażerów wszystkich lotów, wstępnie do i z krajów trzecich, ale przegląd uwzględniał też rozszerzenie tych informacji o przeloty wewnątrz UE.

Natomiast w Opinii 12/2011 w sprawie inteligentnego opomiarowania (smart metering), które toruje drogę dla inteligentnych systemów elektroenergetycznych (smart grids), Grupa Robocza Art. 29 podkreśliła konieczność dokładnego określenia administratora danych, ponieważ technologia ta niesie za sobą ogromny potencjał dla licznych nowatorskich metod przetwarzania danych i dostarczania usług konsumentom, stawiając w ten sposób nowe wyzwania dla stosowania prawa o ochronie danych osobowych. Z kolei w Opinii 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych (WP 185) zwrócono uwagę na istotę przetwarzania danych geolokalizacyjnych w kontekście obecnie stosowanych technologii, takich jak telefonia komórkowa, systemy nawigacji satelitarnej czy też bezprzewodowy dostęp do Internetu (Wi-Fi). Zasygnalizowano również szerokie możliwości łączenia informacji z wielu źródeł, jakimi są z jednej strony informacje o sygnałach otaczających nas stacji telefonii komórkowych i sygnałach systemów nawigacji satelitarnej, z drugiej zaś strony informacje dostępne na stronach internetowych serwisów geolokalizacyjnych są systematycznie zbierane przez operatorów tych serwisów. Z uwagi na to, że użytkownicy smartphonów i tabletów często noszą przy sobie te urządzenia, a one z kolei pozwalają śledzić, w jakich miejscach przebywają, w związku z czym kwestia ochrony prywatności jest tu bardzo istotna. We wnioskach przedstawiono zalecenia dla poszczególnych stron biorących udział w przedmiotowym procesie, zarówno dla operatorów systemów geolokalizacyjnych, podmiotów świadczących usługi geolokalizacyjne, jak i producentów urządzeń i oprogramowania wykorzystywanego do usług geolokalizacyjnych. W zaleceniach tych wskazano m.in. na obowiązek informacyjny, prawa osób, których dane dotyczą, oraz okresy zatrzymywania danych.

Podczas posiedzenia plenarnego w dniu 13 czerwca 2011 r. Grupa Robocza Art. 29 wydała 44 zalecenia dotyczące ochrony prywatności i ochrony danych w związku z zapobieganiem zjawiskom prania pieniędzy i finansowania terroryzmu („AML/CFT”), ujęte w Opinii 14/2011. Celem zaleceń było przedstawienie stanowiska i udostępnienie praktycznych wskazówek ustawodawcom, podmiotom sprawozdawczym, organom regulacyjnym, jednostkom wywiadu finansowego, organom nadzorczym i innym zainteresowanym stronom, które mają za zadanie stosowanie przepisów o zapobieganiu zjawiskom prania brudnych pieniędzy i finansowania terroryzmu oraz w odniesieniu do prywatności i

ochrony danych – zarówno na szczeblu unijnym, jak i na szczeblu poszczególnych państw członkowskich. W opinii Grupy środki stosowane jako środki konieczne w celu zapobiegania tym zjawiskom, powinny zawsze mieć wyraźną podstawę prawną i być niezbędne oraz proporcjonalne do charakteru danych. Grupa Robocza zaleca między innymi dokonanie przeglądu obowiązujących obecnie oraz proponowanych przepisów w celu większego ich ujednolicenia na szczeblu UE, wprowadzenie czytelnej polityki w obszarze ochrony danych, rozpowszechnianie w zrozumiałej formie informacji o koniecznych środkach zapobiegawczych odnośnie tych zjawisk, jak kwestionariusze i ograniczanie usług oraz wyraźne stosowanie zasady celowości w przepisach. Prawa i obowiązki w obszarze prywatności i ochrony danych powinny zawsze być podejmowane i opracowywane **w sposób pozytywny** w odniesieniu do kwestii prywatności i ochrony danych. Przykład podejścia negatywnego zakłada, że ochrona danych i poszanowanie prywatności w walce z przestępczością przedstawiane są jako przeszkoda, którą powinno się obejść, zaś podejście jest ograniczone do ogólnego stosowania wyjątków od przepisów o ochronie danych. Pojęcie podejścia pozytywnego ilustrują między innymi zalecenia dotyczące konkretnych działań, takich jak przyjęcie publicznej i udokumentowanej polityki w celu zachowania zgodności z przepisami dotyczącymi prywatności i ochrony danych, wewnętrzna polityka ochrony poufnych danych, zapobieganie kradzieży tożsamości, wykorzystanie wyłączeń jednostek analityki finansowej dla zastosowania typologii oraz mechanizm informacji zwrotnych, zapewnienie odpowiednich zabezpieczeń dla wszystkich operacji profilowania, nieustanne oceny dokładności danych, przechowywanie informacji o źródłach danych i datach w odniesieniu do wszystkich danych i ocen AML/CFT, dostęp i nadzór za pośrednictwem organów ochrony danych i ochrona danych szczególnie chronionych.

Kolejną ważną kwestią przedstawioną w stanowisku GR Art. 29, była opinia w sprawie definicji zgody (Opinia 15/2011), która jest kluczowym pojęciem w dziedzinie ochrony danych i prawa do prywatności. Zgoda jest bowiem jedną z podstaw mogących stanowić przesłankę legalności przetwarzania danych osobowych. W opinii europejskich organów ochrony danych zgoda wymaga wykorzystania mechanizmów, które nie pozostawiają wątpliwości co do zamiaru jej wyrażenia przez osobę, której dane dotyczą („dobrowolna”, „konkretna”, „jednoznaczna”, „wyraźna”, „świadoma”, itd.). Toteż tylko oświadczenia lub działania, a nie milczenie lub brak działania, mogą stanowić podstawę uznania ważności zgody. Na przykład, gdy osoba, której dane dotyczą, rejestruje się w portalu społecznościowym i domyślne ustawienia prywatności jej profilu powodują, że dotyczące jej dane osobowe są widoczne dla wszystkich, nie można na tej podstawie uznać, że użytkownik wyraził zgodę. Zgoda musi być wyrażona przed rozpoczęciem przetwarzania lub przed każdym wykorzystaniem danych w nowym celu. Europejskie organy ochrony danych podkreślają również, że powinno być zagwarantowane prawo do wycofania zgody. Ponadto, aby osoby, których dane dotyczą, mogły dokonywać świadomych wyborów, muszą być informowane o przetwarzaniu danych, a dobra jakość

i dostępność informacji ma tu kluczowe znaczenie. Oczywiście w tym względzie szczególną uwagę należy zwrócić na osoby nieposiadające zdolności do czynności prawnych, np. nieletnich. I wreszcie, administratorzy danych powinni być w stanie wykazać, że uzyskali ważną zgodę.

Podczas ostatniego w 2011 r. posiedzenia Grupy Roboczej Artykułu 29 ds. Ochrony Danych w Brukseli, przyjęta została Opinia 16/2011 w sprawie zaleceń Europejskiego Stowarzyszenia Standardów Reklamy (EASA) i Europejskiego Biura Reklamy Interaktywnej (IAB) dotyczących najlepszych praktyk w internetowej reklamie behawioralnej. W opinii Grupa Robocza z zadowoleniem przyjęła inicjatywę samoregulacyjną branży w obszarze reklamy behawioralnej. W konkluzji stwierdziła jednak, że przestrzeganie przygotowanego przez EASA i IAB „Kodeksu w zakresie reklamy behawioralnej” oraz aktywność w ramach strony internetowej www.youronlinechoices.eu nie skutkuje zgodnością z Dyrektywą o prywatności i łączności elektronicznej. Co więcej, Grupa Robocza podkreśliła, że Kodeks oraz strona internetowa tworzą niewłaściwe założenie, że możliwe jest wybranie opcji „nie chcę być śledzonym” podczas surfowania po Internecie. To błędne założenie może być szkodliwe dla użytkowników oraz dla branży, jeśli wierzy ona, że poprzez stosowanie Kodeksu spełnia wymogi dyrektywy.

Podczas tego posiedzenia miało miejsce spotkanie z Panią Viviane Reding, Wiceprzewodniczącą Komisji Europejskiej, w celu omówienia przeglądu ram prawnych ochrony danych. Organy ochrony danych podkreśliły znaczenie globalnego podejścia do ochrony danych poza granicami UE, dopracowania mechanizmu zgodności wspólnie podejmowanych działań, potrzebę zapewnienia rzeczywistego prawa do bycia zapomnianym, a także potrzebę spójności i zgodności zasad w przyszłej regulacji, zwłaszcza tych, dotyczących policji i organów sądowych. Podczas tego spotkania Wiceprzewodnicząca KE zasygnalizowała też zamiar utworzenia Europejskiej Rady Ochrony Danych, złożonej z obecnej GR Art. 29.

Na podkreślenie zasługuje także aktywny udział przedstawiciela GIODO – jako eksperta krajowego – w wydarzeniach organizowanych przez Dyрекcję ds. Rozszerzenia Komisji Europejskiej w ramach TAIEX (Technical Assistance and Information Office), podczas których przedstawiał prezentacje tematyczne. I tak, w dniu 28-29 marca 2011 r. w Skopje w Macedonii brał udział w seminarium dotyczących przejrzystości i ochrony danych, a w dniu 23 maja 2011 r. w Sarajewie – w szkoleniu dla urzędników agencji ochrony danych Bośni i Hercegowiny. Natomiast w dniach 11-12 października 2011 r. w Kijowie współprzewodniczył i wygłosił dwa wykłady w trakcie warsztatów poświęconych krajowym doświadczeniom we wdrażaniu przepisów o ochronie danych osobowych.

Oprócz przedstawionej powyżej aktywności Generalnego Inspektora Ochrony Danych Osobowych na polu międzynarodowym, inną formą współpracy GIODO z europejskimi organami ochrony danych osobowych był udział w różnego rodzaju międzynarodowych projektach badawczych i konsultacjach w sprawie stworzenia kompleksowych ram prawnych w zakresie podstawowego prawa

do ochrony danych osobowych. Z tej okazji Generalny Inspektor Ochrony Danych Osobowych uczestniczył w specjalnych spotkaniach z organami państw członkowskich oraz z innymi zainteresowanymi stronami. W dniu 28 stycznia 2011 r. (Dzień Ochrony Danych Osobowych) brał udział w konferencji wysokiego szczebla zorganizowanej przez Komisję Europejską i Radę Europy, w celu omówienia kwestii związanych z reformą ram prawnych ochrony danych osobowych w UE, a także wypracowania wspólnych standardów ochrony danych na całym świecie. Węgierska i polska Prezydencja w Radzie UE były gospodarzami dwóch konferencji na temat ochrony danych, które odbyły się odpowiednio, w dniach 16-17 czerwca 2011 r. w Budapeszcie i 21 września 2011 r. w Warszawie. W związku ze wspomnianymi pracami nad określeniem ram prawnych, przeprowadzone zostały konsultacje z obywatelami Unii Europejskiej za pośrednictwem kwestionariusza Eurobarometru⁴⁵⁴, którego wyniki ogłoszono w 2011 r.

W 2011 r. Generalny Inspektor ochrony Danych Osobowych uczestniczył również w przygotowaniu wielu kwestionariuszy w zakresie dotyczącym technologicznych aspektów przetwarzania danych osobowych będących w zakresie zainteresowania Komisji Europejskiej i Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych. Do najważniejszych z nich należały kwestionariusze dotyczące: stopnia wdrożenia i wykorzystywania w Polsce inteligentnego opomiarowania, zakresu korzystania w Polsce z usług Google Analytics oferowanych nieodpłatnie przez Google Inc (Questionnaire on Google Analytics and web audience measurements, survey of the technical, legal and political issues), kwestionariusz dotyczący prac i działań podjętych w zakresie dotyczącym realizacji prac mających na celu implementację postanowień dyrektywy 2009/136/WE zmieniającej dyrektywę 2002/22/WE, dyrektywę 2002/58/WE oraz rozporządzenie (WE) nr 2006/2004, przetwarzania danych osobowych w sektorze wymiaru sprawiedliwości będący częścią badania przeprowadzanego przez Komitet Konsultacyjny Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych (T-PD), a także kwestionariusz dotyczący skutków i działań podejmowanych w związku z włamaniem do systemu Sony, czy też działań podejmowanych w związku z ujawnieniem mechanizmów śledzenia użytkowników wbudowanych w mobilne telefony firmy Apple.

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.

⁴⁵⁴ Specjalna ankieta Eurobarometru (EB) nr 359 „Ochrona danych i tożsamość elektroniczna w UE” (2011: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).

7.1 Międzynarodowe konferencje, seminaria i spotkania

Generalny Inspektor Ochrony Danych Osobowych oraz przedstawiciele jego Biura uczestniczyli także w konferencjach, seminariach i spotkaniach o charakterze międzynarodowym w kraju i za granicą (zał. 9).

Pierwszym w kolejności wydarzeniem 2011 roku z udziałem dra Wojciecha R. Wiewiórowskiego, GIODO, były - opisane w innej części niniejszego Sprawozdania - uroczystości związane z obchodami **V Europejskiego Dnia Ochrony Danych Osobowych, które odbyły się w Brukseli w dniach 24, 26-27 i 28 stycznia 2011 r.** W szczególności zaś udział GIODO w konferencjach: 24.01.2011 r. „Data Breach Notification In Europe – The way forward” zorganizowanej przez ENISA, gdzie wygłosił referat „Data Protection Authorities’ Views on Data Breach Notifications” i 28.01.2011 r. w Konferencji pt. „Data protection 30 years later: from European to international standards” zorganizowanej przez Radę Europy i Komisję Europejską, podczas której wygłosił referat „From European to international standards on data protection. Introduction”.

Natomiast w dniu **27 stycznia 2011 r. w Budapeszcie, w Konferencji pt. „Portale społecznościowe”** zorganizowanej z okazji V Dnia Ochrony Danych Osobowych przez Urząd Węgierskiego Parlamentarnego Rzecznika Ochrony Danych Osobowych i Wolności Informacji, uczestniczył Pan Piotr Drobek, zastępca Dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej Biura GIODO.

Wśród innych najważniejszych wydarzeń o charakterze międzynarodowym należy wymienić:

1. **Obrady Okrągłego Stołu „Ochrona danych osobowych: normy europejskie i ustawodawstwo ukraińskie”** (Kijów, 10-11 marca 2011 r.)

Seminarium zorganizowane było przez Dyрекcję Generalną ds. Praw Człowieka i Spraw Prawnych w ramach Projektu Rady Europy dotyczącego europejskich standardów w mediach ukraińskich w Kijowie. Podczas tego wydarzenia dr Wojciech Wiewiórowski, GIODO, przedstawił prezentację na temat doświadczeń Polski w zakresie regulacji kwestii dotyczących ochrony danych oraz wyzwań stojących przed państwami Europy Środkowej i Wschodniej. Generalny Inspektor Ochrony Danych Osobowych spotkał się także z nowo powołanym szefem służby ochrony danych Ukrainy. Przedmiotem spotkania było omówienie zasad współpracy GIODO z nowo utworzonym ukraińskim organem ochrony danych, w związku z faktem, że 1 stycznia 2011 r. na Ukrainie weszły w życie Konwencja 108 oraz ustawa o ochronie danych osobowych.

2. **Wiosenna Konferencja Europejskich Rzeczników Ochrony Danych** (Bruksela, 05 kwietnia 2011 r.)

Gospodarzami corocznej Wiosennej Konferencji Europejskich Rzeczników Ochrony Danych byli Europejski Inspektor Ochrony Danych Osobowych (EIOD) i Przewodniczący Grupy Roboczej artykułu

29 ds. Ochrony Danych. Głównym tematem spotkania był przegląd ram prawnych ochrony danych osobowych. Podczas Konferencji przyjęta została rezolucja, w której podkreślono potrzebę opracowania całościowych ram prawnych ochrony danych, obejmujących również sektor egzekwowania prawa. Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości oraz Grupa Robocza Art. 29 postanowiły zacieśnić współpracę, aby zwiększyć skuteczność swojej roli doradczej w sprawach związanych z szeroko rozumianym bezpieczeństwem.

3. Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z Dyrektorem Agencji Praw Podstawowych (Warszawa, 08 kwietnia 2011 r.)

Celem spotkania dra Wojciecha R. Wiewiórowskiego, GIODO, z Dyrektorem Agencji Praw Podstawowych (APP) Panem Morten'em Kjaerum'em było omówienie możliwości i form wzajemnej współpracy. Podczas spotkania Dyrektor APP przedstawił działania Agencji, w tym plan pracy na 2011 r. w odniesieniu do tematyki społeczeństwa informatycznego oraz poszanowania życia prywatnego i ochrony danych osobowych (np. badanie stanu wdrażania oraz wiedzy w społeczeństwie w kwestii mechanizmów ochrony prawnej na podstawie Dyrektywy 95/46/WE), zaś Generalny Inspektor Ochrony Danych Osobowych omówił działania, zadania i kompetencje GIODO, jak również najważniejsze problemy, z jakimi się spotyka w swojej działalności. Poruszył także kwestię zbliżającej się Prezydencji RP w Radzie UE.

4. 13. Spotkanie Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, CEEDPA (Budapeszt, 28-29 kwietnia 2011 r.)

Gospodarzem tego wydarzenia był Węgierski Parlamentarny Rzecznik Ochrony Danych Osobowych i Wolności Informacji. Tegoroczne spotkanie poświęcone było roli i kompetencjom krajowych organów ochrony danych. W spotkaniu uczestniczył dr Wojciech R. Wiewiórowski, GIODO, który przedstawił uczestnikom Spotkania zadania Generalnego Inspektora po wejściu w życie w dniu 7 marca 2011 r. znowelizowanej ustawy o ochronie danych osobowych oraz kierunki prac nad przyszłymi zmianami ustawodawstwa o ochronie danych osobowych w Polsce. Po raz pierwszy w Spotkaniu CEEDPA uczestniczył Jacob Kohnstamm, Przewodniczący Grupy Roboczej Art. 29 ds. Ochrony Danych, który w swoim wystąpieniu poruszył m.in. kwestie dotyczące roli organów ochrony danych osobowych z państw Europy Środkowej i Wschodniej w pracach Grupy. W trakcie spotkania w poczet członków Grupy oficjalnie przyjęto organy ochrony danych z Serbii i Ukrainy, których przedstawiciele uczestniczyli w tym wydarzeniu. Podjęto również decyzję o organizacji kolejnego Spotkania w 2012 r. na Ukrainie.

5. Międzynarodowe seminarium pt. „Wiążące Reguły Korporacyjne – pojęcie, stosowanie, doświadczenia praktyczne” (Warszawa, 14 czerwca 2011 r.)

Wiążące Reguły Korporacyjne (BCR) systematycznie zyskują zainteresowanie jako realna alternatywa pozwalająca zapewnić odpowiednią ochronę danych osobowych, będących przedmiotem transferów

w ramach korporacji międzynarodowych. Ostatnie doświadczenia wykazały, że obecna procedura zatwierdzania BCR powinna zostać uproszczona i zoptymalizowana, aby BCR stały się bardziej atrakcyjnym narzędziem prawnym. W związku z tym Generalny Inspektor Ochrony Danych Osobowych zorganizował międzynarodowe seminarium poświęcone promocji BCR, podczas którego omawiane były m.in. zagadnienia związane z krajowymi wymogami zatwierdzania BCR i praktyczne aspekty ich wdrażania, a także procedury koordynacji i wzajemnego uznawania między organami ochrony danych a środowiskami gospodarczymi. Seminarium to skierowane było głównie do przedsiębiorstw o zasięgu międzynarodowym, kancelarii prawnych, specjalistów z zakresu ochrony danych oraz innych osób zajmujących się ochroną danych oraz przekazywaniem danych osobowych. Podczas seminarium dr Wojciech R. Wiewiórowski, GODO, wręczył nagrody w konkursie dla studentów wydziałów prawa pt. „Zastosowanie przepisów o ochronie danych osobowych w celu stworzenia portalu społecznościowego do wymiany informacji między kibicami piłki nożnej”.

6. Międzynarodowa Konferencja o Ochronie Danych (Budapeszt, 16-17 czerwca 2011 r.)

W ramach współpracy Prezydencji Węgierskiej i Polskiej w Budapeszcie, w dniach 16-17 czerwca 2011 r. odbyła się Międzynarodowa Konferencja o Ochronie Danych Osobowych, której współorganizatorem był Generalny Inspektor Ochrony Danych Osobowych. Konferencja została zorganizowana w ramach projektu realizowanego z Programu Komisji Europejskiej Prawa Podstawowe i Obywatelstwo, który zakładał zorganizowanie w 2011 r. cyklu międzynarodowych konferencji poświęconych tematyce ochrony danych osobowych. Partnerami Projektu byli, poza GODO, Ministerstwo Spraw Wewnętrznych i Administracji, węgierskie Ministerstwo Sprawiedliwości i Administracji Publicznej, węgierski organ ochrony danych, Rada Europy, Europejska Akademia Prawa oraz hiszpańskie Ministerstwo Sprawiedliwości. Podczas Konferencji omówiono obecne zagadnienia związane z ochroną danych osobowych oraz stojące przed nimi wyzwania na przyszłość. Dr Wojciech R. Wiewiórowski, GODO, przedstawił prezentację nt. ochrony prywatności i odpowiedzialności dostawców usług internetowych w chmurach, a także przewodniczył sesji roboczej poświęconej nowym zasadom w dziedzinie ochrony danych. Wykład na temat działań edukacyjnych GODO wygłosiła również Urszula Góral, Dyrektor Departamentu Edukacji Społecznej i Współpracy Międzynarodowej Biura GODO

7. 24. Coroczna Międzynarodowa Konferencja Privacy Laws & Business (Cambridge, 11-13 lipca 2011 r.)

Mottem tegorocznej Konferencji było „Uwzględnienie ochrony prywatności w strategii biznesowej firmy”. Podstawowe tematy Konferencji dotyczyły strategii i rozliczalności, zmian w przepisach dotyczących ochrony danych w Europie, Azji i Ameryce Łacińskiej, rewizji europejskiej dyrektywy o ochronie danych, międzynarodowych przepływów danych osobowych, bezpieczeństwa i ochrony

prywatności i przejrzystości, privacy by design (uwzględnianie ochrony prywatności w fazie projektowania), cloud computing oraz perspektywy dla wspólnych działań w Europie.

Drugiego dnia Konferencji dr Wojciech R. Wiewiórowski, GODO, wygłosił referat pt. „Plany Polski dotyczące ochrony danych na czas polskiej Prezydencji w Radzie Unii Europejskiej, od lipca do grudnia 2011 r.”. Wśród poruszonych tematów znalazły się takie zagadnienia, jak Agenda Cyfrowa dla Europy – stan rzeczy w zakresie zaufania i bezpieczeństwa, ogólny przegląd ram prawnych ochrony danych, aspekty ochrony prywatności w dyrektywie w sprawie ponownego wykorzystywania informacji sektora publicznego, dane osobowe w rejestrach publicznych – współpraca w zakresie e - Administracji w Europie, Ochrona prywatności i RFID – podsumowanie działań krajowych, obowiązkowe zatrzymywanie danych w sektorze internetowym i telekomunikacyjnym, a także zagadnienia związane z europejskim PNR. Następnie dr Wojciech R. Wiewiórowski przedstawił swój komentarz do referatu wygłoszonego przez Europejskiego Inspektora Ochrony Danych Osobowych Petera Hustinx'a zatytułowanego „Aktualne informacje na temat zrewidowanej dyrektywy o ochronie danych UE: w drodze do większej harmonizacji poprzez rozporządzenie lub dyrektywę”. W tym samym dniu podczas popołudniowej sesji poświęconej kwestiom międzynarodowym, Generalny Inspektor wygłosił referat na temat zmian w znowelizowanej polskiej ustawie o ochronie danych osobowych, która weszła w życie 7 marca 2011 r. podkreślając aktywną rolę organu ds. ochrony danych w procesie legislacji, nowe zasady dotyczące zgody, czy procedury egzekwowania prawa.

8. 50. Posiedzenie Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (Berlin, 11-13 września 2011 r.)

Najważniejszymi tematami poruszonymi podczas 50. Posiedzenia Grypy Berlińskiej w kontekście ochrony prywatności były kwestie związane z bezpieczeństwem elektronicznych usług płatności w Internecie, cloud computing, smart grids, dane geolokalizacyjne i ochrona danych użytkowników portali społecznościowych. Dyskutowano również nad Protokołem IPV6 oraz ochroną prywatności w perspektywie międzynarodowej standaryzacji. Z ramienia Generalnego Inspektora Ochrony Danych Osobowych w Spotkaniu tym uczestniczył Andrzej Kaczmarek, Dyrektor Departamentu Informatyki Biura GODO, który zaprezentował perspektywę polską dyskutowanych zagadnień. Organizatorem Spotkania był Berliński Rzecznik Ochrony Danych i Wolności Informacji.

9. Międzynarodowa Konferencja o Ochronie Danych Osobowych (Warszawa, 21 września 2011 r.)

Celem Konferencji była identyfikacja i omówienie aktualnych potrzeb dotyczących ram prawnych ochrony danych na poziomie europejskim, odnoszących się do konkretnych i praktycznych osiągnięć w poszczególnych państwach członkowskich. Organizatorami Konferencji, która w ramach Prezydencji Polski w Radzie UE odbyła się w siedzibie GODO, byli Generalny Inspektor Ochrony Danych Osobowych oraz Ministerstwo Spraw Wewnętrznych i Administracji. Partnerami tego

międzynarodowego wydarzenia byli Węgierski Parlamentarny Rzecznik Ochrony Danych i Wolności Informacji, Węgierskie Ministerstwo Administracji Publicznej i Sprawiedliwości, Rada Europy, Komisja Europejska, Akademia Prawa Europejskiego i Hiszpańskie Ministerstwo Sprawiedliwości.

10. Spotkanie GIODO z przedstawicielami TechAmerica (Bruksela, 27 września 2011 r.)

Tematem Spotkania była harmonizacja prawa w zakresie ochrony danych osobowych, w tym rewizja dyrektywy 95/45/WE, Privacy by Design, a także zgłaszanie naruszeń ochrony danych. Podczas Spotkania dr Wojciech R. Wiewiórowski zaprezentował polski punkt widzenia na ww. zagadnienia. Ponadto na zaproszenie prof. Paula De Herta wygłosił wykład na Vrije Universiteit Brussel pt. „Considerations & Contextual Factors Contributing to the Introduction of Privacy Impact Assessments (PIA) in Poland.”

11. Posiedzenie European Privacy Officers Forum (Bruksela, 28 września 2011 r.)

Podczas posiedzenia EPOF dr Wojciech R. Wiewiórowski, GIODO, przedstawił prezentację pt. „Digital single Market in Europe. European and National Legislation as Promotion and Obstacle for Access to Personal Data”. Omawiając ustawodawstwo krajowe i europejskie odniósł się do idei utworzenia jednolitego rynku cyfrowego w Europie, wskazując na bariery dla dostępu do danych osobowych.

12. II Międzynarodowa Konferencja pt. „Ochrona danych osobowych” (Moskwa, 25-26 października 2011 r.)

Z inicjatywy Federalnej Służby Nadzoru w sektorze Łączności, Technologii Informacyjnych i Masowej Komunikacji Federacji Rosyjskiej, w dniach 25-26 października 2011 r. odbyła się w Moskwie konferencja poświęcona ochronie danych osobowych. Przedstawiciele organów właściwych w zakresie ochrony danych osobowych reprezentowali 15 krajów: Albanię, Armenię, Białoruś, Bośnię i Hercegowinę, Niemcy, Kazachstan, Kirgistan, Litwę, Łotwę, Macedonię, Mołdawię, Polskę, Ukrainę, Chorwację i Estonię. Współpraca międzynarodowa w zakresie ochrony danych osobowych: główne trendy i perspektywy rozwoju oraz zmiany w ustawodawstwie Federacji Rosyjskiej w dziedzinie danych osobowych to tematy, które zostały poruszone na tym spotkaniu. Podczas pierwszego dnia Konferencji, która miała charakter okrągłego stołu, dr Wojciech R. Wiewiórowski, GIODO, omówił prawne, polityczne i społeczne podłoże niezależności organu ochrony danych. Natomiast w drugim dniu tego wydarzenia, GIODO skoncentrował swój wykład na zagadnieniach dotyczących biometrii i ochrony prywatności, a także adekwatności danych przechowywanych dla celów określonych przez administratora danych.

13. 33. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności – Prywatność: Era Globalna (Meksyk, 01-03 listopada 2011 r.)

Konferencja, jak co roku, podzielona została na dwie części. Podczas sesji zamkniętej, w której z prawem głosu uczestniczyli akredytowani rzecznicy ochrony danych osobowych i prywatności,

przyjęto *Rezolucję w sprawie egzekwowania przepisów w zakresie ochrony prywatności i współpracy na poziomie międzynarodowym*. W celu realizacji jej postanowień powołano grupę roboczą, w skład której wszedł m.in. Generalny Inspektor Ochrony Danych Osobowych. Ponadto przyjęto *Rezolucję w sprawie wykorzystania unikalnych identyfikatorów przy wdrażaniu IPv6*, *Rezolucję w sprawie ochrony danych w kontekście wielkich katastrof naturalnych*, a także *Rezolucję akredytacyjną*. Podczas ogólnodostępnych sesji otwartych podzielonych na sesje plenarne oraz równoległe sesje panelowe dyskutowano nad aktualnymi problemami związanymi z ochroną prywatności i danych osobowych, w tym m.in. o wyzwaniach stojących przed organami ochrony prywatności i danych osobowych, związanych z obecnym rozwojem technologicznym i globalizacją, efektywnością ustawodawstwa o ochronie danych osobowych, zmianami ram prawnych ochrony danych osobowych i prywatności w Unii Europejskiej i Stanach Zjednoczonych Ameryki, a także o różnych aspektach działania organów ochrony prywatności i danych osobowych. W sesji poświęconej prywatności w kontekście przetwarzania danych w chmurze (Cloud computing) jednym z panelistów był dr Wojciech R. Wiewiórowski, GODO. Generalny Inspektor wziął również udział w odbywającej się w powiązaniu z 33. Konferencją Rzeczników Ochrony Danych i Prywatności konferencji organizowanej pod egidą OECD oraz odrębnej konferencji zorganizowanej przez organizacje pozarządowe zajmujące się ochroną prywatności i danych osobowych.

14. Konferencja „Ochrona danych osobowych 15 lat po uchwaleniu włoskiej ustawy o ochronie prywatności” (Mediolan, 11 listopada 2011 r.)

W dniu 11 listopada 2011 r. w Mediolanie odbyła się konferencja zorganizowana na Uniwersytecie Bocconi z okazji 15-lecia obowiązywania włoskiej ustawy o ochronie danych. Debata koncentrowała się na omówieniu doświadczeń z dziedziny prawa do prywatności i ochrony danych osobowych przez prelegentów z Włoch, Niemiec oraz Finlandii. Polskie doświadczenia w tej dziedzinie przedstawił dr Wojciech R. Wiewiórowski, GODO, odnosząc się także do takich zagadnień, jak wpływ nowych technologii na ochronę prywatności ze szczególnym uwzględnieniem prywatności w Internecie.

15. 6. Europejska Konferencja Ministerialna „Transgraniczne usługi e-administracji dla Europejczyków” (Poznań, 17-18 listopada 2011 r.)

Podczas Konferencji dyskutowane były przyszłe kierunki rozwoju usług e-administracji w Europie. W sesji pod tytułem „Cloud computing and service oriented architecture in public sector” panelistą był dr Wojciech R. Wiewiórowski, GODO, który wygłosił prezentację na temat prawnych aspektów przetwarzania danych w chmurze obliczeniowej w ramach administracji publicznej oraz uczestniczył w dyskusji podczas sesji „Trust and Privacy”. Tegoroczna Konferencja zorganizowana została przez Ministerstwo Spraw Wewnętrznych i Administracji we współpracy z Komisją Europejską.

16. Kongres IAPP (Paryż, 29-30 listopada 2011 r.)

Celem Kongresu zorganizowanego przez międzynarodową organizację International Association of Privacy Professional (IAPP), była wymiana poglądów na temat najnowszych osiągnięć w dziedzinie ochrony prywatności w gronie regulatorów i ekspertów ds. ochrony danych osobowych z całego świata. Podczas Kongresu dr Wojciech R. Wiewiórowski, GODO, wziął udział w sesji poświęconej perspektywie BCR w kontekście przeglądu dyrektywy 95/45/WE, w szczególności w kwestii zapewnienia rozliczalności oraz możliwości efektywniejszego wykorzystania BCR niż standardowych klauzul umownych czy rozwiązań typu safe harbor.

17. 27. plenarne posiedzenie Komitetu Konsultacyjnego ds. Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Strasburg, 29 listopada – 02 grudnia 2011 r.)

Rezultatem społecznych konsultacji przeprowadzonych przez Radę Europy na początku 2011 r., a także prac prowadzonych przez Biuro Komitetu T-PD, był dokument pt. „Modernisation of Convention 108: proposals”. Podczas 27. plenarnego posiedzenia Komitetu T-PD odbyło się pierwsze czytanie propozycji zmian do Konwencji 108 określone w tym dokumencie. Stanowił on, że przepisami Konwencji objęte są podmioty sektora publicznego i prywatnego. Dokument ten gwarantował zachowanie spójności i zgodności przepisów Konwencji z ustawodawstwem UE, jej neutralność pod względem technologicznym, efektywność określonych w niej środków oraz potwierdzał potencjał Konwencji, jako uniwersalnego standardu o charakterze otwartym. Ponadto przewidywał zachowanie istniejących przepisów Konwencji, jak i dodanie bardziej szczegółowych zapisów, w tym także aktualizację terminologii, prostotę formułowania zasad oraz wprowadzenie nowych, jak np. zasady rozliczalności. Propozycje zmian zostaną poddane pisemnym konsultacjom na początku 2012 r., a następnie zatwierdzone na 28. plenarnym zebraniu Komitetu T-PD w czerwcu 2012 r. Rezultaty prac zostaną przedstawione Komitetowi Ministrów Rady Europy. 27. plenarne zebranie Komitetu T-PD było również okazją do przedyskutowania rewizji dokumentów uszczegóławiających postanowienia Konwencji 108 tj. rekomendacji dotyczących zatrudnienia i sektora policji, w celu dostosowania istniejących już dokumentów do obecnych warunków. Spotkanie było również okazją do wyboru nowego Komisarza do spraw Ochrony Danych Rady Europy, którym została Pani Eva Souhrada-Kirchmayer – Członek Zarządzający i Dyrektor Austriackiej Komisji Ochrony Danych.

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 rozstrzygnięcia rozpatrywanych spraw administracyjnych. Uzyskane zaś

przez Generalnego Inspektora informacje o charakterze porównawczym wykorzystywane były w dalszej jego pracy.

a) Wizyta przedstawicieli rumuńskiego organu ochrony danych

Celem dwudniowej wizyty była wymiana doświadczeń obu urzędów w sprawach związanych z działalnością w kontekście sektora telekomunikacji i Internetu. W dniu 29 czerwca 2011 r. podczas spotkania dra Wojciecha R. Wiewiórowskiego - Generalnego Inspektora Ochrony Danych Osobowych, z Panią Georgetą Basarabescu, Przewodniczącą Krajowego Organu Nadzorczego ds. Przetwarzania Danych Osobowych, zostało podpisane Porozumienie o współpracy i wzajemnej wymianie doświadczeń między polskim a rumuńskim organem ochrony danych.**b) Wizyta przedstawicieli macedońskiego organu ochrony danych osobowych**

W dniach 14-15 lipca 2011 r. miała miejsce wizyta studyjna macedońskiego organu ochrony danych osobowych. Spotkanie to odbyło się w ramach projektu Unii Europejskiej „Wsparcie dla Organu Ochrony Danych Osobowych” i miało na celu wymianę doświadczeń obu urzędów. W dniu 15 lipca 2011 r. podczas spotkania dra Wojciecha R. Wiewiórowskiego, GIODO, z Panem Dymitarem Gjeorgjievskim, Dyrektorem Organu Ochrony Danych Osobowych Macedonii, podpisane zostało Porozumienie o współpracy i wzajemnej wymianie doświadczeń między polskim a macedońskim organem ochrony danych.

c) Wizyta przedstawicieli albańskiego organu ochrony danych osobowych

W dniach 22-23 września 2011 r. w Biurze GIODO odbywała się wizyta studyjna przedstawicieli albańskiego organu ochrony danych, zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych i Komisję Europejską w ramach programu TAIEX. Wizyta studyjna skoncentrowana była na następujących kwestiach: tworzenie projektów ustaw i przepisów wykonawczych, postępowania i kontrole oraz dostosowanie ustawodawstwa albańskiego do dorobku prawnego Unii Europejskiej w zakresie ochrony danych. Wizyta studyjna połączona była z zorganizowaną przez polski organ ds. ochrony danych w dniu 21 września 2011 r. Międzynarodową Konferencją o Ochronie Danych Osobowych.

7.3 Międzynarodowe warsztaty

a) Warsztaty ochrony danych osobowych w kontekście współpracy w dziedzinie konsumentów (Bruksela, 21 marca 2011 r.)

W Warsztatach dotyczących ochrony danych osobowych w związku z systemem współpracy w dziedzinie ochrony konsumentów (CPC Workshop on Data Protection), uczestniczyli przedstawiciele organów ochrony danych osobowych. Organizatorem Warsztatów była Komisja

Europejska, Dyrekcja Generalna ds. Zdrowia i Ochrony Konsumentów – DG SANCO. Celem tego spotkania było omówienie możliwości usprawnienia egzekwowania przepisów prawnych dotyczących ochrony konsumentów na rynku wewnętrznym w przypadku transgranicznych naruszeń wspólnotowych przepisów o ochronie konsumentów (np. reklamy wprowadzającej w błąd, sprzedaży na odległość, kredytu konsumenckiego, transmisji telewizyjnych, nieuczciwych warunków umów, handlu elektronicznego, itd.) w kontekście istniejących podstawowych ram prawnych przetwarzania danych w systemie współpracy w dziedzinie ochrony konsumentów.

b) Warsztaty poświęcone wiążącym regułom korporacyjnym (Warszawa, 15 czerwca 2011 r.)

Warsztaty dla przedstawicieli organów ochrony danych osobowych państw członkowskich UE pt.: „Wiążące reguły korporacyjne w praktyce: wymiana doświadczeń pomiędzy organami ochrony danych”, zorganizowane były przez polski organ ochrony danych we współpracy z francuskim organem ochrony danych (CNIL). Podstawowym celem tego spotkania była wymiana doświadczeń i wiedzy w zakresie praktycznego stosowania wiążących reguł korporacyjnych. Podczas warsztatów zostały poruszone m.in. kwestie dotyczące metodologii analizy wniosku BCR. Ponadto przedstawiono zagadnienie ‘BCR dla przetwarzających’. W spotkaniu wzięły udział 22 osoby reprezentujące 16 europejskich organów ochrony danych osobowych oraz przedstawiciel Komisji Europejskiej

c) Warsztaty z ochrony danych osobowych dla przedsiębiorców (Warszawa, 20 lipca 2011 r.)

W dniu 20 lipca 2011 r. w siedzibie GODO odbyły się warsztaty podsumowujące projekt partnerski pt. „Zwiększanie świadomości w zakresie ochrony danych osobowych wśród przedsiębiorców funkcjonujących na rynkach Unii Europejskiej”. Projekt ten był realizowany wspólnie przez Biuro Generalnego Inspektora Ochrony Danych Osobowych w Polsce, Urząd Ochrony Danych Osobowych Republiki Czeskiej i Parlamentarnego Rzecznika Ochrony Danych i Wolności Informacji na Węgrzech, przy wsparciu finansowym Komisji Europejskiej w ramach programu „Uczenie się przez całe życie”. Podczas warsztatów została zaprezentowana publikacja skierowana do osób prowadzących działalność gospodarczą w Polsce, Republice Czeskiej i na Węgrzech pt.: „Wybrane zagadnienia ochrony danych osobowych. Poradnik dla przedsiębiorców” oraz zostały przedstawione prezentacje poświęcone różnym aspektom ochrony danych osobowych w odniesieniu do działalności gospodarczej w tych krajach.

d) Warsztaty Rozpatrywania Spraw (Warszawa, 4-5 października 2011 r.)

Przedstawiciele Biura Generalnego Inspektora Ochrony Danych Osobowych systematycznie uczestniczą w warsztatach rozpatrywania spraw, tzw. warsztatach skargowych (case handling workshop). W dniach 4-5 października 2011 roku w Warszawie odbyły się **23. warsztaty rozpatrywania spraw**, zorganizowane przez Generalnego Inspektora Ochrony Danych Osobowych. W spotkaniu udział wzięli przedstawiciele organów ochrony danych osobowych działających zarówno na poziomie krajowym jak i lokalnym, oraz Europejskiego Inspektora Ochrony Danych. Warunkiem

udziału w Warsztatach jest akredytacja przy Konferencji Europejskich Organów Ochrony Danych. Warsztaty miały na celu praktyczną wymianę doświadczeń pomiędzy pracownikami poszczególnych organów, którzy na co dzień zajmują się rozpatrywaniem skarg lub przeprowadzaniem inspekcji. Podczas sesji plenarnych oraz paneli dyskusyjnych poruszane były zagadnienia dotyczące rozpatrywania spraw o charakterze transgranicznym, ochrony danych osobowych w związku z działalnością portali społecznościowych i innymi usługami świadczonymi drogą elektroniczną, metodologii inspekcji, czy ochrony prywatności w miejscu pracy.

Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2011 roku

Generalny Inspektor Ochrony Danych Osobowych w ramach swoich kompetencji prowadzi szeroko zakrojone działania informacyjno – edukacyjne i patronuje wielu wydarzeniom związanym z idę ochrony danych osobowych i prawem do prywatności. Jest organizatorem i uczestnikiem szeregu konferencji krajowych i międzynarodowych, aktywnie angażuje się w liczne działania upowszechniające wiedzę (wydawanie informacji, publikacji, broszur w zakresie ochrony danych i prywatności), podejmuje działania edukacyjne, a także organizuje bezpłatne szkolenia i warsztaty adresowane głównie do przedstawicieli administracji rządowej i samorządowej oraz przedstawicieli instytucji publicznych, współpracuje ze szkołami wyższymi, jak Uniwersytet Kardynała Stefana Wyszyńskiego, Akademia Leona Koźmińskiego w Warszawie, WSZECHNICA POLSKA Szkoła Wyższa Towarzystwa Wiedzy Powszechnej w Warszawie, Wyższa Szkoła Finansów i Administracji w Gdańsku, Wyższa Szkoła Biznesu National-Louis University w Nowym Sączu, Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Akademia Obrony Narodowej i Uniwersytet Łódzki, a także z Warszawskim Centrum Innowacji Edukacyjno-Społecznych i Szkoleń. W ramach zawartych z tymi podmiotami porozumień podejmowane są różnego rodzaju inicjatywy, jak organizacja studiów podyplomowych, konferencji, debat i seminariów promujących tematykę prywatności i ochrony danych osobowych, a także szkoleń podnoszących poziom wiedzy zawodowej i umiejętności praktyczne. Generalny Inspektor współpracuje również z różnymi organizacjami, jak np. samorządowe ośrodki doskonalenia zawodowego nauczycieli, z którymi prowadzi na zasadzie partnerstwa ogólnopolski program edukacyjny „Twoje dane – twoja sprawa.” Program ten skierowany jest do nauczycieli i uczniów szkół podstawowych i gimnazjalnych, a jego celem jest zwiększenie ich wiedzy na temat ochrony danych osobowych i prawa każdego człowieka do prywatności.

Charakteryzując działalność Generalnego Inspektora Ochrony Danych Osobowych w 2011 r. nie sposób pominąć aktywności organu w obszarze związanym z przewodnictwem Polski w Radzie Unii Europejskiej (tzw. Prezydencja), w okresie od 1 lipca do 31 grudnia 2011 r. Przedstawiciele

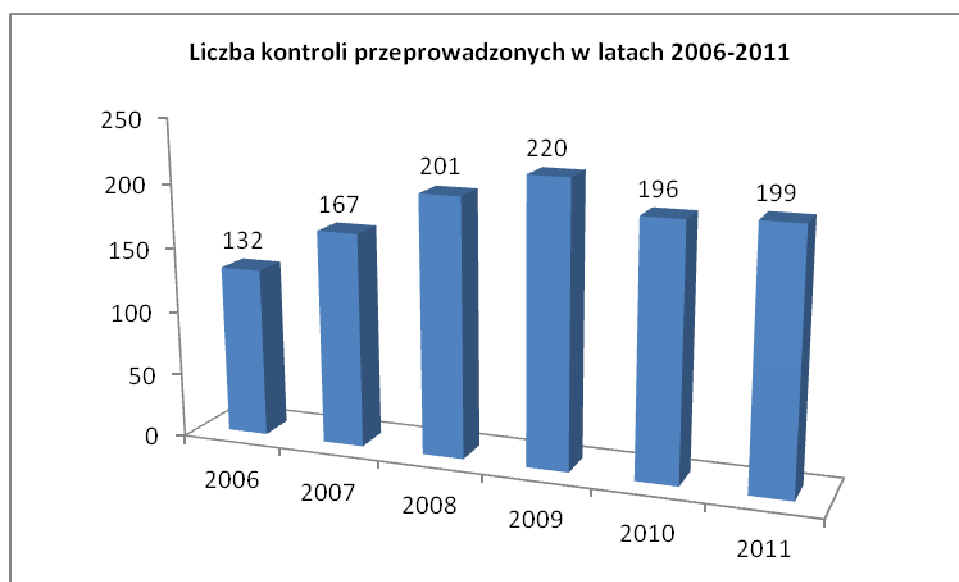
organu ds. ochrony danych osobowych byli członkami Korpusu Prezydencji, którego zadaniem było uczestnictwo w koordynacji prac grup roboczych Rady Unii Europejskiej. Kalendarz Prezydencji polskiej przewidywał aktywny udział Generalnego Inspektora Ochrony Danych Osobowych w spotkaniach na najwyższym szczeblu z przedstawicielami istotnych z punktu widzenia ochrony praw podstawowych resortów i instytucji. Tematyka spotkań odnosiła się do dziedziny szeroko rozumianej problematyki społeczeństwa informacyjnego, a w szczególności poszanowania prawa do życia prywatnego oraz ochrony danych osobowych. W okresie Prezydencji GIODO wzmocnił współpracę z organami administracji rządowej, zwłaszcza z Ministerstwem Spraw Wewnętrznych i Administracji, które było 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, polski organ ds. ochrony danych osobowych aktywnie uczestniczył w posiedzeniach ww. Grupy Roboczej, udzielając polskiej delegacji merytorycznego wsparcia.

Podczas polskiej Prezydencji Generalny Inspektor Ochrony Danych Osobowych był gospodarzem Międzynarodowej Konferencji o Ochronie Danych Osobowych, która odbyła się w Warszawie 21 września 2011 r. Konferencja realizowana była w zakresie projektu współfinansowanego przez Komisję Europejską w ramach programu „Prawa podstawowe i obywatelstwo” („Środki ochrony danych na poziomie europejskim, międzynarodowe wyzwania i kierunki przyszłych usprawnień”), który przewidywał cykl konferencji w ramach Prezydencji węgierskiej (16-17 czerwca 2011 r. odbyła się konferencja w Budapeszcie) i polskiej.

Ponadto Generalny Inspektor Ochrony Danych Osobowych uczestniczył w charakterze gospodarza jednej z sesji oraz prelegenta podczas 6. Europejskiej Konferencji Ministerialnej „Transgraniczne usługi e-administracji dla Europejczyków”, której tematem były przyszłe kierunki rozwoju usług e-administracji w Europie i wyzwania na najbliższe lata. Organizatorem tego wydarzenia, które odbyło się w dniach 17-18 listopada 2011 r. w Poznaniu, było Ministerstwo Spraw Wewnętrznych i Administracji we współpracy z Komisją Europejską. Konferencje nt. e-administracji organizowane są co dwa lata w państwie sprawującym Przewodnictwo w Radzie Unii Europejskiej. Biorą w nich udział przedstawiciele ze świata polityki, nauki, biznesu i administracji. Wspomniana Konferencja była jednym z najważniejszych wydarzeń europejskich w dziedzinie społeczeństwa informacyjnego i jednym z najbardziej prestiżowych spotkań organizowanych podczas polskiej Prezydencji. W sesji pod tytułem „Cloud Computing and Service Oriented Architecture in Public Sector” jednym z panelistów był dr Wojciech R. Wiewiorowski, Generalny Inspektor Ochrony Danych Osobowych, który wygłosił prezentację na temat prawnych aspektów przetwarzania danych w chmurze w ramach administracji publicznej, jak również uczestniczył w dyskusji w sesji „Trust and Privacy”.

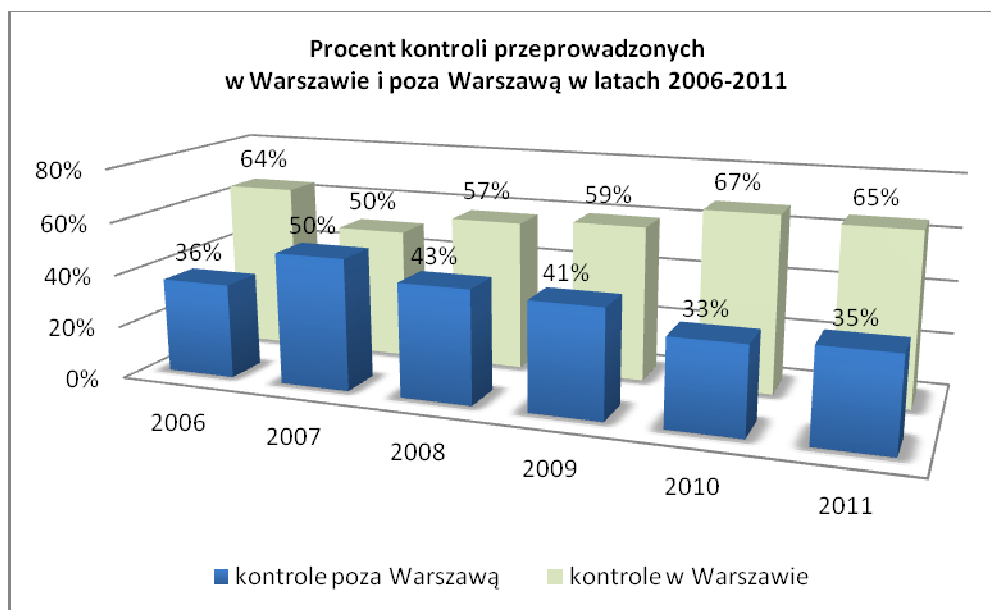
Natomiast charakteryzując działalność Generalnego Inspektora Ochrony Danych Osobowych w obszarze związanym z przeprowadzonymi w 2011 r. **kontrolami** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych należy stwierdzić, że – podobnie jak w latach ubiegłych – znaczna 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 2011 r. przeprowadzonych zostało **199 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W porównaniu z poprzednim rokiem sprawozdawczym, w którym było 196 kontroli, liczba ta nieznacznie wzrosła (zob. *Wykres 41*) i wciąż utrzymuje się na wyrównanym poziomie.



Wykres 41: ***Porównanie liczby kontroli przeprowadzonych w latach 2009–2011.***

W analizowanym 2011 roku na ogólną liczbę 199 kontroli, 129 z nich przeprowadzonych było w Warszawie, zaś 70 poza Warszawą. Wykres 42 przedstawia procentowe zastawienie kontroli przeprowadzonych w 2011 r. przez Generalnego Inspektora Ochrony Danych Osobowych na terenie Warszawy oraz poza nią.



Wykres 42: *Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2009–2011.*

Najwięcej kontroli przeprowadzonych zostało z urzędu (97). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący:

Inicjatywa kontroli	Liczba kontroli
Z urzędu	97
Departament Orzecznictwa, Legislacji i Skarg	61
Departament Rejestracji Zbiorów Danych Osobowych	15
Departament Informatyki	1
Prokuratura	2
Najwyższa Izba Kontroli	2
Komisja Nadzoru Finansowego	1
Ministerstwo Finansów	1
Ministerstwo Infrastruktury	1
W związku z inną kontrolą	18
RAZEM	199

Czynnościom kontrolnym poddane zostały m.in. podmioty świadczące usługi doradztwa podatkowego i finansowego, podmioty zajmujące się organizacją imprez masowych na stadionach, agencje pośrednictwa pracy, dostawcy usług telekomunikacyjnych oraz przedszkola. 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 2011 r. podmioty świadczące usługi doradztwa podatkowego i finansowego (15 kontroli), podmioty zajmujące się organizacją imprez masowych na stadionach (14 kontroli), agencje pośrednictwa pracy (17 kontroli), dostawców usług telekomunikacyjnych (10 kontroli) przedszkola (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 przetwarzania danych osobowych w Krajowym Systemie Informatycznym (KSI) umożliwiającym organom administracji publicznej i organom wymiaru sprawiedliwości wykorzystywanie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym. Spośród tych kontroli najistotniejsza była kontrola związana z uruchomieniem w dniu 11 października 2011 r. przez państwa należące do strefy Schengen Wizowego Systemu Informacyjnego. Ponadto sprawdzano, czy wykorzystywanie przez Szefa Urzędu do Spraw Cudzoziemców danych osobowych, przetwarzanych w Krajowym Systemie Informatycznym, nie narusza praw osoby, której dane dotyczą, a w szczególności, na jakiej podstawie dokonano wpisu tych danych do Systemu Informacyjnego Schengen.

W 2011 r. Generalny Inspektor w związku z przeprowadzonymi kontrolami wydał łącznie **104 decyzje administracyjne**.



Wykres 43: *Porównanie liczby decyzji wydanych w związku z kontrolami przeprowadzonymi w latach 2009–2011.*

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, 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 w szczególności zbierania w szerszym zakresie danych osobowych niż wynika to z przepisów prawa lub w zakresie nieadekwatnym do celu przetwarzania. Stwierdzano bowiem w toku kontroli, iż administratorzy danych – pomimo istnienia przepisów prawa określających w sposób szczegółowy sposób przetwarzania danych osobowych, w tym dopuszczalny zakres zbierania danych osobowych - pozyskiwali od osób, których one dotyczą, dane wykraczające poza katalog danych zawartych w tych przepisach. Zdarzały się przypadki, iż przekroczenie wynikającego z przepisów prawa dozwolonego zakresu przetwarzania danych miało charakter istotnego naruszenia, gdyż było związane z pozyskaniem danych objętych szczególną ochroną na gruncie przepisów o ochronie danych osobowych, tj. danych o karalności. Administratorzy danych cały czas mają także problemy z właściwym dopełnianiem wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 24 i art. 25 ustawy. Kontrole niejednokrotnie wykazywały, że ten obowiązek albo nie był w ogóle realizowany albo też był wykonywany w sposób nieprawidłowy z uwagi na niezawarcie w nim wszystkich informacji wymaganych przez ww. przepisy ustawy lub też na „ukrycie” tych informacji wśród np. postanowień umowy bądź regulaminu, co czyniło je w konsekwencji trudno dostępnymi i mało czytelnymi.

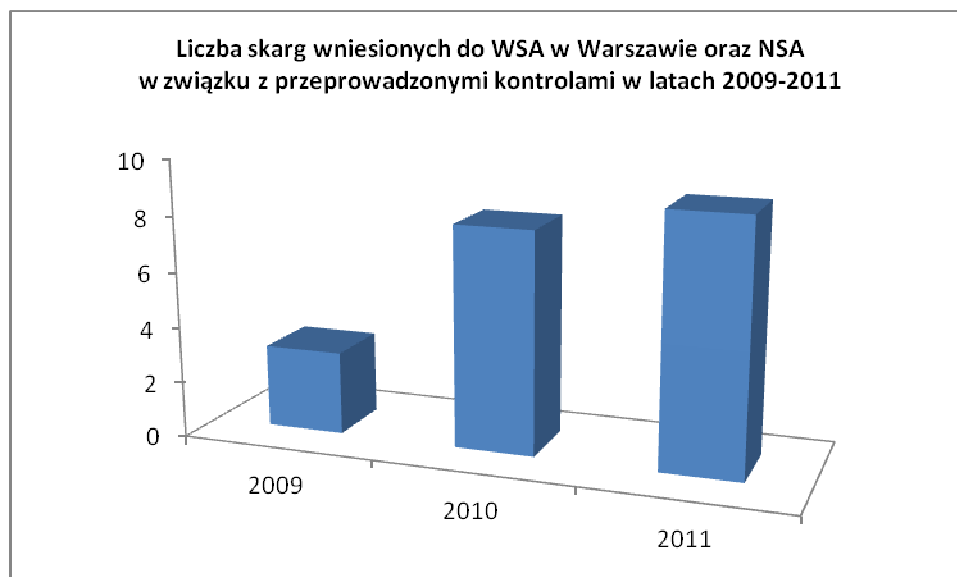
Przeprowadzone kontrole wykazały również, że kontrolowane jednostki nadal mają problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem 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. 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 niniejszym Sprawozdaniu.

Obowiązki określone w przepisach o ochronie danych nie były wykonywane przez jednostki kontrolowane najczęściej z powodu błędnej interpretacji tych przepisów oraz ich niekonsekwentnego stosowania. Często 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 2011 r. kontroli były podmioty, dla których ochrona przetwarzanych danych osobowych była ważnym zagadnieniem. Stosowane przez nie zasady przetwarzania danych osobowych odpowiadały wymogom wynikającym z przepisów o ochronie danych osobowych.

Na podkreślenie zasługuje fakt, że w wielu przypadkach działania inspektorów przeprowadzających kontrolę powodowały, że stwierdzone w trakcie kontroli uchybienia były usuwane przez jednostki kontrolowane w toku postępowania administracyjnego, a nawet jeszcze przed jego wszczęciem. 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. Podkreślić w tym miejscu także należy, że wydawane przez sądy administracyjne orzeczenia niejednokrotnie potwierdzały stanowisko Generalnego Inspektora Ochrony Danych Osobowych zaprezentowane w decyzjach administracyjnych wydanych na skutek przeprowadzonych kontroli.

W roku 2011 do Wojewódzkiego Sądu Administracyjnego oraz Naczelnego Sądu Administracyjnego skierowanych zostało **9 skarg** w związku z przeprowadzonymi kontrolami, w których zapadło **7 orzeczeń** dotyczących decyzji wydanych na skutek przeprowadzonych kontroli.



Wykres 44: Zestawienie porównawcze liczby skarg wniesionych do Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Naczelnego Sądu Administracyjnego w związku z przeprowadzonymi kontrolami w latach 2009-2011.

W jednej z takich spraw Wojewódzki Sąd Administracyjny w Warszawie wyrokiem z dnia 2 czerwca 2011 r.⁴⁵⁵, oddalił skargę przedsiębiorcy prowadzącego serwis internetowy, umożliwiający dostęp do danych pozyskanych z Krajowego Rejestru Sądowego (KRS), na decyzję Generalnego Inspektora Ochrony Danych Osobowych nakazującą, m.in. dopełnienie wobec osób, których dane pochodziły ze źródeł powszechnie dostępnych i zostały zebrane i utrwalone przez ww. przedsiębiorę jako administratora danych, obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych. W uzasadnieniu ww. wyroku, Wojewódzki Sąd Administracyjny w Warszawie jako błędny uznał pogląd skarżącego, iż podstawa prawna zaniechania przez niego obowiązku informacyjnego określonego we wskazanym przepisie istnieje w art. 25 ust. 2 pkt 1 ustawy o ochronie danych osobowych⁴⁵⁶ w związku z art. 8 ust. 1 i ust. 2 ustawy z dnia 27 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2007 r. Nr 168, poz.1186 z późn. zm.), zgodnie z którym Krajowy Rejestr Sądowy (KRS) jest jawny i każdy ma prawo dostępu do danych zawartych w tym rejestrze za pośrednictwem Centralnej Informacji. Sąd wskazał, że art. 8 ust. 1 i ust. 2 ustawy o Krajowym Rejestrze Sądowym statuuje zasadę jawności danych zawartych w rejestrze. Jednocześnie ww. ustawa reguluje w sposób całkowity zasady udostępnienia danych osobowych osób, których dane umieszczone są w KRS. Dane te są udostępniane każdemu zainteresowanemu, dla jego potrzeb związanych z pewnością obrotu gospodarczego, a osoba, która podejmuje działalność, która ma być wpisana do KRS wie, że jej dane są w prowadzonym przez Państwo rejestrze i tylko na podstawie

⁴⁵⁵ Sygn. akt II SA/Wa 720/11

⁴⁵⁶ Art. 25 ust. 2 pkt 1 ustawy o ochronie danych osobowych. Przepisu ust. 1 nie stosuje się, jeżeli: przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą.

przepisów dotyczących funkcjonowania tego rejestru te dane będą wykorzystane. Sąd podniósł, że skarżący pobiera dane osobowe osób znajdujących się w KRS, takie jak imię, nazwisko, numer PESEL do własnej bazy danych. Dane z KRS nie mają służyć do takiego celu, a osoby które udostępniają swoje dane osobowe nie wyrażają zgody na to, aby ich dane osobowe były umieszczane w innej, prywatnej bazie danych. Od wyroku Wojewódzkiego Sądu Administracyjnego administrator danych złożył w sierpniu 2011 r. skargę kasacyjną do Naczelnego Sądu Administracyjnego.

Natomiast w sprawie, która toczyła się przed Naczelnym Sądem Administracyjnym utrzymane zostało stanowisko Generalnego Inspektora Ochrony Danych Osobowych wyrażone w decyzji skierowanej do naczelnika urzędu skargowego⁴⁵⁷. W decyzji tej nakazano m.in. usunięcie i zaprzestanie zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników, przetwarzanych w celu ewidencji czasu pracy. W uzasadnieniu wyroku NSA wyraził pogląd, iż wyrażona na życzenie pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych w ww. celu i zakresie narusza prawa pracownika i swobodę wyrażania przez niego woli, ze względu na zależność pracownika od pracodawcy (z tego względu ustawodawca ograniczył przepisem art. 22¹ Kodeksu pracy), a także prowadzi do zakwestionowania zasady adekwatności wyrażonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych⁴⁵⁸. Ponadto podkreślił, że regulamin pracy nie może być sprzeczny z powszechnie obowiązującymi uregulowaniami prawa. Regulamin, jako wewnętrzny akt wydany przez kierownictwo danej jednostki, nie może być traktowany jako źródło prawa upoważniające do podjęcia działań w zakresie pobierania i przetwarzania danych osobowych obejmujących dane biometryczne.

W podsumowaniu, na podstawie ustaleń z kontroli przeprowadzonych w 2011 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 2011 r. był brak współpracy

⁴⁵⁷ Sygn. akt I OSK 1476/10

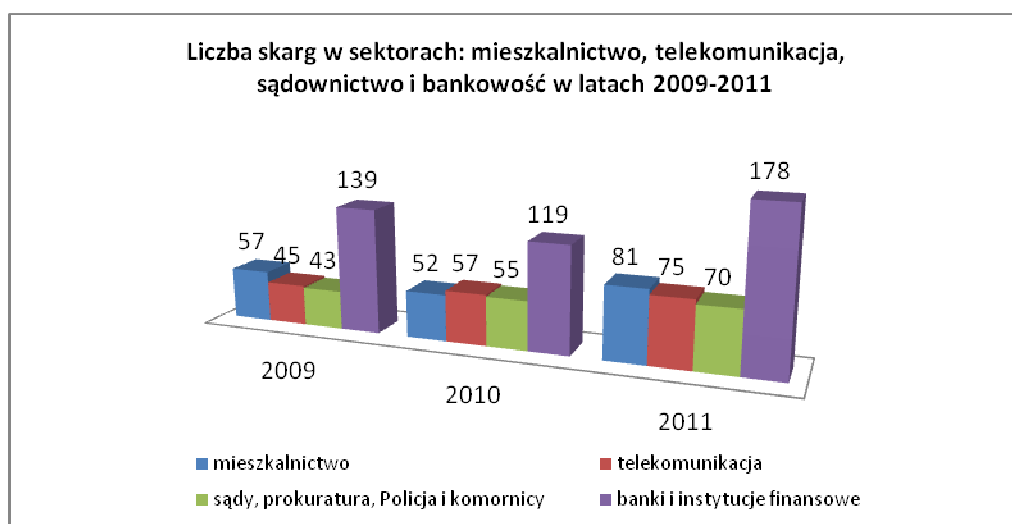
⁴⁵⁸ Art. 26 ust. 1 pkt 3. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

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 w związku z nowelizacją ustawy o ochronie danych osobowych, która wprowadziła sankcje karne za udaremnianie lub utrudnianie inspektorowi wykonania czynności kontrolnej⁴⁵⁹.

W porównaniu z poprzednimi latami, w 2011 r. daje się zauważyć systematyczny wzrost liczby **skarg**, które wpłynęły do Biura GODO. W roku 2008 wpłynęło 986 skarg, w 2009 – 1049, w 2010 – 1114, zaś w 2011 - 1271. Należy podkreślić, że przyczyn wzrostu liczby skarg, które wpłynęły do GODO w analizowanym okresie 2011 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.

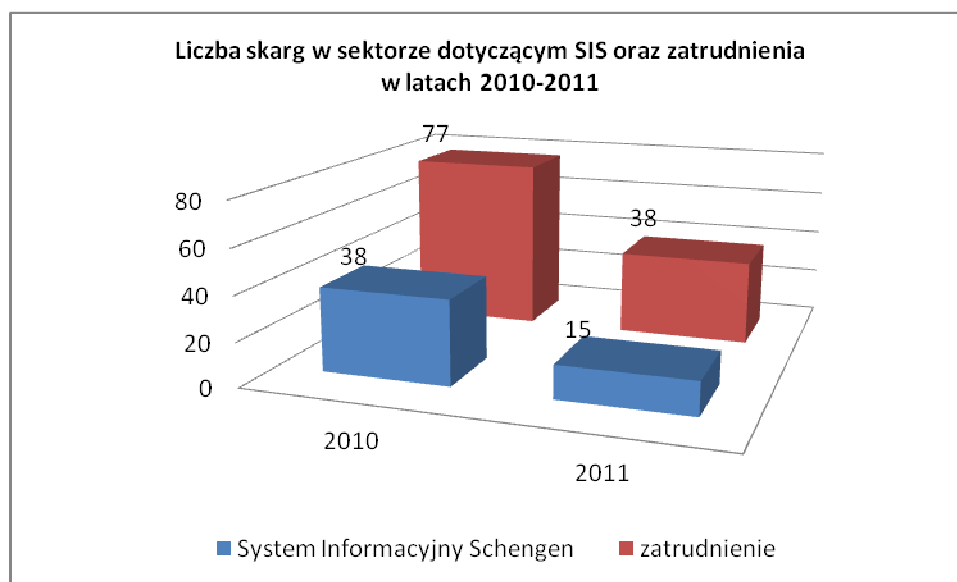
Porównanie liczby skarg w poszczególnych sektorach na przestrzeni lat 2009-2011 pozwala zauważyć charakterystyczne trendy. Pierwszym z nich był znaczący wzrost liczby skarg w sektorze dotyczącym mieszkalnictwa (2009 r. - 57, 2010 r. - 52, 2011 r. - 81), telekomunikacji (2009 r. - 45, 2010 r. - 57, 2011 r. - 75), w sektorze odnoszącym się do działalności sądów, prokuratur, Policji i komorników (2009 r. - 43, 2010 r. - 55, 2011 r. - 70) oraz w sektorze dotyczącym działalności banków i innych instytucji finansowych (2009 r. – 139, 2010 r. - 119, 2011 r. - 178). W tym miejscu należy podkreślić, że w okresie 2008 – 2010 r. 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. oznaczało to spadek liczby skarg o 66 %. Natomiast w analizowanym 2011 r. liczba skarg na podmioty sektora bankowości jest porównywalna z rokiem 2008.

⁴⁵⁹ Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.



Wykres 45: Porównanie liczby skarg w sektorach: mieszkalnictwo, telekomunikacja, sądownictwo i bankowość w latach 2009–2011 – trend wzrostowy.

Należy także wskazać dwie tendencje malejące. O ile w 2010 r. skarg dotyczących Systemu Informacyjnego Schengen wpłynęło 38, to w 2011 r. było ich 15. Spadek liczby skarg dotyczy także sektora zatrudnienia. Dla porównania, w roku 2010 r. wpłynęło 77 skarg, zaś w analizowanym 2011 r. zaledwie 38.



Wykres 46: Porównanie liczby skarg w sektorze dotyczącym Systemu Informacyjnego Schengen oraz zatrudnienia w latach 2010-2011 – trend malejący.

Jak już o tym wspomniano w innej części Sprawozdania⁴⁶⁰, w sprawach zainicjowanych skargami na uwagę zasługują rozstrzygnięcia sądów administracyjnych dotyczące **przetwarzania**

⁴⁶⁰ zob. s. 59 niniejszego Sprawozdania.

danych osobowych skarżących w Krajowym Systemie Informacji Policji⁴⁶¹. W decyzjach wydanych w 2011 roku z tego zakresu⁴⁶², Generalny Inspektor nakazywał Komendantowi Policji usunięcie danych osobowych skarżących z Krajowego Systemu Informacji Policji.

Komendant Policji we wnioskach o ponowne rozpatrzenie sprawy oraz w skargach skierowanych do Wojewódzkiego Sądu Administracyjnego w Warszawie wskazywał m.in. że ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 43, poz. 277) stanowi *lex specialis* w stosunku do ustawy o ochronie danych osobowych. Sąd, dokonując oceny legalności zaskarżonej decyzji w wyroku z dnia 24 października 2011 r.⁴⁶³ podzielił ocenę GODO, iż zastosowanie powinna znaleźć ustawa o ochronie danych osobowych. Ponadto WSA w Warszawie w uzasadnieniu do wyroku oddalającego skargę Komendanta Policji wskazał, że cyt.: „(...) przy takiej treści i konstrukcji przepisów pragmatycznych w przedmiocie usuwania danych osobowych nie można w żaden sposób zgodzić się z twierdzeniem, że ustawa o Policji i rozporządzenie wykonawcze stanowią *lex specialis* w stosunku do ustawy o ochronie danych osobowych (...)”. Jednak orzecznictwo w tym zakresie nie jest jednolite. Jako przykład można wskazać wyroki Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 10 marca 2011 r.⁴⁶⁴ oraz z dnia 28 listopada 2011 r.⁴⁶⁵ W uzasadnieniu do ww. wyroków WSA w Warszawie wskazał, że cyt.: „(...) zdaniem Sądu przetwarzania danych osobowych osób wymienionych w art. 2a ustawy o Policji, zostały przez ustawodawcę uregulowane kompleksowo i stanowią *lex specialis* w stosunku do ustawy o ochronie danych osobowych. Słuszne jest stanowisko Generalnego Inspektora Ochrony Danych Osobowych, że prawodawca nie określił konkretnych kryteriów pozwalających na dokonanie oceny przydatności danych osobowych znajdujących się w KSIP, lecz posłużył się kryteriami ogólnymi. Co wskazuje, iż ocenę przydatności danych w zbiorze informatycznym pozostawił organom Policji, albowiem to one stoją na straży porządku publicznego i znają specyfikę środowisk przestępczych (...)”⁴⁶⁶.

W innej z kolei sprawie, dotyczącej wniosków skarżących o udostępnienie na ich rzecz **danych osobowych innych podmiotów w celu dochodzenia swych praw przed sądem**, Wojewódzki Sąd Administracyjny w Warszawie w uzasadnieniu do wyroku z dnia 7 października 2011 r.⁴⁶⁷, podkreślił, że cyt.: „(...) do wiarygodnego uzasadnienia potrzeby posiadania danych osobowych abonenta o przyznanej IP (...) nie wystarczy sam hipotetyczny zamiar wytoczenia przeciwko niemu powództwa cywilnego (...)”. Podobnie w tej kwestii wypowiedział się Naczelny Sąd Administracyjny

⁴⁶¹ zob. DOLiS-440-698/11, DOLiS-440-699/11, DOLiS-440-963/11, DOLiS-440-1213/11.

⁴⁶² zob. DOLiS/DEC-188/11/10381,10385 dot. DOLiS-440-712/10.

⁴⁶³ Wyrok WSA w Warszawie z dnia 24 października 2011 r. sygn. akt II SA/Wa 625/11.

⁴⁶⁴ Wyrok WSA w Warszawie z dnia 10 marca 2011 r. sygn. akt II SA/Wa 1885/10.

⁴⁶⁵ Wyrok WSA w Warszawie z dnia 28 listopada 2011 r. sygn. akt II SA/Wa 978/11.

⁴⁶⁶ Wyrok WSA w Warszawie z dnia 28 listopada 2011 r. sygn. akt II SA/Wa 978/11.

⁴⁶⁷ Wyrok WSA w Warszawie z dnia 7 października 2011 r. sygn. akt II SA/Wa 364/11.

w uzasadnieniu do wyroku z dnia 22 marca 2011 r.⁴⁶⁸. Z jednej strony NSA w ww. wyroku wskazał, że cyt.: (...) osoba, która czuje się pokrzywdzona publikacją materiału prasowego ma niewątpliwie prawo dochodzenia przysługującej jej z tego tytułu roszczeń. (...) Niewskazanie przez powoda miejsca zamieszkania pozwanego wprawdzie nie wyklucza dopuszczalności złożenia pozwu, ale uniemożliwia nadanie mu prawidłowego biegu, a tym samym może skutkować podjęciem przez przewodniczącego czynności przewidzianych w art. 130 § 2 K.p.c. W toku zaś wszczętego procesu przedmiotowy brak może stanowić przesłankę zawieszenia postępowania na podstawie art. 177 § 1 pkt 6 K.p.c. (...). Z drugiej strony jednak, NSA wskazał, że cyt.: „(...) uzasadniona potrzeba posiadania danych adresowych (...) – w znaczeniu przewidzianym w art. 29 ust. 2 ustawy - mogła zachodzić, ale dopiero po wszczęciu przez poszkodowanego procesu (...). Odmienna sytuacja ma miejsce wówczas, gdy (...) nie toczy się żadne postępowanie sądowe. Dlatego sama deklaracja dotycząca zainicjowania w przyszłości procesu omawianej przesłanki nie spełnia. Taki hipotetyczny zamiar nie musi być w ogóle zrealizowany (...)”.

Na uwagę zasługuje także wyrok NSA z dnia 6 grudnia 2011 r.⁴⁶⁹ jaki zapadł w sprawie, w której skarżący, działając jako pełnomocnik strony w postępowaniu przed Naczelnikiem Urzędu Skarbowego, zakwestionował **legalność pozyskania jego danych osobowych przez organ podatkowy**, w postaci adresów miejsca zamieszkania, co miało miejsce przy doręczeniu decyzji ustalającej zobowiązanie podatkowe dla reprezentowanej przez niego strony. Naczelny Sąd Administracyjny stwierdził, że decyzja Generalnego Inspektora odmawiająca uwzględnienia wniosku była zgodna z prawem. W uzasadnieniu do ww. wyroku NSA wskazał, że cyt.: „(...) w toku ogólnego postępowania administracyjnego osoba, której dane dotyczą, nie jest uprawniona do żądania zaprzestania przetwarzania swoich danych osobowych w toku postępowania administracyjnego. (...) Odnosi się to wprost do postępowania administracyjnego uregulowanego ustawą z dnia 29 września 1997 r. Ordynacja podatkowa. Zasadnie Generalny Inspektor w zaskarżonej decyzji przyjął, iż organ podatkowy, w myśl regulacji prawnych zawartych w przytoczonych i szczegółowo omówionych przepisach Ordynacji podatkowej, uprawniony jest do przetwarzania danych osobowych skarżącego, a proces przetwarzania jest dopuszczalny na podstawie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. (...) zważywszy na to, iż pozyskane dane osobowe stanowiły część postępowania administracyjnego, a żądanie ich usunięcia zgłoszono w trakcie trwania tego postępowania, wyłączona była ingerencja w trybie kontroli i wydania nakazów Generalnego Inspektora. (...) Zasadnie Generalny Inspektor rozstrzygnął pozorną kolizję kompetencji organów przyjmując, iż nie jest uprawniony do dokonywania kontroli, a następnie wkraczania swoimi nakazami w materiał dowodowy zawarty w aktach sprawy administracyjnej (...)”.

⁴⁶⁸ Wyrok NSA z dnia 22 marca 2011 r. sygn. akt I OSK 623/10.

⁴⁶⁹ Wyrok NSA z dnia 6 grudnia 2011 r. sygn. akt I OSK 268/11.

Warto wskazać, że sporną kwestią stanowił również **status Zastępcy Generalnego Inspektora Ochrony Danych Osobowych** postrzegany przez pryzmat wydania obu decyzji w danym postępowaniu przez Zastępcę. Orzecznictwo w tym zakresie nie jest jednolite. W uzasadnieniu do wyroku NSA z dnia 13 grudnia 2011 r.⁴⁷⁰, sąd wskazał, że cyt.: „(...) przepisy tej ustawy [ustawy o ochronie danych osobowych] wprowadzają rozróżnienie pozycji ustrojowej Zastępcy Generalnego Inspektora (...) od aparatu pomocniczego - Biura Generalnego Inspektora (...). Generalny Inspektor (...) określa zakres działań Zastępcy. Nie jest to zatem upoważnienie do działania pracownika aparatu pomocniczego. Zastępca Generalnego Inspektora (...) ma ustrojowo wyodrębnioną pozycję realizując określony przez Generalnego Inspektora (...) zakres zadań. Oznacza to, że pozycja ustrojowa Zastępcy Generalnego Inspektora (...) nie może być zrównana z pozycją pracownika, który działa wyłącznie w zakresie upoważnienia, a nie przypisanych zadań (...)”. Natomiast w uzasadnieniu do wyroku z dnia 16 grudnia 2011 r.⁴⁷¹ NSA wskazał, że cyt.: „(...) okoliczność bowiem, że przedmiotowemu postępowaniu (przed GODO) nie można przypisać cechy dewolutywności nie wyłącza po stronie organu obowiązku zagwarantowania wnioskodawcy rozpatrzenia sprawy z zachowaniem standardów rzetelności, bezstronności i obiektywizmu. (...) Należy przyjąć, że działania podmiotu upoważnionego należy traktować jako działania samego organu, to jednak istotne w tym przypadku znaczenie ma okoliczność, że kwestionowana decyzja w sprawie nie została wydana przez organ, lecz jego pracownika (...)”.

W tym miejscu warto również przytoczyć jeszcze przykłady innych rozstrzygnięć, jakie zapadły przed WSA w Warszawie na skutek wniesionych skarg. Dotyczyły one **spraw z zakresu przetwarzania danych osobowych osób należących do związków wyznaniowych**. Skarżący podnosili, iż pomimo złożenia oświadczenia o wystąpieniu z Kościoła Katolickiego, związek wyznaniowy w dalszym ciągu przetwarza ich dane osobowe. Generalny Inspektor Ochrony Danych Osobowych zwracał się w poszczególnych sprawach o wyjaśnienia do odpowiednich podmiotów przetwarzających dane członków lub byłych członków Kościoła Katolickiego. Organ ochrony danych osobowych umarzał postępowania administracyjne w takich sprawach wskazując na brak swojej kognicji do wydania merytorycznej decyzji administracyjnej w tym względzie, wskazany w art. 43 ust. 2 ustawy o ochronie danych osobowych.⁴⁷² Wiele z tych rozstrzygnięć zostało poddanych kontroli sądowej wskutek ich zaskarżenia do Wojewódzkiego Sądu Administracyjnego w Warszawie. W jednej z takich spraw, WSA w Warszawie w uzasadnieniu do wyroku z dnia 21 lutego 2012 r.⁴⁷³ wskazał, że cyt.: „(...) należy uznać za prawidłowe działania podjęte przez organ, który ograniczył swoją aktywność do czynności na jakie pozwala mu ustawa - czyli czynności wyjaśniających (...). Organ nie

⁴⁷⁰ Wyrok NSA z dnia 13 grudnia 2011 r. sygn. akt I OSK 834/11.

⁴⁷¹ Wyrok NSA z dnia 16 grudnia 2011 r. sygn. akt I OSK 632/11.

⁴⁷² DOLiS/DEC-21/11/1560,1570 dot. DOLiS-440-845/10, DOLiS/DEC- 33/11/2429,2430 dot. DOLiS-440-588/10, DOLiS/DEC- 44/11/3079,3082 dot. DOLiS-440-771/10, DOLiS/DEC- 45/11/3167,3170 dot. DOLiS-440-810/10, DOLiS/DEC- 91/11/5808,5812 dot. DOLiS-440- 954/10, DOLiS/DEC- 413/11/24660,24662 dot. DOLiS-440- 313/11.

⁴⁷³ Wyrok WSA w Warszawie z dnia 21 lutego 2012 r. sygn. akt 2350/11.

niał natomiast uprawnień do przeprowadzenia czynności kontrolnych w pomieszczeniach Parafii oraz dokonania wglądu do dokumentacji parafialnej. Nie mógł też wydać rozstrzygnięcia merytorycznego w formie decyzji administracyjnej w kwestii przetwarzania przez Parafię danych osobowych skarżącego (...). Ponadto sąd w ww. wyroku podkreślił, że cyt.: „(...) bez wpływu na wskazane wyżej wyłączenie kompetencji Generalnego Inspektora Ochrony Danych Osobowych pozostaje okoliczność, że skarżący w sposób skuteczny wystąpił z Kościoła Katolickiego. (...) Badanie w niniejszym postępowaniu kwestii wystąpienia skarżącego z Kościoła Katolickiego nie ma znaczenia w sprawie (...)”.

W 2011 r. przełomowe z punktu widzenia przetwarzania danych osobowych w sektorze obejmującym działalność w Internecie, było stwierdzenie Naczelnego Sądu Administracyjnego zawarte w uzasadnieniu do wyroku z dnia 19 maja 2011 r.⁴⁷⁴, że cyt.: „(...) Internet często pozornie, a czasami faktycznie zapewnia anonimowość jego użytkownikom. Stanowi medialne forum, na którym prezentowane są treści naruszające ludzką godność, cześć i dobre imię. Dlatego też wszędzie tam gdzie numer IP pozwala pośrednio na identyfikację konkretnej osoby fizycznej powinien on być uznany za dane osobowe w rozumieniu art. 6 ust. 1 i 2 ustawy o ochronie danych osobowych. Odmienne interpretacja byłaby sprzeczna z normami konstytucyjnymi zawartymi w art. 30 i 47 Konstytucji RP (...)”. Skład sędziowski w ww. wyroku jako pierwszy jednoznacznie stwierdził, że adres IP (Internet Protocol Address) jest daną osobową.

W podsumowaniu należy zauważyć, że ogólna liczba skarg związanych z przetwarzaniem danych osobowych sukcesywnie wzrasta. Przyczyną powyższego jest nie tylko naruszanie ustawy o ochronie danych osobowych przez administratorów danych, czy też brak znajomości jej przepisów przez obywateli, ale także wzrost świadomości prawnej podmiotów uczestniczących w procesie przetwarzania danych, z którym nierozzerwalnie wiąże się intensyfikacja potrzeb związanych z ochroną danych i konieczność wyjaśniania przez GODO coraz większej liczby wątpliwości. Systematycznie jednak poprawia się poziom przetwarzania danych osobowych przez administratorów danych, którzy – jak wynika z podejmowanych przez nich działań – współdziałają z organem ochrony danych osobowych w celu wypracowywania lepszych standardów ochrony danych. W wielu sprawach, po interwencji Generalnego Inspektora, podejmowali oni odpowiednie działania zmierzające do zmian kwestionowanych przez organ praktyk.

Ponadto należy wskazać, że poziom świadomości prawnej tak podmiotów przetwarzających dane, jak i osób fizycznych, których dane dotyczą z roku na rok się zwiększa. Najłatwiej można to zaobserwować w przypadku dużych podmiotów gospodarczych, które traktują politykę bezpieczeństwa danych swoich klientów jako jeden z ważniejszych elementów ich pozytywnego wizerunku. Odnosząc się do drobnych przedsiębiorców czy podmiotów pożytku publicznego można zauważyć, że często nie

⁴⁷⁴ Wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011 r. sygn. akt I OSK 1079/10.

są świadomi faktu, że są administratorami danych osobowych i że spoczywają na nich konkretne obowiązki określone przez przepisy prawa.

Analizując z kolei działalność **opiniotwórczą** Generalnego Inspektora Ochrony Danych Osobowych w 2011 r., można było dostrzec szczególne zaniepokojenie organu tendencją do tworzenia przez różne podmioty tzw. megabaz danych osobowych. W przesyłanych do zaopiniowania Generalnemu Inspektorowi projektach zaobserwować można było duże znaczenie przypisywane tym z nich, które dotyczyły baz teleinformatycznych. Projektodawcy wychodzili bowiem naprzeciw rozwojowi technologii i tendencji do tworzenia centralnych baz, zasilanych niejednokrotnie danymi z baz o mniejszym zasięgu. Podstawowej przyczyny zainteresowania regulacjami prawnymi przetwarzania danych osobowych upatrywać należy w postępującym z coraz większą dynamiką procesie wprowadzania nowoczesnych, skomputeryzowanych systemów zapisywania, przetwarzania i udostępniania danych osobowych. Przy tak zorganizowanych i funkcjonujących bazach danych osobowych niepomiarowo wzrasta ryzyko naruszenia słuszných interesów osób, na temat których gromadzone są różnorodnego rodzaju informacje. Wiąże się to m.in. z możliwością koncentracji, a także kojarzenia danych – prowadzącego do profilowania osób – znajdujących się w rozmaitych, rozproszonych, rozbudowanych i przewidzianych dla odmiennych celów zbiorach. Skomputeryzowane bazy danych o osobach były więc przedmiotem szczególnej uwagi Generalnego Inspektora Ochrony Danych Osobowych. Istnienie takich baz danych może bowiem sprzyjać niedozwolonemu ingerowaniu w szeroko pojętą wolność osobistą jednostki i jej prywatność, pozbawiając jej możliwości swobodnego dysponowania informacją na swój temat. Generalny Inspektor Ochrony Danych Osobowych wykazywał wzmożone zainteresowanie wszelkimi projektami regulującymi funkcjonowanie takich baz: nowego systemu informacji oświatowej (SIO) – systemu teleinformatycznego obsługującego scentralizowany zbiór danych zawierający spersonalizowane informacje dotyczące ponad 5 milionów uczniów, około 900 tysięcy przedszkolaków, 600 tysięcy słuchaczy i ponad 600 tysięcy nauczycieli; systemu informacji w ochronie zdrowia obejmującego bazy danych tworzone przez podmioty zobowiązane do ich prowadzenia, zawierające dane o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej, usługodawcach i pracownikach medycznych oraz usługobiorcach; zintegrowanego systemu informacji o nieruchomościach (ZSIN), który komunikuje się z innymi rejestrami publicznymi⁴⁷⁵, w tym wymianę danych między tymi rejestrami oraz zawiadomień o zmianach danych z tych rejestrów; Centralnego Rejestru Podmiotów – Krajowej Ewidencji Podatników (CRP KEP), dla którego projektodawca przewidział automatyczne zapisywanie imienia,

⁴⁷⁵ zob. art. 24b ust. 1 pkt 3 ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (Dz. U. z 2010 r. Nr 193, poz. 1287 z późn. zm.), tj. księga wieczysta, państwowy rejestr granic i powierzchni jednostek podziałów terytorialnych kraju, krajowy rejestr urzędowy podziału terytorialnego kraju, krajowy rejestr urzędowy podmiotów gospodarki narodowej, krajowy system ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności.

nazwiska i numeru PESEL każdej osoby posiadającej ten numer, co narusza zasadę **adekwatności danych w stosunku do celów**, a także **zakaz zbierania danych na zapas**.

Co więcej, Generalny Inspektor Ochrony Danych Osobowych niejednokrotnie wskazywał też, że w procesie tworzenia prawa brakowało **dyskusji publicznej co do oczekiwań społecznych nad kwestiami poruszanymi w projektach**. Tak było w przypadku trwających prawie 2 lata prac Ministerstwa Edukacji Narodowej nad przygotowaniem wspomnianego Systemu Informacji Oświatowej (SIO). Zabrakło tu szerokiej dyskusji publicznej, co do oczekiwań od Systemu oraz wymagań, jakie powinny zostać mu postawione, co mogłoby przełożyć się na bardziej efektywny przebieg prac nad tym projektem.

GIODO 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”.⁴⁷⁶ 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.

Projektowanie megazbiorów zawierających dane osobowe zawsze było, jest i będzie przedmiotem wyjątkowej uwagi i zainteresowania organu ds. ochrony danych osobowych. Dostęp do takich zbiorów 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.

⁴⁷⁶ Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. w sprawie o sygn. K. 32/2004.

W przesyłanych Generalnemu Inspektorowi do zaopiniowania projektach często pojawiał się również błąd polegający na **braku dookreślenia zakresu przetwarzanych danych osobowych**. Projektodawcy często wychodzili z założenia, że wprowadzając sformułowanie takie, jak np. „dane wskazujące wnioskodawcę”, „dane osobowe, w tym (...)”; „dane osobowe, w szczególności”⁴⁷⁷ będzie to wystarczające dla uznania prawidłowości jego brzmienia z punktu widzenia ochrony danych osobowych. Generalny Inspektor w takich sytuacjach podkreślał, iż każdorazowo przepis prawa odnoszący się do przetwarzania danych osobowych powinien wprost wskazywać zakres informacji, jakie na jego podstawie mają być przetwarzane. W przeciwnym razie zachodzi ryzyko przedkładania przez osoby, których dane dotyczą lub żądania przez administratorów danych, informacji w zakresie szerszym niż wynikający z przepisu prawa, niedookreślonym, jak również nieadekwatnym do rzeczywistego celu przetwarzania danych i tym samym do naruszenia jednej z naczelných zasad wynikających z przepisów o ich ochronie, a mianowicie zasady adekwatności danych w stosunku do celów ich przetwarzania⁴⁷⁸.

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 GODO 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 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

⁴⁷⁷ np. § 7 projektu rozporządzenia Ministra Finansów w sprawie sposobu archiwizacji danych oraz zakresu danych związanych z urządzaniem zakładów wzajemnych przez sieć Internet podlegających archiwizacji (wydanego na podstawie delegacji zawartej w art. 15 d ust. 8 ustawy z dnia 19 listopada 2009 r. o grach hazardowych – Dz. U. Nr 201, poz. 1540 z późn. zm.).

⁴⁷⁸ Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

18 lipca 2002 r. o świadczeniu usług drogą elektroniczną⁴⁷⁹ powinna być pozyskiwana mocą odrębnego oświadczenia woli). Niezadowalająca 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.

W tym miejsce należy podkreślić, że rola organu ds. ochrony danych osobowych w procesie legislacyjnym jest znacząco ograniczona. O ile bowiem – zgodnie z art. 12 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Generalny Inspektor jest uprawniony do opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych, o tyle nie jest on władny zablokować prac nad projektem nawet w sytuacji stwierdzenia rażącego naruszenia przepisów o ochronie danych osobowych. Wyłączna kompetencja w tym zakresie przysługuje posłom na Sejm Rzeczypospolitej Polskiej.

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.

Jak już była o tym mowa, po prawie trzech latach intensywnych prac parlamentarnych ustawa o ochronie danych osobowych została w dniu 7 marca 2011 r. **znowelizowana** ustawą z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw⁴⁸⁰.

W znowelizowanej ustawie zasadniczy wpływ na zwiększenie poziomu ochrony danych mają – zawarte w art. 2 ustawy o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw - modyfikacje art. 2 § 1 oraz art. 20 § 2 ustawy z dnia 17 czerwca 1966 roku o postępowaniu egzekucyjnym w administracji⁴⁸¹, które zdecydowanie zwiększają skuteczności działań GODO. W ustawie o postępowaniu egzekucyjnym w administracji dodano do obowiązków, które podlegają egzekucji administracyjnej, obowiązki z zakresu ochrony danych osobowych, nałożone w drodze decyzji Generalnego Inspektora Ochrony Danych Osobowych. Natomiast GODO został uznany za organ egzekucyjny w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym. Powyższe zmiany przyczyniły się znacznie do wzmocnienia pozycji GODO, który jako organ egzekucyjny w zakresie obowiązków o charakterze niepieniężnym wynikających z decyzji

⁴⁷⁹ Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.

⁴⁸⁰ Dz. U. Nr 229, poz. 1497

⁴⁸¹ Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.

administracyjnych wydanych w sprawach wykonania przepisów o ochronie danych osobowych będzie mógł, w przypadku niewykonania takiej decyzji administracyjnej przez zobowiązanego, zastosować środek egzekucyjny.

Nowe regulacje umożliwiają 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.

Ponadto z ustawy o ochronie danych osobowych wykreślony został art. 29 oraz art. 30 regulujący udostępnianie przez administratora danych posiadanych danych osobowych w celach innych, niż włączenie do zbioru (na mocy art. 1 pkt 7 ustawy nowelizującej). W związku z powyższym w sprawach, które wpłynęły do Biura GODO po 7 marca 2011 r. w zakresie udostępnienia danych osobowych, GODO wydaje decyzje na podstawie art. 23 ust. 1 ustawy o ochronie danych osobowych⁴⁸².

Charakter porządkujący ma również zmiana art. 33 ustawy, który określa obowiązek administratora danych do informowania danej osoby o prawach, które przysługują jej w zakresie ochrony danych osobowych oraz informacji o zebranych danych. Ponadto administrator danych ma obowiązek odmówić udzielenia powyższych informacji, jeżeli mogłoby to spowodować ujawnienie wiadomości zawierających informacje niejawne, zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, czy też istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób. Stanowi o tym znnowelizowany art. 34 ustawy.

Ponadto nadano nowe brzmienie art. 7 pkt 5 ustawy o ochronie danych osobowych, który obecnie jednoznacznie przesądza, sporną niegdyś w doktrynie, kwestię dopuszczalności odwołania zgody na przetwarzanie danych osobowych przewidując, iż zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie. Ustawodawca niejako potwierdził to, co doktryna nauki prawa uważała za słuszne w tej kwestii.

⁴⁸² DOLiS/DEC-817/11/44928,44930,44932 dot. DOLiS-440-250/11.

Podkreślenia wymaga, że przedmiotowy projekt ustawy - obok upoważnienia do stosowania środków o charakterze dyscyplinująco-penalnym - 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.

Natomiast odnosząc się do charakterystyki **pytań prawnych** kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w 2011 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.

Podobnie jak w latach poprzednich, w roku 2011 problematyka opinii prawnych dotyczyła różnorodnych zagadnień. Wśród nich znalazły się kwestie związane z przetwarzaniem informacji o osobie za pośrednictwem Internetu, w tym skutecznego usuwania z zasobów sieci publicznych danych osobowych, wizerunku oraz innych treści naruszających dobre imię użytkowników⁴⁸³. W korespondencji kierowanej do GODO wskazywano zwłaszcza na brak reakcji ze strony administratorów odpowiedzialnych za prowadzenie konkretnych witryn/stron internetowych, a tym samym brak skuteczności w egzekwowaniu prawa do kontroli przetwarzania danych osobowych. Natomiast osoby zainteresowane działalnością portali społecznościowych najczęściej pytały o wymagania, jakim sprostać powinny portale internetowe, za pośrednictwem których przetwarzane będą dane osobowe⁴⁸⁴, w tym szczegółowe wymogi, jakim powinny odpowiadać urządzenia zabezpieczające przetwarzane zasoby.

Wiele pytań dotyczyło obowiązku rejestracji zbiorów danych osobowych oraz interpretacji art. 43 ustawy o ochronie danych osobowych. W dużej mierze pytania dotyczyły zwolnienia z obowiązku zgłoszenia Generalnemu Inspektorowi zbioru danych oraz tego, na kim spoczywa obowiązek zgłoszenia zbioru w przypadku powierzenia danych osobowych. Niejednokrotnie również pytania dotyczyły rejestracji zbiorów obejmujących dane szczególnie chronione⁴⁸⁵.

Wśród pytających wiele niejasności budziła także kwestia tajemnicy bankowej, w szczególności uprawnień konkretnych podmiotów czy to prywatnych czy publicznych, do żądania

⁴⁸³ DOLiS-035-49/11/ 776, DOLiS-035-83/11/1101, DOLiS-035-122/11, DOLiS-035-2127/11/ 34341.

⁴⁸⁴ DOLiS-035-552/11/ 7570, DOLiS-035-762/11/ 10946.

⁴⁸⁵ DOLiS-035-12/11/ 159, DOLiS-035-77/11/ 1004, DOLiS-035-94/11/ 1443.

udostępnienia informacji objętych w/w tajemnicą⁴⁸⁶, szeroko pojętego marketingu, w tym legalności jego prowadzenia oraz formy zgłaszania sprzeciwu wobec przetwarzania danych osobowych⁴⁸⁷, a także uprawnień organów ścigania, w szczególności policji, do przetwarzania danych osobowych, w tym możliwości pozyskiwania informacji na temat danych gromadzonych przez organy ścigania przez osoby, których te dane dotyczą⁴⁸⁸.

Pytania kierowane w 2011 r. do organu ds. ochrony danych osobowych dotyczyły również kwestii legalności przetwarzania danych szczególnie chronionych (wrażliwych). W odniesieniu do placówek medycznych chodziło głównie o informacje o stanie zdrowia, w tym powierzania przetwarzania danych o charakterze medycznym,⁴⁸⁹ zaś w odniesieniu do kościołów i związków wyznaniowych – legalności przetwarzania danych osobowych przez te podmioty w szczególności w świetle procedury apostazji⁴⁹⁰.

Zakres tematyczny innych pytań prawnych obejmował zagadnienia związane z uprawnieniami pracodawcy oraz legalności przetwarzania przez niego danych osobowych pracowników w zakresie szerszym niż wskazany w ustawie z dnia 26 czerwca 1974 r. Kodeks pracy⁴⁹¹, legalności udostępniania danych osobowych przez jednostki administracji publicznej, samorządy terytorialne bądź podmioty prywatne w sytuacji braku jednoznacznych przepisów uprawniających do wykonywania takich operacji na danych osobowych⁴⁹², czy też przetwarzania danych osobowych przez fundacje i stowarzyszenia, w kontekście zakresu przetwarzania tych danych oraz możliwości powierzenia przetwarzania podmiotom zewnętrznym⁴⁹³.

Problematyka opinii prawnych sporządzonych w 2011 r. obejmowała również zagadnienia związane z działalnością spółdzielni oraz wspólnot mieszkaniowych w przedmiocie przetwarzania danych osobowych, w tym podstaw prawnych dla przetwarzania danych ich członków, jak również osób zobowiązanych do pełnienia zarządu nad konkretną nieruchomością/spółdzielnią. Zainteresowanie budziły zwłaszcza zasady udostępniania dokumentacji wytwarzanej przez te podmioty oraz okoliczności publikacji danych osobowych członków tych podmiotów⁴⁹⁴.

Jak już o tym była mowa, w dniu 7 marca 2011 r. weszła w życie ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw⁴⁹⁵, dzięki której organ do spraw ochrony danych osobowych zyskał nowe uprawnienia, w tym możliwość kierowania na

⁴⁸⁶ DOLiS-035-2436/11/ 39974, DOLiS-035-663/11/ 8935, DOLiS-035-1918/11/ 29958.

⁴⁸⁷ DOLiS-035-16/11/ 40, DOLiS-035-216/11/3063.

⁴⁸⁸ DOLiS-035-22/11/5261, DOLiS-035-167/11/ 2422, DOLiS-035-874/11.

⁴⁸⁹ DOLiS-035-583/11/8096, DOLiS-035-583/11/ 8096.

⁴⁹⁰ DOLiS-035-687/11/ 9529, DOLiS-035-2765/11/ 44922, DOLiS-035-1209/11/ 17944.

⁴⁹¹ DOLiS-035-219/11/3240, DOLiS-035-249/11/ 3490, DOLiS-035-1140/11.

⁴⁹² DOLiS-035-54/11/857, DOLiS-035-523/11/ 13751, DOLiS-035-532/11/7715.

⁴⁹³ DOLiS-035-234/11/ 3437, DOLiS-035-824/11/11863, DOLiS-035-743/11/10809, DOLiS-035-1069/11/ 15825.

⁴⁹⁴ DOLiS-035-39/11/ 679, DOLiS-035-214/11/3245.

⁴⁹⁵ Dz. U. z 2010 r. Nr 229 poz. 1497

podstawie art. 19a ustawy **wystąpić** w celu zmiany przepisów godzących w zasady prawidłowego przetwarzania danych osobowych. Będące przedmiotem wystąpień Generalnego Inspektora nieprawidłowości w dużej mierze wiązały się z brakiem uregulowania trybu postępowania z danymi osobowymi, nieprzestrzeganiem zasad prawidłowego przetwarzania danych oraz przetwarzaniem danych osobowych przez podmioty nieposiadające ku temu właściwych kompetencji.

Analiza pytań, które w 2011 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.

Analizując działania Generalnego Inspektora Ochrony Danych Osobowych w roku 2011 polegające na udzielaniu odpowiedzi na pytania prawne celem tworzenia wiedzy na temat zasad przetwarzania danych osobowych, wykładni przepisów regulujących przetwarzanie danych osobowych będące elementem jego kompetencji z zakresu doskonalenia ochrony danych osobowych, można pozwolić sobie na stwierdzenie, że tak jak i w roku 2010 istnieje wiele problemów dotyczących przetwarzania danych osobowych nieuregulowanych od strony prawnej, czy też wynikających z ich niedoskonałości bądź błędnej ich interpretacji.

Wyjątkowo niepokojące jest również, to iż organy administracji publicznej przetwarzają dane osobowe szczególnie chronione bądź zobowiązują podległe im podmioty do przetwarzania takich danych w oparciu o przepisy aktów wykonawczych bądź dokumentów wewnętrznych, co stanowi naruszenie podstawowej zasady prawidłowego przetwarzania danych osobowych.

Równie negatywnie należy oceniać praktyki organów pełniących funkcje publiczne do przetwarzania danych osobowych (np. gromadzenia, przechowywania) wbrew ich kompetencjom określonym przepisami prawa.

Kolejny wniosek nasuwający się po analizie kolejnego roku funkcjonowania organu do spraw ochrony danych osobowych, w szczególności w ramach udzielania odpowiedzi na pytania prawne to niewystarczająca wiedza obywateli na temat podstaw prawnych do przetwarzania ich danych osobowych, a tym samym brak prawidłowego informowania o tych podstawach przez podmioty publiczne i prywatne.

W porównaniu do poprzednich okresów sprawozdawczych zmniejszyła się liczba spraw, w których organ skierował **zawiadomienia o podejrzeniu popełnienia przestępstwa**. W roku 2008 było 31 zawiadomień, w 2009 – 27, w 2010 – 23, zaś w 2011 – 10. 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 postępowań przygotowawczych zakończonych bez sformułowania aktu oskarżenia. 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, co zawsze budziło zaniepokojenie organu ds. ochrony danych osobowych. Dlatego znowelizowana ustawa o ochronie danych osobowych, która weszła w życie z dniem 7 marca 2011 r. wyposażała organ ds. ochrony danych osobowych w bardziej skuteczne instrumenty egzekwowania prawa.

W tym miejscu należy podkreślić, że w 2011 r. sądy karne, na podstawie zawiadomień skierowanych w oparciu o ustalenia kontroli przeprowadzone w poprzednich okresach sprawozdawczych, wydały **dwa wyroki skazujące za przestępstwa określone w ustawie o ochronie danych osobowych**⁴⁹⁶, **1 wyrok o warunkowym umorzeniu postępowania z okresem próby na jeden rok**⁴⁹⁷, a **dwa postępowania karne są toku**⁴⁹⁸.

W odniesieniu do wyroków skazujących, w jednej sprawie sąd wymierzył karę sześćdziesięciu stawek dziennych grzywny (ustalając wysokość każdej z nich na sześćdziesiąt zł) za popełnienie czynu określonego w art. 54 ustawy o ochronie danych osobowych polegającego na tym, iż będąc administratorem danych osobowych użytkowników portalu internetowego, przedsiębiorca ten nie poinformował użytkowników portalu o tym, że gromadzi i przetwarza dotyczące ich dane osobowe, nie poinformował też o przysługujących im prawach wynikających z ustawy o ochronie danych osobowych uniemożliwiając w ten sposób korzystanie z nich⁴⁹⁹, a także czynu określonego w art. 53 ustawy o ochronie danych osobowych⁵⁰⁰ polegającego na niedopełnieniu obowiązku wynikającego z art. 40 ustawy o ochronie danych osobowych⁵⁰¹, tj. niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji zbioru danych osobowych zalogowanych użytkowników portalu internetowego.

W innej sprawie karnej osoba prowadząca działalność polegającą na prowadzeniu agencji pracy tymczasowej, została skazana na karę 5 miesięcy ograniczenia wolności w zawieszeniu w związku

⁴⁹⁶ DIS/ZAW-14/24571/10, DIS/ZAW-4/4295/10

⁴⁹⁷ DIS/ZAW-18/27349/09

⁴⁹⁸ DIS/ZAW-6/7473/10, DIS/ZAW-8/11430/10

⁴⁹⁹ Art. 24 ust. 1 ustawy o ochronie danych osobowych. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, 3) prawie dostępu do treści swoich danych oraz ich poprawiania, 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

⁵⁰⁰ Art. 53 ustawy o ochronie danych osobowych. Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

⁵⁰¹ Art. 40 ustawy o ochronie danych osobowych. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

z popełnieniem przestępstwa wskazanego w art. 49 ust. 1 ustawy o ochronie danych osobowych⁵⁰² polegającego na przetwarzaniu danych osobowych niezgodnie z prawem, w związku z kojarzeniem matek zastępczych – surogatek ze zleceniodawcami (osobami zainteresowanymi wynajęciem surogatki).

Jak już o tym wspomniano, w jednej sprawie zapadł wyrok o warunkowym umorzeniu postępowania z okresem próby na jeden rok wobec sprawcy, któremu zarzucono naruszenie art. 52, art. 53 i art. 54 ustawy o ochronie danych osobowych w związku z niezabezpieczeniem danych osobowych osób, które za pośrednictwem strony internetowej dokonały rezerwacji biletów, a także na zaniechaniu wykonania obowiązku zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych ww. osób oraz niedopełnieniu wobec nich obowiązku poinformowania o ich prawach lub przekazania tym osobom informacji umożliwiających korzystanie z praw przyznanych im w ustawie⁵⁰³. Zawiadomienie o przestępstwie zostało skierowane na podstawie wyników kontroli podmiotu, który stosował realizowany za pośrednictwem strony internetowej system rezerwacji biletów na przejazd należącymi do niego środkami transportowymi. Osoba zainteresowana dokonaniem rezerwacji biletu we wskazanym systemie zobowiązana była do założenia konta i akceptacji regulaminu przewozu osób i bagażu w komunikacji regularnej i podania swoich danych osobowych.

W toku jest postępowanie karne dotyczące niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osobowych umieszczonych na stronie internetowej prowadzonej przez kontrolowany podmiot⁵⁰⁴, a także postępowanie w sprawie niezabezpieczenia danych osobowych pracowników przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem⁵⁰⁵.

W 2011 r. do Generalnego Inspektora wpłynęło **65 wniosków o wydanie zgody na przekazanie danych osobowych do państw trzecich tzn. do państw nienależących do Europejskiego Obszaru Gospodarczego (EOG)**. Dla porównania w 2010 r. wpłynęło 37 wniosków o wydanie zgody na przekazanie danych do państw trzecich, czyli o 28 wniosków mniej niż w analizowanym roku sprawozdawczym.

Spośród 65 wniosków, które w 2011 r. wpłynęły do Biura GIODO, 40 z nich zostało rozpatrzonych i zakończonych w 2011 r. poprzez wydanie przez Generalnego Inspektora decyzji administracyjnej, 2 decyzje wydane w 2011 r. dotyczyły skomplikowanych spraw z 2009 r., natomiast pozostałe 8 spraw dotyczyło wniosków, które zostały złożone pod koniec 2010 r. **Ogółem Generalny Inspektor wydał w 2011 r. 50 decyzji administracyjnych dotyczących przekazania danych osobowych do państw trzecich.**

⁵⁰² Art. 49 ust. 1 ustawy o ochronie danych osobowych. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

⁵⁰³ DIS/ZAW-18/27349/09

⁵⁰⁴ DIS/ZAW-8/11430/10

⁵⁰⁵ DIS/ZAW-6/7473/10

Dla porównania w 2010 r. wpłynęło 37 wniosków, z których 28 zostało rozpatrzonych i zakończonych w tym samym 2010 roku poprzez wydanie przez Generalnego Inspektora decyzji administracyjnej, jedno postępowanie zostało zawieszone na wniosek strony, zaś 8 wspomnianych wniosków złożonych pod koniec 2010 r. zostało rozpatrzonych i zakończonych w 2011 r. Na podstawie powyższych danych można stwierdzić, że liczba złożonych wniosków w 2011 r. w porównaniu z rokiem 2010 wzrosła o 75%.

W analizowanym 2011 roku, podobnie jak w poprzednim roku sprawozdawczym, niejednokrotnie administratorzy danych należących do tych samych korporacji międzynarodowych składali wnioski zawierające podobne stany faktyczne i prawne. Wiązało się to z działaniami podejmowanymi w obrębie całych korporacji, do których należeli poszczególni administratorzy danych.



Wykres 47: *Zestawienie porównawcze liczby decyzji dotyczących wyrażenia zgody na przekazanie danych osobowych do państwa trzeciego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2011.*

W 48 sprawach Generalny Inspektor zezwolił na przekazanie danych, w tym w 3 sprawach częściowo umorzył postępowanie ze względu na przekazywanie danych: do odbiorców objętych zastosowaniem kanadyjskiej ustawy o ochronie danych osobowych i dokumentów elektronicznych (ang. *PIPEDA*), do odbiorców należących do amerykańskiego programu 'bezpiecznej przystani' (ang. *Safe Harbor*) oraz na wniosek strony postępowania. W dwóch sprawach Generalny Inspektor umorzył postępowania ze względu na cofnięcie wniosków przez strony postępowania.

Podobnie jak w 2009 r. i 2010 r., również w 2011 r. znaczna część wniosków dotyczyła przekazywania danych osobowych pracowników, kandydatów do pracy, klientów lub dostawców (także byłych pracowników czy przyszłych/potencjalnych klientów) w ramach międzynarodowych

grup kapitałowych, w celu ujednolicenia procesów zarządzania zasobami ludzkimi, prowadzenia rachunkowości lub zwiększaniem bezpieczeństwa danych poprzez zastosowanie jednolitych praktyk oraz procedur. Nadal pozostają popularne także transfery w ramach tzw. outsourcingu. Zasadniczo niezmieniona została 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. Pierwszy raz również Generalny Inspektor rozpatrzył i wyraził zgodę na przekazanie danych osobowych do państw trzecich na podstawie wiążących reguł korporacyjnych, względem których brał czynny udział w ramach procedury koordynacyjnej.

Podkreślenia wymaga, że znacząco zmalała liczba wniosków, w których występują różnego rodzaju błędy formalne, takie jak brak załączonego dowodu opłaty skarbowej. Zmalała również liczba wniosków zawierająca błędy merytoryczne, w tym m.in. zbyt ogólnie i niejasno określone kategorie danych czy cele przekazania. Zwiększyła się znacząco liczba odbiorców w państwach trzecich, którzy zastosowali środki organizacyjno-techniczne bazujące na polskim rozporządzeniu dotyczącym tej materii. Niemniej, nadal częstym błędem było składanie załączników do wniosku w języku angielskim, tj. 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.).

W roku 2011 wśród **10590 zgłoszeń do rejestracji** pochodzących od podmiotów publicznych stosunkowo dużą liczbę stanowiły zbiory danych osobowych prowadzone na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779 z późn. zm.). Nadsyłane zgłoszenia dotyczyły przede wszystkim prowadzonych przez straże gminne (miejskie) postępowań mandatowych. Niewątpliwie miało to związek z pismem Generalnego Inspektora z dnia 5 stycznia 2011 r.⁵⁰⁶ dotyczącym obowiązku rejestracji tych zbiorów skierowanym do Zastępcy Dyrektora Departamentu Analiz i Nadzoru Ministerstwa Spraw Wewnętrznych i Administracji. Straże Gminne, w związku z wykonywanymi zadaniami, prowadzą m.in. zbiory danych osób ukaranych za popełnienie wykroczenia w postępowaniu mandatowym. Zbiory te podlegają obowiązkowi zgłoszenia do rejestracji.

W okresie sprawozdawczym do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były także zbiory danych dotyczących osób dotkniętych przemocą i stosujących przemoc w rodzinie, zebranych w wyniku działalności zespołów interdyscyplinarnych, powołanych z dniem 1 sierpnia 2010 r. na podstawie przepisów ustawy z dnia 10 czerwca 2010 r. o zmianie ustawy o przeciwdziałaniu przemocy w rodzinie oraz niektórych ustaw (Dz. U. Nr 125, poz. 842 z późn. zm.). Większość zgłoszeń dotyczących ww. zbiorów dokonywana była przez ośrodki pomocy społecznej.

⁵⁰⁶ DRZDO-071/1/11/493

Jednakże w części zgłoszeń - jako administratorzy danych - wskazywane były jednostki samorządu terytorialnego, tj. gminy reprezentowane przez wójtów, burmistrzów i prezydentów miast.

Zespół interdyscyplinarny, zgodnie z art. 9a ust. 2 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie (Dz. U. Nr 180, poz. 1493 z późn. zm.) jest powoływany przez wójta, burmistrza albo prezydenta miasta. Jednakże, zgodnie z art. 9a ust. 9 powołanej ustawy, obsługę organizacyjno-techniczną zespołu interdyscyplinarnego zapewnia ośrodek pomocy społecznej. Treść ww. przepisu wskazuje, iż administratorem danych przetwarzanych w wyniku działalności zespołów interdyscyplinarnych jest ośrodek pomocy społecznej i to na tym podmiocie, zgodnie z art. 40 ustawy o ochronie danych osobowych, spoczywa obowiązek zgłoszenia do rejestracji zbioru danych osobowych dotyczących osób dotkniętych przemocą i stosujących przemoc w rodzinie. Stanowisko Generalnego Inspektora Ochrony Danych Osobowych w tej sprawie zostało przedstawione w piśmie z dnia 27 lipca 2011 r. skierowanym do Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych i Administracji.

Natomiast w piśmie z dnia 30 czerwca 2011 r. Dyrektor Narodowego Centrum Krwi skierował do Generalnego Inspektora zapytanie, czy zbiory danych osobowych dawców krwi oraz potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej prowadzonych przez regionalne centra krwiodawstwa i krwiolecznictwa, podlegają obowiązkowi zgłoszenia do rejestracji. Na podstawie analizy dokonanej w Departamencie Rejestracji Zbiorów Danych Osobowych została przygotowana odpowiedź zawierająca stanowisko Generalnego Inspektora, zgodnie z którym ww. zbiory danych osobowych podlegają obowiązkowi rejestracji.

W świetle przepisów ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi ww. podmioty prowadzą rejestr dawców krwi. Z kolei przepisy ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz.U. Nr 169, poz.1411 z późn. zm.) zawierają uregulowania dotyczące zasad prowadzenia czynności polegających na pozyskiwaniu potencjalnych dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej. Czynności te mogą być wykonywane przez podmioty lecznicze albo fundacje, które uzyskały odpowiednie pozwolenie ministra właściwego do spraw zdrowia (art. 16a ust. 1 ustawy transpalntacyjnej). Zgodnie z art. 16a ustawy transpalntacyjnej ośrodek dawców szpiku gromadzi dane potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej. Biorąc pod uwagę, że art. 16a ust. 1 ustawy transplantacyjnej wyróżnia wśród podmiotów, które mogą być ośrodkami dawców szpiku, obok podmiotów leczniczych również fundacje, uznać należy, że zadania ośrodka dawców szpiku związane z gromadzeniem i przechowywaniem danych potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej w ramach pozyskiwania potencjalnych dawców mogą być realizowane przez podmioty w ogóle nieprowadzące działalności leczniczej, a tym samym nieudzielające jakichkolwiek świadczeń zdrowotnych. Na gruncie definicji świadczeń zdrowotnych zawartej w art. 2 ust. 1 pkt 10

ustawy o działalności leczniczej (Dz.U. Nr 112, poz. 654), która powinna stanowić punkt wyjścia dla określenia znaczenia użytego w art. 43 ust. 1 pkt 5 ustawy pojęcia usługi medycznej, brak jest podstaw, aby różnicować realizację tego samego zadania i kwalifikować działalność polegającą na gromadzeniu i przechowywaniu danych potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej jako świadczenie zdrowotne, gdy ośrodek jest podmiotem leczniczym, a odmawiać takiej kwalifikacji w przypadku fundacji. Ponieważ działalność tę prowadzić może fundacja nie będąca podmiotem leczniczym uznać należy, że działalność ta nie jest świadczeniem zdrowotnym. Mimo więc, że regionalne centrum jako podmiot leczniczy w ogóle wykonuje działalność leczniczą, to jednak nie wykonuje jej w zakresie, w jakim realizuje zadania ośrodka dawców szpiku związane z prowadzeniem rejestru potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej.

Za rozstrzygającą o obowiązku zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych prowadzonych przez regionalne centra zbiorów danych osobowych dawców krwi oraz potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej, uznać należy okoliczność, że osób tych nie można zakwalifikować jako korzystające z usług medycznych administratora danych w rozumieniu art. 43 ust. 1 pkt 5 ustawy. W związku z powyższym trudno jest przyjąć, że w przypadku dawców krwi oraz potencjalnych dawców szpiku i komórek krwiotwórczych mamy do czynienia z osobami korzystającymi z usług medycznych regionalnego centrum. Oceny tej nie zmienia fakt, że np. w ramach badań lekarskich poprzedzających pobranie krwi od kandydata na dawcę krwi lub dawcy krwi, czy w zakresie badań lekarskich potencjalnych dawców szpiku, wobec tych osób, co do zasady, będą wykonywane przez regionalne centra działania medyczne. Działania te podejmowane są jednak na potrzeby pozyskania dawcy krwi lub potencjalnego dawcy szpiku i w ostatecznym rozrachunku mają na celu korzyść biorcy. Natomiast nie będą służyć zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia (leczeniu) krwiodawcy lub potencjalnego dawcy szpiku. Osoby te, co do zasady, nie będą działań medycznych potrzebować. Ich wykonanie nie jest więc równoznaczne ze skorzystaniem przez dawcę krwi lub potencjalnego dawcę z usługi medycznej w rozumieniu art. 43 ust. 1 pkt 5 ustawy.

W związku z powyższym oraz biorąc pod uwagę ogólną zasadę, zgodnie z którą przepisy przewidujące wyjątki od ogólnej reguły należy interpretować ściśle, a wszelka interpretacja rozszerzająca w tym zakresie jest zakazana, uznać należało, że zwolnienie od obowiązku rejestracji przewidziane w art. 43 ust. 1 pkt 5 ustawy, nie ma zastosowania do zbiorów danych osobowych krwiodawców oraz potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej prowadzonych przez regionalne centra.

Oprócz spraw związanych z rejestracją lub odmową rejestracji konkretnego zbioru danych osobowych, opiniowane były również projekty z zakresu legislacji. Jako przykład można wskazać opinię do „Projektu założeń projektu ustawy o redukcji obowiązków informacyjnych oraz

o ograniczeniu barier administracyjnych dla obywateli i przedsiębiorców” jak również uwagi do projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, w szczególności do art. 174a-174c, które dotyczą nowych zadań Generalnego Inspektora Ochrony Danych Osobowych.

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 zawierającego analizę spraw dotyczących naruszeń ochrony danych, wyników przeprowadzonych kontroli, wydanych opinii, przedsięwzięć legislacyjnych, orzecznictwa sądów karnych i administracyjnych, a także 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 ze wszystkimi podmiotami, które mają wpływ na tworzenie prawa, jego stosowanie i egzekwowanie, a także ze stowarzyszeniami, ośrodkami naukowymi i organizacjami branżowymi zajmującymi się ochroną danych osobowych i prawami obywateli oraz ze środkami masowego przekazu. Współdziała także z różnymi podmiotami na arenie międzynarodowej, aktywnie uczestnicząc w ich działalności i wpływając na podejmowane przez nich decyzje o międzynarodowym zasięgu. Wszystkie te elementy aktywności GODO składają się na sumę jego doświadczeń w kwestii usprawnienia pracy organu i zapewnienia skutecznej realizacji prawa do prywatności i ochrony danych osobowych zarówno w Polsce, jak i poza jej granicami.

Szybki rozwój technologiczny i globalizacja przyniosły nowe wyzwania w sferze ochrony danych osobowych. Poszerzają się zwłaszcza obszary wymiany informacji i zbierania danych osobowych. Nowoczesne technologie umożliwiają osobom fizycznym, przedsiębiorcom prywatnym i organom publicznym wykorzystywanie danych osobowych do wykonywania powierzonych im zadań i dzielenie się informacjami na niespotykaną dotąd skalę. Przykładem mogą być sieci społecznościowe, czy przetwarzanie w chmurze – tzn. przetwarzanie dokonywane w Internecie przy pomocy oprogramowania, dzielonych zasobów i informacji znajdujących się na zewnętrznych serwerach (w chmurze obliczeniowej). Stanowią one poważne wyzwanie dla ochrony danych, ponieważ wiąże się to z możliwością utraty kontroli jednostki nad informacjami, które jej dotyczą. Przewiduje się też rozwój dużej liczby różnego rodzaju rejestrów zakładających możliwość współdzielenia zawartych w nich danych i – jak to zastało na przykład zapowiedziane w ustawie o informatyzacji - będą one

prorowadzone przy użyciu systemów teleinformatycznych. Dla przykładu, Centrum Projektów Informatycznych realizuje projekt pl.ID – polska ID karta, w wyniku którego powstanie nowoczesny elektroniczny dowód osobisty. System, który jest budowany w ramach tego projektu zakłada gromadzenie danych o osobach fizycznych i dokumentach w trzech rejestrach publicznych: PESEL (Powszechny Elektroniczny System Ewidencji Ludności), CRASC (Centralny Rejestr Aktów Stanu Cywilnego – zostanie zbudowany w latach 2012-2013) i RDO (Rejestr Dowodów Osobistych). Dzięki bezpłatnemu podpisowi elektronicznemu zapisanemu w dowodzie, możliwe będzie korzystanie za pomocą Internetu z usług oferowanych przez urzędy. Z drugiej jednak strony, w ramach tego projektu mają powstać rozwiązania techniczne, które umożliwią urzędnikowi elektroniczny dostęp do różnych rejestrów publicznych prowadzonych przez inne urzędy. Stąd ogromnym wyzwaniem dla GIODO, który będzie kontrolował realizację tego zadania, będzie sprawdzenie, czy stworzony system autoryzacji zapewnia dostęp poszczególnych urzędników do takiego zakresu danych rejestrowych, jakie przewiduje obecnie obowiązujące prawo. Obawy też budzi to, na ile wybrana technologia gwarantować będzie odpowiedni poziom bezpieczeństwa danych w czasie transmisji i chronić przed kradzieżą tożsamości. GIODO wskazuje też na niebezpieczeństwo powierzenia administracji publicznej zestawu danych, które mogą posłużyć do profilowania obywateli.

Ogółem w 2011 r. znacząco wzrosła liczba baz danych tworzonych przez podmioty sektora publicznego. Często przybierały one postać megabazy, jak np. zmodyfikowany system informacji oświatowej, czy system informacji w ochronie zdrowia. Ruszyła też część planowanych dużych projektów realizowanych przez Centrum Systemów Informacyjnych Opieki Zdrowotnej, między innymi budowa prototypu internetowego konta pacjenta czy e-recepty, które znalazły się w polu szczególnego zainteresowania organu z uwagi na przetwarzanie danych wrażliwych. W przypadku systemu informacji oświatowej, jak i systemu informacji w ochronie zdrowia, w 2011 r. nastąpił koniec pracy legislacyjnej na poziomie Sejmu. Ale dla GIODO praca się dopiero zaczyna. Systemy te należy teraz uważnie kontrolować i monitorować ich pracę.

Otwartym też wciąż pozostaje pytanie, w jaki sposób zagwarantować realizację konstytucyjnego prawa do informacji publicznej z poszanowaniem prawa jednostki do prywatności. Rozwój Internetu spowodował bowiem zmianę podejścia do informacji publicznej, które powinno uwzględniać jakość, aktualność i ochronę prywatności. Potrzebne są jednak działania wspierające, jak podnoszenie kwalifikacji kadr sektora publicznego i zwiększenie wymagań dotyczących komunikacji teleinformatycznej. Stąd pilna potrzeba monitorowania przez GIODO koniecznych zmian w uchwalonej w 2011 r. ustawie o dostępie do informacji publicznej w kierunku ograniczeń prawa do informacji, w tym do tajemnicy. W opinii GIODO problem wspomnianego dostępu nabiera szczególnego znaczenia w obliczu wprowadzenia do polskiego porządku prawnego regulacji dotyczących ponownego wykorzystywania informacji publicznej. Zdaniem organu konieczne jest

dokonanie rzetelnej analizy w celu ustalenia, w jakich przypadkach i jak długo, dane osobowe objęte informacją publiczną powinny być prezentowane na stronach internetowych.

Kolejną kwestią niedostatecznie uregulowaną w polskim prawie, to problem jawnego dostępu do danych oraz problem otwartego dostępu do danych w Internecie. Cały czas posługujemy się pojęciem jawności formalnej rejestrów publicznych, które pochodzi z lat 30. XX wieku. Tymczasem to, co było jawne w formie papierowej jest dzisiaj jawne w Internecie. Nie mamy rozstrzygnięcia, czy każdy dokument, który był jawny na przykład w związku z jawnością ksiąg wieczystych, powinien być umieszczany w internetowych, łatwych do przeszukania, skopiowania i wykorzystania w innych celach, bazach danych. Dlatego Generalny Inspektor Ochrony Danych Osobowych zwraca uwagę, że w przypadku rejestrów sądowych, ksiąg wieczystych czy wokand sądowych, ten problem zaczyna być problemem bezpieczeństwa obywateli, którzy mogą być łatwo sprofilowani przy pomocy danych udostępnionych z **formalnie jawnych źródeł**.

Istotnym i wciąż aktualnym zadaniem stojącym przed organem ds. ochrony danych osobowych będzie kwestia zwiększenia świadomości podmiotów przetwarzających dane osobowe w Internecie oraz osób prywatnych korzystających z sieci. Organy ochrony danych, zrzeszenia przedsiębiorców i organizacje konsumenckie zgodne są co do tego, że wzrasta zagrożenie dla prywatności i ochrony danych osobowych w związku z działalnością w Internecie. Podkreślić należy, że budowanie zaufania do technologii informatycznych jest kluczowym elementem rozwoju gospodarczego. Jego brak może wprowadzić niepewność w korzystaniu z usług internetowych, spowolnić rozwój innowacyjnego wykorzystania nowych technologii i tym samym blokować rozwój europejskiego jednolitego rynku cyfrowego oraz ożywienie gospodarcze. Z drugiej strony mamy również ważne zadanie dla organu ds. ochrony danych dotyczące kwestii związanej z zachęceniem administratorów danych do inwestowania, od początku, w prawidłową ochronę danych (ocena wpływu na ochronę prywatności, prywatność w fazie projektowania, ustawienia domyślne) oraz wzrostu ich świadomości co do odpowiedzialności i rozliczalności za przetwarzane dane osobowe przez cały cykl życia informacji. Konieczne jest również zapewnienie spójności przepisów prawa o ochronie danych w odniesieniu do działalności podmiotów gospodarczych. Złożoność przepisów odnoszących się do międzynarodowych transferów danych osobowych jest bowiem często uważana za istotną przeszkodę w prowadzonej przez te podmioty działalności. Dlatego ochrona danych osobowych odgrywa tak ważną, wręcz kluczową rolę w Europejskiej Agendzie Cyfrowej⁵⁰⁷ i strategii „Europa 2020”⁵⁰⁸.

Brak zaufania do Internetu, przy jednoczesnym zaciekawieniu nowoczesnymi technologiami, potwierdza wspomniane wcześniej w niniejszym Sprawozdaniu badanie Eurobarometru dotyczące

⁵⁰⁷ COM(2010) 245 wersja ostateczna.

⁵⁰⁸ COM(2010) 2020 wersja ostateczna.

ochrony danych osobowych oraz tożsamości elektronicznej w Unii Europejskiej. Badanie to zostało zlecone przez wydziały Komisji odpowiedzialne za wymiar sprawiedliwości, społeczeństwo informacyjne i media oraz jej Wspólne Centrum Badawcze. Wyniki badań pokazują, że w obszarze ochrony danych osobowych większym zaufaniem cieszą się organy publiczne, takie jak szpitale (78 %), rządy (70 %) oraz instytucje UE (55 %), niż firmy prywatne, np. sklepy (39 %), dostawcy Internetu (32 %) czy usługodawcy Internetowi (22 %). Z drugiej jednak strony, na pytanie o zainteresowanie Internetem, 60 % Europejczyków, którzy korzystają z sieci (40 % wszystkich obywateli UE) kupuje lub sprzedaje rzeczy on-line oraz korzysta z portali społecznościowych. Co więcej, na stronach tych ujawniają swoje dane osobowe, w tym informacje biograficzne (prawie 90 % badanych), informacje o swoim otoczeniu (ok. 50 %), a nawet dane podlegające szczególnej ochronie (ok. 10 %). Spośród badanych ponad 70 % wyraziło obawy co do tego, w jaki sposób firmy korzystają z tych danych oraz uważa, że ma jedynie częściową (a najczęściej znikomą) kontrolę nad własnymi danymi.

W tym miejscu warto podkreślić, że 58 % użytkowników Internetu czyta informacje o prywatności on-line, ale nie wszyscy ją jednak rozumieją. Ogółem 62 % użytkowników sieci bądź nie rozumie tych informacji, nie czyta ich, nie może ich znaleźć, bądź je ignoruje. Dlatego jednym z głównych celów unijnej reformy ochrony danych jest wzmocnienie przepisów, tak by usługodawcy w sposób bardziej przejrzysty informowali klientów o proponowanej usłudze i gwarantowali odpowiednie środki bezpieczeństwa przetwarzanym danym osobowym.

Ankieta Eurobarometru ujawniła także znaczące różnice postaw w odniesieniu do kwestii udostępniania danych osobowych między młodą generacją, która ma mniejsze opory przed ujawnianiem danych na temat swojej osoby oraz starszą, która częściej wyraża zaniepokojenie kwestią prywatności, wykazując mniejsze zaufanie do nowoczesnych technologii informatycznych.

W celu budowy i zwiększenia tego zaufania zaproponowane zostały rewolucyjne zmiany w unijnym prawie o ochronie danych osobowych. Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych zastąpić ma rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, którego projekt został oficjalnie przedstawiony podczas uroczystości związanych z obchodami VI Europejskiego Dnia Ochrony Danych Osobowych w Brukseli. Wspomniane rozporządzenie będzie obowiązywać bezpośrednio w krajach członkowskich, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Dzięki jego wprowadzeniu nastąpi pełna harmonizacja prawa materialnego w ramach UE. Natomiast zasady ochrony danych osobowych w policji i wymiarze sprawiedliwości w sprawach karnych uregulowane zostaną w dyrektywie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie

przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych.

W opinii Generalnego Inspektora Ochrony Danych Osobowych proponowane zmiany idą we właściwym kierunku. Dzięki ich wprowadzeniu powstanie wspólny rynek przepływu informacji, a jednocześnie zapewniona zostanie odpowiednia ochrona danych osobowych przed działaniami z zewnątrz UE i przy przekazywaniu danych do państw trzecich. Projektowane przepisy są doprecyzowane pod względem terminologii, która jest używana w świecie nowych technologii i jednocześnie są one technologicznie neutralne, tzn. nie opisują konkretnych modeli biznesowych czy technologii, lecz wprowadzają rozwiązania prawne umożliwiające wyjaśnianie problemów występujących w związku z wykorzystywaniem nowoczesnych rozwiązań. GODO z zadowoleniem przyjmuje przyjęte przez Komisję Europejską propozycje, które mają na celu wzmocnienie pozycji osób, których dane dotyczą, zwiększenie odpowiedzialności administratorów danych i umocnienie pozycji organów nadzorczych, zarówno na poziomie krajowym, jak i międzynarodowym. Dla przykładu, nieudostępnienie możliwości darmowego przeglądania, poprawiania i usuwania swoich danych przez użytkowników Internetu będzie karany grzywną do 250 tysięcy euro, albo pół procenta globalnego obrotu firmy. Duży nacisk położony jest też na prawo do bycia zapomnianym skierowane przede wszystkim pod adresem serwisów społecznościowych - użytkownik będzie mógł zażądać usunięcia z serwisu wszystkich informacji jakie tam zamieścił, i żądanie to musi być przekazane i uwzględnione przez firmy trzecie, którym informacje te zostały przekazane (np. w celach reklamowych). Co więcej, zgodnie z planami KE w przyszłości ma także zniknąć obowiązek rejestrowania zwykłych baz danych, co zdaniem GODO jest bardzo dobrym pomysłem, wartym uwzględnienia w polskim prawie o ochronie danych osobowych zanim wejdzie w życie europejskie rozporządzenie. W nadchodzącym czasie GODO planuje nowelizację ustawy o ochronie danych osobowych w tym właśnie zakresie.

Generalny Inspektor Ochrony Danych Osobowych podkreśla, że proponowane zmiany stanowią solidną podstawę dla europejskich ram regulacyjnych, aby skutecznie chronić prawo do ochrony danych, ale podkreśla potrzebę kontynuacji prac nad ostatecznym ich kształtem. Zdaniem Generalnego Inspektora szczególną rolę w polskim systemie prawnym odegra proponowana dyrektywa dotycząca policji i wymiaru sprawiedliwości, jako że zasady zawarte w zaprezentowanym projekcie nie są obecne w istniejących dziś polskich przepisach prawa. Stąd potrzebny jest aktywny udział polskiego organu ds. ochrony danych w pracach legislacyjnych na poziomie UE, w tym również Parlamentu Europejskiego.

Poprzez aktywne uczestnictwo GODO w międzynarodowych konsultacjach na temat przyszłych ram prawnych ochrony danych osobowych, Generalny Inspektor czuwał 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. Dokładał też starań, aby poprzez szeroko zakrojone działania edukacyjno-informacyjne efekty jego działalności oraz działań instytucji europejskich, w pełni przeniknęły do świadomości społecznej, przyczyniając się do wzrostu kultury prawnej. Publiczna dyskusja na temat kierunków dalszych zmian w polskiej ustawie o ochronie danych osobowych była kontynuowana przez Generalnego Inspektora Ochrony Danych Osobowych przez cały 2011 r. Odbывała się ona z udziałem przedstawicieli różnych środowisk (akademickich, branżowych, różnych stowarzyszeń, mediów) w formie spotkań, seminariów i konferencji.

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 przeglądu polskiej legislacji pod kątem dopracowania przepisów odnoszących się do ochrony danych osobowych w celu zgodnego z prawem i sprawniejszego wykonywania ustawowych obowiązków przez różne podmioty. Dla przykładu - ustawa o Policji upoważnia ten organ do wkraczania w chronioną konstytucyjnie sferę danych osobowych, dając uprawnienie do tworzenia różnego rodzaju baz, w których są gromadzone, przetwarzane i wykorzystywane dane o osobach, w tym nieletnich. W ślad za uprawnieniem do utworzenia, np. Krajowego Systemu Informacyjnego Policji (KSIP) nie pojawiły się jednak szczegółowe przepisy normujące w sposób jednoznaczny i precyzyjny kryteria gromadzenia danych i mechanizm ich weryfikacji, a w konsekwencji usuwania i niszczenia. Takiego mechanizmu nie ma także w systemach informatycznych innych służb i organów państwowych, co stwarza poważne zagrożenie dla konstytucyjnie chronionej prywatności obywateli. Tym większe, że służby te wymieniają się zgromadzonymi informacjami i powstają coraz to nowe bazy danych tworzone na potrzeby różnych instytucji, zawierające informacje kryminalne, o należnościach podatkowych, udzielonych świadczeniach zdrowotnych, o nieruchomościach czy procesie edukacyjnym. Docelowo planowana jest wymiana danych między poszczególnymi bazami, a akty prawne je regulujące często w ogóle nie przewidują opcji usuwania z nich danych. Wobec tych regulacji prawnych ustawa o ochronie danych osobowych nie zapewnia gwarancji adekwatności gromadzonych danych i zasady czasowego ich przetwarzania.

Niepokój GODO budzi także to, że w wielu przypadkach przetwarzanie danych osobowych jest przedmiotem przepisów szczególnych, które dają ogromne kompetencje i do których ustawa o ochronie danych osobowych jedynie odsyła. Stąd Generalny Inspektor ogromną wagę przywiązuje do legislacji, czyli monitoringu przez organ ds. ochrony danych, projektów aktów prawnych przed ich uchwaleniem oraz wskazuje na konieczność istnienia silnych, także wewnętrznych, procedur kontroli

i nadzoru nad tymi systemami. Z uwagi na to, że Generalny Inspektor Ochrony Danych Osobowych nie ma uprawnień pozwalających na zaskarżenie ustawy do Trybunału Konstytucyjnego, jego rola siłą rzeczy ogranicza się jedynie do ich opiniowania.

Obszar działań Generalnego Inspektora Ochrony Danych Osobowych jest bardzo szeroki i wymaga kompetencji organu w wielu różnych dziedzinach prawa, nauki czy gospodarki. Charakterystycznym przykładem różnych dziedzin, którymi organ ds. ochrony danych zajmował się w minionym 2011 r. był m.in. monitoring wizyjny, usługi typu cloud computing, tzw. internet przedmiotów oraz przepisy dotyczące inteligentnych liczników energetycznych, czyli projekt nowego Prawa energetycznego. W odniesieniu do tych ostatnich, przygotowano wystąpienie GODO do Ministra Gospodarki w sprawie uwzględnienia w przygotowanych założeniach do ustawy o inteligentnych sieciach energetycznych oraz innych regulacjach, w tym dotyczących wdrażania systemów inteligentnego opomiarowania, zasad wynikających z przepisów ustawy o ochronie danych osobowych.

Natomiast główny problem z **monitoringiem wizyjnym** – sygnalizowany przez organ również w poprzednim okresie sprawozdawczym – to ciągły 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”.

W 2011 r. w Generalny Inspektor Ochrony Danych Osobowych prowadził prace na potrzeby uregulowania przetwarzania danych osobowych pozyskiwanych przez systemy monitoringu. Ich rezultatem było opracowanie dokumentu przedstawiającego uzasadnienie i wstępne założenia do prac mających na celu prawne uregulowanie zasad stosowania monitoringu w obszarach dotąd nieuregulowanych. W opracowaniu wskazano obszary wymagające regulacji w zakresie zasad stosowania monitoringu, wstępne propozycje wymagań w zakresie warunków, jakie systemy te powinny spełniać, potrzebę określenia trybu i zasad wydawania zgody na stosowanie monitoringu, jak również propozycję warunków i zasad udostępniania i przechowywania danych pozyskanych w wyniku jego stosowania. Przygotowany dokument został przekazany do Ministerstwa Spraw Wewnętrznych

i Administracji jako wkład GIODO na potrzeby przygotowania regulacji prawnych w zakresie dotyczącym stosowania monitoringu.

Podobnie sytuacja przedstawia się 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 zainteresowany 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.

Pomimo ograniczenia przez ustawodawcę uprawnień organu ds. ochrony danych osobowych do kontroli przetwarzania danych osobowych w działalności **kościół i innych związków wyznaniowych**, pojawiły się jednak w tym obszarze pewne kwestie wymagające pilnego rozwiązania. Na podstawie art. 43 ust. 2 ustawy o ochronie danych osobowych, w odniesieniu do zbiorów dotyczących osób należących do kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub innego związku wyznaniowego, Generalnemu Inspektorowi nie przysługują uprawnienia do rozpatrywania skarg, wydawania decyzji administracyjnych, przeprowadzania czynności kontrolnych, wglądu do dokumentów oraz wstępu do pomieszczeń, w których przetwarzane są dane osobowe. W sytuacji braku takich uprawnień GIODO nie jest w stanie określić, czy gromadzone w zbiorach dane są adekwatne do celu przetwarzania związanego z realizacją działań statutowych tych podmiotów. W przeciwnym razie należałoby przyjąć, że dane pozyskane na podstawie innej niż art. 27 ust. 2 pkt 4 ustawy, podlegają reżimowi ustawy o ochronie danych osobowych, również w zakresie ich usunięcia i zaprzestania przetwarzania. Generalny Inspektor Ochrony Danych Osobowych może natomiast występować w takich sprawach o wyjaśnienia, sygnalizować nieprawidłowości, ewentualnie zawiadamiać o popełnieniu przestępstwa.

Podkreślić także trzeba, że kościoły i inne związki wyznaniowe w stosunku do osób niebędących ich członkami, nie korzystają z wyłączenia wskazanego w art. 27 ust. 2 pkt 4 ustawy, który stanowi, że przetwarzanie danych szczególnie chronionych (m.in. danych o przekonaniach religijnych, przynależności wyznaniowej) jest dopuszczalne jeżeli jest to niezbędne m.in. do wykonywania statutowych zadań kościołów i innych związków wyznaniowych pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji, albo osób utrzymujących z nimi stałe kontakty w związku z prowadzoną działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych. W takiej sytuacji kościół lub związek wyznaniowy ma obowiązek zaprzestania przetwarzania danych osobowych takiej osoby, a jedyną adnotacją, którą może

dokonać w prowadzonym przez siebie zbiorze, jest odnotowanie daty wystąpienia tej osoby z kościoła lub związku wyznaniowego.

Równie ważna jest kwestia **usunięcia danych zebranych przez kościół lub związek wyznaniowy w okresie, gdy dana osoba do niego jeszcze należała**. GODO przyjął interpretację – do tej pory niekwestionowaną przez sądy – że osobie fizycznej nie przysługuje prawo do wykreślenia dotyczących jej danych z okresu przynależności do kościoła lub związku wyznaniowego. Dzieje się tak dlatego, że w opinii GODO zasady archiwizowania informacji zawartych w księgach kościelnych wynikają z innych niż ustawa o ochronie danych osobowych regulacji. W przypadku Kościoła katolickiego jest to kanon 535 Kodeksu prawa kanonicznego, który wskazuje na konieczność stałego przechowywania informacji związanych z działalnością Kościoła i ich odpowiedniego zabezpieczenia. Natomiast fakt wystąpienia z Kościoła katolickiego jest odnotowywany w księdze chrztów po przejściu procedury apostazji.

W praktyce swego działania organ ds. ochrony danych napotykał też problemy z określeniem, czy dana osoba należy czy też nie należy do danego kościoła lub związku wyznaniowego. W opinii GODO wskazane byłoby uregulowanie tej kwestii zarówno w przypadku kościołów i związków wyznaniowych, które posiadają osobną regulację ustawową o stosunku Państwa do nich, jak i w przypadku innych kościołów i związków wyznaniowych wpisanych do rejestru prowadzonego przez Ministra Administracji i Cyfryzacji.

W opinii Generalnego Inspektora autonomia kościołów i związków wyznaniowych gwarantowana przez Konstytucję RP nie wyklucza innego uregulowania kwestii uprawnień kontrolnych GODO i kwestii związanych z rejestracją zbiorów danych osobowych prowadzonych przez kościoły i związki wyznaniowe, niż jest to przewidziane przez obecnie obowiązujące przepisy prawa, co można by rozważyć przy kolejnej nowelizacji ustawy o ochronie danych osobowych.

Zagadnienie formy wystąpienia z kościoła lub związku wyznaniowego znacząco przekracza uprawnienia GODO i zapewne powinno być zróżnicowane w stosunku do różnych kościołów i związków wyznaniowych. **Byłoby jednakże wskazane określenie w przypadku każdego z kościołów i związków wyznaniowych, od którego momentu należy uznawać publiczno-prawne skutki wystąpienia z kościoła lub związku wyznaniowego.** Obecna sytuacja prawna prowadzi do znaczącej niepewności i – choć decyzję Generalnego Inspektora Ochrony Danych Osobowych, opierające się na dziś obowiązujących przepisach, nie są kwestionowane przez Wojewódzki Sąd Administracyjny w Warszawie, to *de lege ferenda* Generalny Inspektor Ochrony Danych Osobowych sugeruje, by w przyszłych rozwiązaniach prawnych dotyczących statusu kościołów i związków wyznaniowych w Polsce kwestie te uregulować prawnie w sposób niepozostawiający wątpliwości interpretacyjnych.

Podsumowując, wśród zasygnalizowanych kierunków działań organu na przyszłość, priorytetem będzie intensyfikacja prac nad wdrożeniem nowych ram prawnych ochrony danych osobowych tak, aby przeszły próbę czasu. Po zakończeniu tego procesu reform europejskie przepisy o ochronie danych osobowych powinny gwarantować wysoki poziom ochrony i pewność prawną zarówno osobom fizycznym, administracji publicznej, jak i przedsiębiorcom prywatnym na rynku wewnętrznym. Niezależnie bowiem od stopnia zaawansowania nowoczesnych technologii, musi panować jasność co do obowiązujących przepisów prawa o ochronie danych osobowych. Zadanie to realizowane będzie przez Generalnego Inspektora Ochrony Danych Osobowych przy pomocy niepowiększonej od 2 lat liczbie pracowników Biura GIODO i utrzymującym się na tym samym poziomie budżecie. Sytuacja finansowa i kadrowa Biura GIODO nie pozwala na szerokie rozwinięcie działalności, co wskazuje że konieczne jest wzmocnienie instytucjonalne organu ds. ochrony danych osobowych.

ZAŁĄCZNIKI:**Załącznik nr 1**

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych
w roku 2011 o charakterze generalnym do centralnych organów państwa i do innych podmiotów
z sektora publicznego**

L.p.	Nazwa podmiotu, do którego skierowano wystąpienie	Data wystąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	Naczelna Dyrekcja Archiwów Państwowych	11.01.2011 DOLiS-035-42/11	Wystąpienie do Naczelnej Dyrekcji Archiwów Państwowych w Warszawie z prośbą o przedstawienie stanowiska w przedmiocie przechowywania danych stanowiących informację publiczną, dotyczących osób sprawujących funkcje publiczne.
2.	Narodowy Fundusz Zdrowia	18.01.2011 DOLiS-035-108/11	Wystąpienie do Narodowego Funduszu Zdrowia w sprawie ujawnienia danych o stanie zdrowia na blankiecie zlecenia na zaopatrzenie w wyroby medyczne będące przedmiotami ortopedycznymi i środkami pomocniczymi.
3.	Minister Sprawiedliwości	03.02.2011 DOLiS-035-277/11	Wystąpienie do Ministra Sprawiedliwości z prośbą o podjęcie prac legislacyjnych mających na celu uregulowanie zakresu danych dotyczących kandydatów na aplikację gromadzonych za pomocą kwestionariuszy osobowych.
4.	Komendant Straży Gminnej Zbrosławice	07.02.2011 DOLiS-035-314/11	Wystąpienie do Komendanta Straży Gminnej Zbrosławice z prośbą o zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających właściwą ochronę przetwarzanych danych osobowych, dotyczących przesyłania korespondencji za pośrednictwem poczty elektronicznej.
5.	Dyrektor Zakładu Karnego w Chełmie	11.02.2011 DOLiS-035-382/11	Wystąpienie do Dyrektora Zakładu Karnego w Chełmie z prośbą o dostosowanie zasad postanowień regulaminu organizacyjno-porządkowego do wymogów określonych w ustawie o ochronie danych osobowych.
6.	Wójt Gminy Klombów	15.02.2011 DOLiS-035-423/11	Wystąpienie do Wójta Gminy Klombów z prośbą o zmianę formularza wniosku o udostępnienie informacji publicznej i dostosowanie go do przepisów o ochronie danych osobowych.
7.	Minister Sprawiedliwości	15.02.2011 DOLiS-434/11	Wystąpienie do Ministra Sprawiedliwości w sprawie wyeliminowania nieprawidłowości w procesie udostępniania danych osobowych tłumaczy przysięgłych.
8.	Prezes GUS, Rzecznik Praw Obywatelskich, Prezes Rady Ministrów	22.02.2011 DOLiS-033-37/11	Wystąpienie do Prezesa Głównego Urzędu Statystycznego, Rzecznika Praw Obywatelskich oraz Prezesa Rady Ministrów Pana Donalda Tuska w sprawie niezgodności z Konstytucją przepisów ustawy o statystyce publicznej.
9.	Minister Gospodarki	23.02.2011 DOLiS-035-530/11	Wystąpienie do Ministra Gospodarki z prośbą o rozważenie możliwości podjęcia działań legislacyjnych mających na celu zmianę brzmienia przepisów ustawy o gospodarce nieruchomościami odnoszących się do zakresu danych osobowych

			osób, którym nadano uprawnienia i licencje zawodowe publikowanych w dzienniku urzędowym ministra właściwego do spraw budownictwa, gospodarki przestrzennej i mieszkaniowej oraz na stronach internetowych urzędu obsługującego ministra.
10.	Prezes Krajowej Rady Komorniczej	4.03.2011 DOLiS-440-196/11	Wystąpienie do Prezesa Krajowej Rady Komorniczej w Warszawie z prośbą o rozważenie zmiany praktyki stosowanej przez komorników sądowych, polegającej na udostępnianiu w treści pism kierowanych do stron postępowań egzekucyjnych zbyt szerokiego zakresu danych osobowych dłużników.
11.	Minister Zdrowia	20.04.2011 DOLiS-035-1187/11	Wystąpienie do Ministra Zdrowia z prośbą o podjęcie prac legislacyjnych zmierzających do kompleksowego uregulowania problematyki dotyczącej przetwarzania danych osobowych przez gminne komisje rozwiązywania problemów alkoholowych.
12.	Minister Spraw Wewnętrznych i Administracji	27.04.2011 DOLiS-035-1297/11	Wystąpienie do Ministra Spraw Wewnętrznych i Administracji z prośbą o przekazanie organom reprezentującym gminy informacji o obowiązkach wynikających z ustawy o ochronie danych osobowych (dot. gminnych zespołów interdyscyplinarnych).
13.	Minister Spraw Wewnętrznych i Administracji	28.04.2011 DOLiS-035-1277/11	Wystąpienie do Ministra Spraw Wewnętrznych i Administracji z prośbą o podjęcie prac legislacyjnych zmierzających do zmiany aktualnego stanu prawnego dotyczącego zasad działania komisji rewizyjnych kontrolujących działalność jednostek samorządu terytorialnego.
14.	Minister Spraw Wewnętrznych i Administracji	31.05.2011 DOLiS-035-1587/11	Wystąpienie do Ministra Spraw Wewnętrznych i Administracji z prośbą o podjęcie inicjatywy ustawodawczej w sprawie zmiany ustawy o orderach i odznaczeniach.
15.	Minister Sprawiedliwości	27.06.2011 DOLiS-035-1860/11	Wystąpienie do Ministra Sprawiedliwości z prośbą o szczegółowe uregulowanie problematyki dotyczącej udostępnienia danych osobowych osób objętych nadzorem kuratorów sądowych w związku z wykonywaniem czynności kuratora.
16.	Przewodniczący Komisji Nadzoru Finansowego	13.07.2011 DOLiS-035-2033/11	Wystąpienie do Przewodniczącego Komisji Nadzoru Finansowego w związku z tym, iż GIODO pozyskał informacje dotyczące przejęcia znaczącej części udziałów Krajowego Biura Informacji Kredytowej Sp. z o.o. przez Krajowy Rejestr Długów BIG S.A.
17.	Minister Pracy i Polityki Społecznej	28.07.2011 DOLiS-035-2170/11	Wystąpienie do Ministra Pracy i Polityki Społecznej z prośbą o rozważenie możliwości zainicjowania przez MPiPS prac legislacyjnych w celu unormowania w przepisach rangi ustawowej zasad pozyskiwania oraz określenie zakresu danych osobowych przetwarzanych w procesie rekrutacji do żłobków dzieci w wieku do lat 3.
18.	Prezes Urzędu Komunikacji Elektronicznej	10.08.2011 DOLiS-035-2305/11	Wystąpienie do Prezesa Urzędu Komunikacji Elektronicznej w sprawie nieprawidłowości we właściwym zabezpieczeniu skrzynek pocztowych w miejscowości Barchanie woj. kujawsko-pomorskie.
19.	Komendant Wojewódzkiej Policji w Kielcach	23.08.2011 DOLiS-035-2399/11	Wystąpienie do Komendanta Wojewódzkiej Policji w Kielcach w sprawie dotyczącej ochrony danych osobowych osób zatrzymanych, zawartych w BIP

			Komendy w związku ze sprawozdaniem z kontroli w 2010 r.
20.	Minister Nauki i Szkolnictwa Wyższego	23.08.2011 DOLiS-035-2410/11	Wystąpienie do Ministra Nauki i Szkolnictwa Wyższego (oraz do wiadomości Prezesa ZUS) o podjęcie działań mających na celu zapobieżenie pozyskiwania danych osobowych absolwentów przez wyższe uczelnie lub podmioty działające na ich zlecenie.
21.	Minister Pracy i Polityki Społecznej	25.08.2011 DOLiS-035-2427/11	Wystąpienie do Ministra Pracy i Polityki Społecznej z prośbą o podjęcie prac legislacyjnych zmierzających do zmiany obowiązującego wzoru załącznika nr 1, część C do rozporządzenia Ministra Pracy i Polityki Społecznej w sprawie rejestracji bezrobotnych i poszukujących pracy.
22.	Minister Zdrowia	30.08.2011 DOLiS-035-2464/11	Wystąpienie do Ministra Zdrowia z prośbą o podjęcie prac legislacyjnych mających na celu wprowadzenie podstaw prawnych dla zlecenia informatycznej obsługi procesu przetwarzania danych osobowych przez administratorów danych przetwarzających dane osobowe pacjentów, w związku z udzielaniem świadczeń zdrowotnych innym wyspecjalizowanym w tym zakresie podmiotom.
23.	Minister Nauki i Szkolnictwa Wyższego	03.11.2011 DOLiS-035-3221/11	Wystąpienie do Ministra Nauki i Szkolnictwa Wyższego z prośbą o podjęcie prac legislacyjnych mających na celu zmianę znowelizowanej ustawy o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki oraz rozporządzenia MNiSW w sprawie szczegółowego trybu i warunków przeprowadzenia czynności w przewodach doktorskich, postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora.
24.	Minister Finansów	29.11.2011 DOLiS-035-3484/11	Wystąpienie do Ministra Finansów z prośbą o podjęcie prac legislacyjnych w celu zmiany przepisu ustawy o finansach publicznych, dotyczącego zasad podawania do publicznej wiadomości informacji o osobach prawnych i fizycznych oraz jednostkach organizacyjnych nieposiadających osobowości prawnej, którym w zakresie podatków lub opłat udzielono ulg, odroczeń, umorzeń lub rozłożono spłatę raty na raty w kwocie przewyższającej łącznie 500 zł, wraz z wskazaniem wysokości umorzonych kwot i przyczyn umorzenia.
25.	Powiatowy Urząd Pracy w Kętrzynie	01.12.2011 DOLiS-440-1122/11	Wystąpienie do Dyrektora Powiatowego Urzędu Pracy w Kętrzynie dotyczące sposobu organizacji wypłacania zasiłku osobom bezrobotnym przez PUP w Kętrzynie (tj. tworzenia zbiorczej listy osób uprawnionych do wypłaty zasiłku)
26.	Minister Finansów	14.12.2011 DOLiS-035-3716/11	Wystąpienie do Ministra Finansów z prośbą o podjęcie prac legislacyjnych w celu zmiany przepisów ustawy o podatku od towarów i usług dotyczących zwolnienia z podatku VAT usług w zakresie opieki medycznej.
27.	Minister Administracji i Cyfryzacji	23.12.2011 DOLiS-035-42/11	Wystąpienie do Ministra Administracji i Cyfryzacji z prośbą o podjęcie inicjatywy ustawodawczej celem uregulowania kwestii usuwania informacji publicznych zamieszczanych w sieci Internet.
28.	Minister Gospodarki	29.12.2011 DOLiS-035-3868/11	Wystąpienie do Ministra Gospodarki w sprawie ujednolicenia przepisów oraz formularza CEIDG-1.

**Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych
w roku 2011 do podmiotów prywatnych**

L.p.	Nazwa podmiotu, do którego skierowano wystąpienie	Data wystąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	Blue Media S.A. Sopot	18.01.2011 DOLiS-035-107/11	Wystąpienie do Blue Media S.A. Sopot w sprawie regulaminu konkursu „Gorączka złota”.
2.	Katowickie Towarzystwo Budownictwa Społecznego Sp. z o.o.	11.02.2011 DOLiS-035-381/11	Wystąpienie do Katowickiego Towarzystwa Budownictwa Społecznego Sp. z o.o. w sprawie nieprawidłowości przekazywania rozliczeń czynszów.
3.	TNT Express Worldwide (Poland) Sp. z o.o.	15.02.2011 DOLiS-035-420/11	Wystąpienie do TNT Express Worldwide (Poland) Sp. z o.o. w kwestii związanej ze sposobem doręczania przez kurierów korespondencji.
4.	Gold's Gym Fitness & Wellness Centrum Rezydencja Królewska Warszawa	15.02.2011 DOLiS-035-421/11	Wystąpienie do Gold's Gym Fitness & Wellness Center Rezydencja Królewska Warszawa dotyczyło pozyskiwania za pośrednictwem formularza „Bez członkostwa” i „Karta Gościa” danych osób korzystających z usług świadczonych przez sieć klubów.
5.	Świat Zdrowia S.A. Toruń	16.02.2011 DOLiS-035-433/11	Wystąpienie do Świat Zdrowia S.A. Toruń w sprawie pozyskiwania przez jedną z aptek danych osobowych w postaci numerów NIP, klientów apteki uczestniczących w programie lojalnościowym Świat Zdrowia.
6.	Hrtec Sp. z o.o. Gdynia	10.03.2011 DOLiS-035-691/11	Wystąpienie do Hrtec Sp. z o.o. Gdynia z prośbą o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych osobowych do wymogów ustawy o ochronie danych osobowych w związku ze stosowanym formularzem zapisu na audytora www.ebiznes.ocdl.pl .
7.	Praktiker Polska Sp. z o.o.	24.05.2011 DOLiS-440-458/11	Wystąpienie do Praktiker Polska Sp. z o.o. w kwestii wymaganej od klientów zbyt dużej ilości danych osobowych przy zakupie oleju opałowego.
8.	Super Pharm Poland Sp. z o.o.	05.07.2011 DOLiS-035-1973/11	Wystąpienie do Super Pharm Poland Sp. z o.o. dotyczące nieprawidłowości w sformułowanej zgodzie na przetwarzanie danych klientów chcących wziąć udział w programie lojalnościowym Klub LifeStyle.
9.	NZOZ Mulimedis Kraków	21.07.2011 DOLiS-440-676/11	Wystąpienie do NZOZ Mulimedis Kraków w sprawie pozyskiwania za pomocą formularza „opis warunków rodzinno–środowiskowych „danych osobowych pacjenta zapisującego się na wizytę do lekarza w zakresie sytuacji majątkowej i rodzinnej”.
10.	Grupa Onet.pl Kraków	22.07.2011 DOLiS-440-677/11	Wystąpienie do Grupy Onet.pl Kraków w sprawie przetwarzania danych osobowych użytkowników portalu internetowego sympatia.pl .
11.	Centrum Zdrowia i Urody	02.09.2011	Wystąpienie o wyeliminowanie nieprawidłowości

	Orchid	DOLiS-440-608/11	w procesie przetwarzania danych bez podstawy prawnej.
12.	LOT S.A.	08.09.2011 DOLiS-440-824/11	Wystąpienie do LOT S.A. dotyczące konieczności okazania dowodów osobistych/paszportów małoletnich dzieci, których rodzice wraz z nimi chcą skorzystać z krajowej podróży samolotem.
13.	Spółdzielnia Mieszkaniowa w Ciechocinku	16.09.2011 DOLiS-440-1039/11	Wystąpienie w sprawie wyeliminowania praktyki udostępniania danych osobowych bez podstaw prawnych.
14.	BRE Bank S.A.	30.09.2011 DOLiS-440-362/11	Wystąpienie w sprawie zastosowania odpowiednich środków technicznych i organizacyjnych celem zabezpieczenia danych osobowych.
15.	LUX – DOM Sp. z o.o.	18.10.2011 DOLiS-440-573/11	Wystąpienie w sprawie niewywieszania w przyszłości na klatkach schodowych danych osobowych członków wspólnoty mieszkaniowej.
16.	Open Finanse S.A.	26.10.2011 DOLiS-440-998/11	Wystąpienie do Open Finanse S.A. dotyczące przetwarzania danych osobowych przez ten podmiot.
17.	Polish Soccer Skills	28.10.2011 DOLiS-440-948/11	Wystąpienie do Polish Soccer Skills dotyczące regulaminu.
18.	FS Holding S.A.	3.11.2011 DOLiS-440-634/11	Wystąpienie do FS Holding S.A. o wyeliminowanie nieprawidłowości przy przetwarzaniu danych osobowych w celach marketingowych.
19.	Vital Park Sp. z o.o.	9.11.2011 DOLiS-440-571/11	Wystąpienie w sprawie zaprzestania praktyki polegającej na udostępnianiu danych osobowych zadłużonych mieszkańców osiedla osobom nieupoważnionym.
20.	Spółdzielnia Mieszkaniowa „Nowe Miasto”	7.12.2011 DOLiS-440-193/11	Wystąpienie w sprawie wyeliminowania praktyki udostępniania informacji o sprawach sądowych z udziałem lokatorów osobom nieupoważnionym.
21.	Deutsche Bank PBC S.A.	30.12.2011 DOLiS-440-773/09	Wystąpienie w sprawie wprowadzenia odpowiednich zabezpieczeń danych przed ich dostępem osobom nieupoważnionym.

Wykaz kontroli przeprowadzonych w 2011 r.

L.p.	Data / Sygnatura kontroli	Nazwa i miejsce podmiotu kontrolowanego	Inicjatywa kontroli	Rozstrzygnięcie oraz/lub data i sygnatura decyzji
1.	11-13.01.2011 DIS-K-421/1/11	Klub Piłkarski Legia Warszawa S.S.A., Warszawa, ul. Łazienkowska 3	DOLiS	03.08.2011 decyzja DIS/DEC-651/37118/11
2.	11.01.2011 DIS-K-421/2/11	PFG Partnerzy Kancelaria Finansowa Sp. z o.o., Warszawa, ul. Aroniowa 14	DOLiS	nie stwierdzono uchybień
3.	11-14.01.2011 DIS-K-421/3/11	Jobland Sp. z o.o., Warszawa, ul. Sezamkowa 18,	Z urzędu	22.08.2011 decyzja DIS/DEC-688/39620/11
4.	12-14.01.2011 DIS-K-421/4/11	Szkoła Główna Handlowa w Warszawie, Al. Niepodległości 162	w związku z kontrolą DIS-K- 421/150/10	06.06.2011 decyzja DIS/DEC-453/26460/11
5.	12-14.01.2011 DIS-K-421/5/11	ESTIS Sp. z o.o., Warszawa, ul. Bonifraterska 17	DOLiS	01.09.2011 decyzja DIS/DEC-762/41629/11
6.	17-20.01.2011 DIS-K-421/6/11	Start People Sp. z o.o., Warszawa, ul. Grzybowska 77	Z urzędu	03.08.2011 decyzja DIS/DEC-650/37116/11
7.	17-19.01.2011 DIS-K-421/7/11	First Data Polska S.A., Warszawa, Al. Jerozolimskie 92	w związku z kontrolą DIS-K- 421/171/10	nie stwierdzono uchybień
8.	18-21.01.2011 DIS-K-421/8/11	Grafton Recruitment Polska Sp. z o.o., Warszawa, ul. Sienna 39	Z urzędu	nie stwierdzono uchybień
9.	18-21.01.2011 DIS-K-421/9/11	Zakład Doskonalenia Zawodowego w Warszawie, ul. Podwałe 13	Z urzędu	10.03.2011 decyzja DIS/DEC-191/10390/11
10.	24-28.01.2011 DIS-K-421/10/11	Prezydent Miasta Wrocławia - Urząd Miejski Wrocławia, Wrocław, Pl. Nowy Targ 1/8	Z urzędu	11.07.2011 decyzja DIS/DEC-560/32587/11
11.	24-27.01.2011 DIS-K-421/11/11	Stefan Wałęka prowadzący działalność gospodarczą pod nazwą „Agencja Capital Stefan Wałęka”, Warszawa, ul. Orzycka 24/7	Z urzędu	03.06.2011 decyzja DIS/DEC-449/26359/11
12.	25-28 i 31.01.2011 DIS-K-421/12/11	Polski Związek Piłki Siatkowej, Warszawa, ul. Grażyny 13	DOLiS	15.06.2011 decyzja DIS/DEC-490/28474/11
13.	25-27.01.2011 DIS-K-421/13/11	Małgorzata Radzikowska prowadząca działalność gospodarczą pod nazwą „Perfect Care24 Małgorzata Radzikowska”, Warszawa, ul. Świętokrzyska 18/209	Z urzędu	przywrócono stan zgodny z prawem
14.	25-28.01.2011 DIS-K-421/14/11	Grupa Pracuj Sp. z o.o., Warszawa, ul. Prosta 51	Z urzędu	19.12.2011 decyzja DIS/DEC-1063/61951/11
15.	25-27.01.2011 DIS-K-421/15/11	Jarosław Malec prowadzący działalność gospodarczą pod nazwą „MEMEX Jarosław Malec”, Piaseczno, ul. Warszawska 32c lok. 36	DROZD	nie stwierdzono uchybień
16.	26-28.01.2011 i 09.02.2011 DIS-K-421/16/11	Mennica Polska S.A. - Biuro Obsługi Klienta, Wrocław, ul. Grabiszyńska 9	w związku z kontrolą DIS-K- 421/10/11	nie stwierdzono uchybień
17.	01-04.02.2011 DIS-K-421/17/11	HR Progress Sp. z o.o., Warszawa, ul. Arkuszowa 39	z urzędu	13.06.2011 decyzja DIS/DEC-474/27860/11
18.	02-03.02.2011 DIS-K-421/18/11	Sygma Banque Societe Anonyme (Spółka Akcyjna) Oddział w Polsce, Warszawa, ul. Suwak 3	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
19.	02-04.02.2011 DIS-K-421/19/11	Szkoła Główna Gospodarstwa Wiejskiego w Warszawie, Warszawa, ul. Nowoursynowska 166	w związku z kontrolą DIS-K- 421/150/10	26.05.2011 decyzja DIS/DEC-410/24576/11
20.	03.02.2011 DIS-K-421/20/11	Szef Urzędu do Spraw Cudzoziemców Warszawa, ul. Koszykowa 16	DOLiS	wnioski przekazano do Departamentu Orzecznictwa,

				Legislacji i Skarg
21.	07-09.02.2011 DIS-K-421/21/11	Call Center Poland S.A., Warszawa, ul. Marynarska 11	w związku z kontrolą DIS-K- 421/152/10	nie stwierdzono uchybień
22.	07-11.02.2011 DIS-K-421/22/11	Anna Suchecka prowadząca działalność gospodarczą pod nazwą „AS”, Częstochowa, ul. Michałowskiego 22/9	z urzędu	10.05.2011 decyzja DIS/DEC-353/21603/11
23.	07-11.02.2011 DIS-K-421/23/11	BRE Bank S.A., Warszawa, ul. Senatorska 18 i Łódź, ul. Mickiewicza 10 i Al. Piłsudskiego 3	DOLiS	nie stwierdzono uchybień
24.	07-11.02.2011 DIS-K-421/24/11	Trinity Management Sp. z o.o. Lublin, ul. Kołłątaja 3/15	z urzędu	przywrócono stan zgodny z prawem
25.	10-11.02.2011 DIS-K-421/25/11	ITI Neovision Sp. z o.o. Warszawa, ul. Kłobucka 23	w związku z kontrolą DIS-K- 421/185/10	18.05.2011 decyzja DIS/DEC-375/22957/11
26.	14-18.02.2011 DIS-K-421/26/11	Anna Droś prowadząca działalność gospodarczą pod nazwą „Better HR Anna Droś”, Poznań, ul. Piękna 59 lok. 3	z urzędu	26.05.2011 decyzja DIS/DEC-411/24579/11
27.	15-17.02.2011 DIS-K-421/27/11	Zakład Handlowo - Usługowy Henryk Fendorf & Tomasz Fendorf sp.j. Głogów, ul. Galileusza 18	DOLiS	nie stwierdzono uchybień
28.	14-15.02.2011 DIS-K-421/28/11	Iwona Tomzik prowadząca działalność gospodarczą pod nazwą „ArtFLORA Tomzik Iwona”, Katowice, ul. Markiefki 92	z urzędu	nie stwierdzono uchybień
29.	14 i 16.02.2011 DIS-K-421/29/11	Artur Bińczyk, Warszawa, ul. Wolska 81/39	DRZDO	12.05.2011 decyzja DIS/DEC-365/22004/11
30.	15-17.02.2011 DIS-K-421/30/11	Hanna Puzewicz prowadząca działalność gospodarczą pod nazwą „Biuro rachunkowe”, Warszawa, ul. Herbsta 1	z urzędu	nie stwierdzono uchybień
31.	23-25.02.2011 DIS-K-421/31/11	Truecore Solutions s. c. Łukasz Pikuła, Krystian Parka, Warszawa, ul. Przy Łasku 1/26	z urzędu	nie stwierdzono uchybień
32.	21-23.02.2011 DIS-K-421/32/11	Adam Kaczorowski prowadzący działalność gospodarczą pod firmą „Prowork Adam Kaczorowski”, Warszawa, ul. Smolna 38/8	z urzędu	13.06.2011 decyzja DIS/DEC-476/27863/11
33.	22-25.02.2011 DIS-K-421/33/11	Simplika Sp. z o.o., Warszawa, ul. Wspólna 50A lok. 22	z urzędu	12.05.2011 decyzja DIS/DEC-364/22002/11
34.	23-25.02.2011 DIS-K-421/34/11	Marszałek Województwa Mazowieckiego - Urząd Marszałkowski Województwa Mazowieckiego, Warszawa, ul. Jagiellońska 26	z urzędu	przywrócono stan zgodny z prawem
35.	23-25.02.2011 DIS-K-421/35/11	Anna Kukła - Gryz prowadząca działalność gospodarczą pod nazwą „Exvena Anna Kukła – Gryz”, Warszawa, ul. Wyspiańskiego 5 m 52	DRZDO	21.06.2011 decyzja DIS/DEC-504/29526/11
36.	07-09.03.2011 DIS-K-421/36/11	Polskie Linie Lotnicze „LOT”, Warszawa, ul. 17 Stycznia 39	DOLiS	13.06.2011 decyzja DIS/DEC-477/27867/11
37.	07-11.03.2011 DIS-K-421/37/11	Politechnika Śląska, Gliwice, ul. Akademicka 2A	z urzędu	11.07.2011 decyzja DIS/DEC-559/32585/11
38.	08-10.03.2011 DIS-K-421/38/11	Panterra Sp. z o.o. Spółka Komandytowa, Warszawa, Al. Jana Pawła II 29	z urzędu	29.04.2011 decyzja DIS/DEC-338/20025/11
39.	08-10.03.2011 DIS-K-421/39/11	DHL Express (Poland) Sp. z o.o. Warszawa, ul. Osmańska 2	DOLiS	przywrócono stan zgodny z prawem

40.	14-17.03.2011 DIS-K-421/40/11	GG Network S.A., Warszawa, ul. Kamionkowska 45	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
41.	14-16.03.2011 i 06.04.2011 DIS-K-421/41/11	Grupa o2 Sp. z o.o. Warszawa, ul. Jutrzenki 177	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
42.	14-17.03.2011 DIS-K-421/42/11	VICTOR G. Górak i Wspólnicy Sp. j., Kraków, Al. Pokoju 81C lok. 68	z urzędu	03.08.2011 decyzja DIS/DEC-652/37121/11
43.	14-17.03.2011 DIS-K-421/43/11	Wspólnota Mieszkaniowa „Apartamenty Krakowskie Cztery Korony”, Kraków, ul. Pilotów 2D	DOLiS	13.06.2011 decyzja DIS/DEC-478/27870/11
44.	14-17.03.2011 DIS-K-421/44/11	Ernst & Young Sp. z o.o. Warszawa, rondo ONZ 1	z urzędu	nie stwierdzono uchybień
45.	16-18.03.2011 DIS-K-421/45/11	ESTIS Sp. z o.o., Warszawa, ul. Bonifraterska 17	w związku z kontrolą DIS- K-421/5/11	materiał dowodowy wykorzystano w kontroli DIS-K-421/5/11
46.	21-22.03.2011 DIS-K-421/46/11	Kodop - Consulting Spółka Doradztwa Podatkowego Sp. z o.o., Warszawa, ul. Widok 5/7/9	z urzędu	nie stwierdzono uchybień
47.	21-25.03.2011 DIS-K-421/47/11	Michał Chrzęszcz (forum.siechnice.com.pl), Siechnice, ul. Jarzębinowa 3/4	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
48.	21-23.03.2011 DIS-K-421/48/11	Spółka Doradztwa Podatkowego „Manugiewicz, Trzaska i Wspólnicy” Sp. z o.o., Warszawa, ul. Księżykowa 66B	z urzędu	nie stwierdzono uchybień
49.	28.03.2011 DIS-K-421/49/11	242 Group Sp. z o.o., Warszawa, ul. Opaczewska 43 lok. 21	z urzędu	nie stwierdzono uchybień
50.	28-30.03.2011 DIS-K-421/50/11	RF Finans Sp. z o.o., Warszawa, ul. Grochowska 326 lok. 8	z urzędu	03.06.2011 decyzja DIS/DEC-447/26291/11
51.	28.03-01.04.2011 DIS-K-421/51/11	Kancelaria Doradztwa Podatkowego Gawrychowska & Nierzwicka Sp. z o.o., Gdańsk, ul. Żeglarska 4	z urzędu	13.06.2011 decyzja DIS/DEC-475/27861/11
52.	28.03-01.04.2011 DIS-K-421/52/11	Actif Consulting Sp. z o.o. Kraków, ul. Jabłonowskich 8	z urzędu	nie stwierdzono uchybień
53.	28.03-01.04.2011 DIS-K-421/53/11	Niepubliczny Zakład Opieki Zdrowotnej „Medi – Spatz” Szalsza, ul. Wiejska 4	z urzędu	25.08.2011 decyzja DIS/DEC-715/40244/11
54.	06-07.04.2011 DIS-K-421/54/11	Reader`s Digest Przegląd Sp. z o.o. Warszawa, ul. Taśmowa 7	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
55.	06-07.04.2011 DIS-K-421/55/11	Grupa Pracuj Sp. z o.o. Warszawa, ul. Prosta 51	w związku z kontrolą DIS-K- 421/14/11	materiał dowodowy wykorzystany w kontroli DIS-K-421/14/11
56.	06-08.04.2011 DIS-K-421/56/11	Raiffeisen Financial Services Polska Sp. z o.o., Warszawa, Al. Jerozolimskie 179	Prokuratura Rejonowa w Chorzowie	22.09.2011 DIS/DEC-820/45360, 45362/11
57.	06-07.04.2011 DIS-K-421/57/11	Info Veriti Polska Sp. z o.o. Obsługa Serwisu Internetowego Sp. j. Warszawa, ul. Serwituty 23	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
58.	06-08.04.2011 DIS-K-421/58/11	Ministerstwo Skarbu Państwa, Warszawa, ul. Krucza 36	Najwyższa Izba Kontroli	brak przetwarzania danych osobowych w poddanym kontroli systemie informatycznym
59.	11-14.04.2011 DIS-K-421/59/11	SOLID MCG Sp. z o.o. Warszawa, ul. Postępu 2	DOLiS	08.09.2011 decyzja DIS/DEC-778/42886/11
60.	11-15.04.2011 DIS-K-421/60/11	Grupa Allegro Sp. z o.o. Poznań, ul. Marcelińska 90	DOLiS	11.07.2011 decyzja DIS/DEC-558/32582/11
61.	11-15.04.2011 DIS-K-421/61/11	Wójt Gminy Wejherowo - Urząd Gminy Wejherowo, Wejherowo, Oś. Przyjaźni 6	DOLiS	przywrócono stan zgodny z prawem

62.	12-15.04.2011 DIS-K-421/62/11	Marciniuk i Wspólnicy Sp. z o. o. - Spółka Doradztwa Podatkowego, Warszawa, Al. Szucha 13/15	z urzędu	11.07.2011 decyzja DIS/DEC-561/32592/11
63.	13-22.04.2011 DIS-K-421/63/11	Główny Urząd Statystyczny, Warszawa, Al. Niepodległości 208	z urzędu	w toku
64.	18-19.04.2011 DIS-K-421/64/11	Ekstraklasa S.A., Warszawa, ul. Wybrzeże Gdynskie 6d	w związku z kontrolami DIS- K-421/5/11 i DIS-K- 421/44/11	05.09.2011 decyzja DIS/DEC-770/42047/11
65.	18-22.04.2011 DIS-K-421/65/11	Aleksandra Gortych prowadząca działalność gospodarczą pod nazwą „Kancelaria Podatkowa WIOL”, Łódź, Al. Kościuszki 23/25	z urzędu	22.06.2011 decyzja DIS/DEC-512/29903/11
66.	18-22.04.2011 DIS-K-421/66/11	Profit Doradcy Finansowi Sp. z o.o. Łódź, Al. Kościuszki 71	z urzędu	nie stwierdzono uchybień
67.	18-19.04.2011 DIS-K-421/67/11	Telewizja Polsat S.A., Warszawa, ul. Ostrobramska 77	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
68.	09-13.05.2011 DIS-K-421/69/11	Wielkopolski Dom Finansowy Sp. z o.o., Bydgoszcz, ul. Krasińskiego 19	z urzędu	nie stwierdzono uchybień
69.	12-13.05.2011 DIS-K-421/70/11	Sebastian Gneciecki prowadzący działalność gospodarczą pod nazwą „Usługi internetowe Revenue Sebastian Gneciecki”, Warszawa, ul. Kasprzaka 29/31 lok. 213	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
70.	10-12.05.2011 DIS-K-421/71/11	Google Inc., Warszawa, ul. E. Plater 53	z urzędu	01.12.2011 decyzja DIS/DEC-1020/58246/11
71.	16-20.05.2011 DIS-K-421/72/11	Homefinance Sp. z o.o., Lublin, ul. Krakowskie Przedmieście 17	z urzędu	nie stwierdzono uchybień
72.	16-20.05.2011 DIS-K-421/73/11	Agnieszka Olbryś prowadząca działalność gospodarczą pod nazwą „OPI Biuro Rachunkowości i Finansów”, Gliwice, ul. Jasna 28	z urzędu	nie stwierdzono uchybień
73.	16-19.05.2011 DIS-K-421/74/11	Sąd Okręgowy Warszawa - Praga w Warszawie - VII Wydział Pracy i Ubezpieczeń, Warszawa, Al. Solidarności 127	z urzędu	25.10.2011 decyzja DIS/DEC-894/51260/11
74.	16-20.05.2011 DIS-K-421/75/11	Xelion. Doradcy Finansowi Sp. z o. o. Warszawa, ul. Puławska 107	z urzędu	16.11.2011 decyzja DIS/DEC-967/55196/11
75.	23-25.05.2011 DIS-K-421/76/11	Główny Urząd Statystyczny, Warszawa, Al. Niepodległości 208	DOLiS	nie stwierdzono uchybień
76.	24-27.05.2011 DIS-K-421/77/11	Open Finance S.A., Warszawa, ul. Domaniewska 39	z urzędu	05.10.2011 decyzja DIS/DEC-849/47675/11
77.	24-27.05.2011 DIS-K-421/78/11	Bożena Klepek prowadząca działalność gospodarczą pod nazwą „Dialog Bożena Klepek”, Mikołów, ul. Wincentego Bromboszcza 11	z urzędu	25.08.2011 decyzja DIS/DEC-716/40255/11
78.	24-27.05.2011 DIS-K-421/79/11	Prezydent Miasta Stołecznego Warszawy - Urząd Dzielnicy Warszawa Śródmieście, Warszawa, ul. Nowogrodzka 43	DOLiS	25.10.2011 decyzja DIS/DEC-895/51326/11
79.	23-27.05.2011 DIS-K-421/80/11	Expander Advisors Sp. z o.o. Warszawa, ul. Domaniewska 50A	z urzędu	nie stwierdzono uchybień
80.	06-10.06.2011 DIS-K-421/81/11	Poli Invest Sp. z o.o., Suwałki, ul. Emilii Plater 5/7	DRZDO	08.09.2011 DIS/DEC-777/42869/11
81.	06-09.06.2011 DIS-K-421/82/11	Warszawski Ośrodek Sportu i Rekreacji, Warszawa, ul. Rozbrat 26	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
82.	07-10.06.2011 DIS-K-421/83/11	Bioton S.A., Macierzysz, ul. Poznańska 12	w związku z kontrolą DIS-K-	nie stwierdzono uchybień

			421/15/11	
83.	06-08.06.2011 DIS-K-421/84/11	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
84.	06-08.06.2011 DIS-K-421/85/11	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
85.	13-14.06.2011 DIS-K-421/86/11	Jarosław Malec prowadzący działalność gospodarczą pod nazwą „MEMEX Jarosław Malec”, Piaseczno, ul. Warszawska 32c lok. 36	w związku z kontrolą DIS-K- 421/15/11	nie stwierdzono uchybień
86.	13-17.06.2011 DIS-K-421/87/11	Spółdzielnia Mieszkaniowa w Parczewie, Parczew, ul. Spółdzielcza 13A	z urzędu	21.10.2011 decyzja DIS/DEC-884/50681/11
87.	13-17.06.2011 DIS-K-421/88/11	Ośrodek Sportu i Rekreacji Bytom, ul. Parkowa 1	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
88.	13-15.06.2011 DIS-K-421/89/11	Med Casco Sp. z o.o., Warszawa, ul. Emilii Plater 53	DRZDO	nie stwierdzono uchybień
89.	14-17-06-2011 DIS-K-421/90/11	Klub Sportowy Polonia Bytom S.A., Bytom, ul. Piekarska 5	z urzędu	19.12.2011 decyzja DIS/DEC-1064/61954/11
90.	14-17.06.2011 DIS-K-421/91/11	Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m. st. Warszawie S.A., Warszawa, Pl. Starynkiewicza 5	z urzędu	19.09.2011 decyzja DIS/DEC-808/44667/11
91.	27.06-01.07.2011 DIS-K-421/92/11	Gimnazjum nr 1 w Tucholi Tuchola, ul. Piastowska 23	DOLiS	nie stwierdzono uchybień
92.	27.06-01.07.2011 DIS-K-421/93/11	Miejski Ośrodek Sportu i Rekreacji, Łódź, ul. Ks. Skorupki 21	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
93.	27.06-01.07.2011 DIS-K-421/94/11	Miejski Ośrodek Sportu i Rekreacji w Zabrzu Sp. z o.o., Zabrze, ul. Matejki 6	z urzędu	nie stwierdzono uchybień
94.	27.06-01.07.2011 DIS-K-421/95/11	Wojewódzki Szpital Specjalistyczny im. F. Chopina, Rzeszów, ul. Chopina 2	Prokuratura Okręgowa w Rzeszowie	02.12.2011 decyzja DIS/DEC-1025/58622/11
95.	27.06-01.07.2011 DIS-K-421/96/11	Łódzki Klub Sportowy S.A. Łódź, Al. Unii Lubelskiej 2	z urzędu	16.01.2012 DIS/DEC-45/12/2550
96.	29.06.2011 DIS-K-421/97/11	Paweł Tkaczyk (terazpraca.pl) Mińsk Mazowiecki, ul. Topolowa 17/24	z urzędu	ustalenia przekazano do Komendy Główniej Policji
97.	04-08.07.2011 DIS-K-421/98/11	Prezydent Miasta Białystok - Urząd Miasta Białystok, Białystok, ul. Słonimska 1	DOLiS	19.09.2011 decyzja DIS/DEC-804/44522/11
98.	05-08.07.2011 DIS-K-421/99/11	Górniki Zabrze Sportowa Spółka Akcyjna, Zabrze, ul. Roosevelta 81	z urzędu	11.01.2012 DIS/DEC-30/12/1718
99.	06-08.07.2011 DIS-K-421/100/11	Kupiec Warszawski Sp. z o.o. Warszawa, ul. Marywilska 44 lok. 4C	DOLiS	nie stwierdzono uchybień
100.	06.07.2011 DIS-K-421/101/11	Info Veriti Polska Sp. z o.o. Obsługa Serwisu Internetowego Sp. j. Warszawa, ul. Serwituty 23	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
101.	06.07.2011 DIS-K-421/102/11	Info Veriti Polska Sp. z o.o. Obsługa Serwisu Internetowego Sp. j. Warszawa, ul. Serwituty 23	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
102.	11-14.07.2011 DIS-K-421/103/11	EFG Eurobank Ergasias S.A. Spółka Akcyjna Oddział w Polsce Warszawa, ul. Mokotowska 19	DOLiS	nie stwierdzono uchybień
103.	12-14.07.2011 DIS-K-421/104/11	Solid Security Sp. z o.o. Warszawa, ul. Postępu 2	w związku z kontrolą DIS-K- 421/59/11	ustalenia wykorzystano w kontroli DIS-K-421/59/11
104.	12-15.07.2011 DIS-K-421/105/11	Andrzej Kosieradzki prowadzący działalność gospodarczą pod nazwą	DOLiS	wnioski przekazano do Departamentu Orzecznictwa,

		„GoWork.pl Andrzej Kosieradzki” Warszawa, ul. ul. Żurawia 47/49		Legislacji i Skarg
105.	12-15.07.2011 DIS-K-421/106/11	Krajowa Rada Izb Rolniczych, Warszawa, ul. Wspólna 30	DOLiS	nie stwierdzono uchybień
106.	18-20.07.2011 DIS-K-421/107/11	Komenda Główna Policji, Warszawa, ul. Puławska 148/150	w związku z kontrolą DIS-K- 421/44/11	21.10.2011 decyzja DIS/DEC-883/50669/11
107.	19-22.07.2011 DIS-K-421/108/11	Polski Holding Nieruchomości S.A. Warszawa, ul. Świętokrzyska 36	DOLiS	20.09.2011 decyzja DIS/DEC-816/44889, 44891/11
108.	25-29.07.2011 DIS-K-421/109/11	Zakład Elektroniki Górniczej "ZEG" S.A., Tychy, ul. Burschego 3	DOLiS	16.02.2012 zawiadomienie o przestępstwie DIS/ZAW-2/12/10355
109.	25-29.07.2011 DIS-K-421/110/11	Wrocławski Klub Sportowy „Śląsk Wrocław” S.A., Wrocław, ul. Oporowska 62	z urzędu	22.12.2011 decyzja DIS/DEC-1078/63085/11
110.	25-29.07.2011 DIS-K-421/111/11	Komornik Sądowy przy Sądzie Rejonowym w Lubaczowie, Kancelaria Komornicza, Lubaczów, ul. Unii Lubelskiej 6	DOLiS	14.11.2011 decyzja DIS/DEC-964/54638/11
111.	25-28.07.2011 DIS-K-421/112/11	KSP Polonia Warszawa Sportowa S.A., Warszawa, ul. Konwiktorska 6	z urzędu	30.12.2011 DIS/DEC-1110/64638/11
112.	25-29.07.2011 DIS-K-421/113/11	Główny Inspektor Transportu Drogowego, Warszawa, ul. Postępu 21	z urzędu	nie stwierdzono uchybień
113.	03-05.08.2011 DIS-K-421/114/11	Burmistrz Gminy Konstancin - Jeziorna, Konstancin - Jeziorna, ul. Warszawska 32	z urzędu	20.12.2011 decyzja DIS/DEC-1069/62252/11
114.	03-05.08.2011 DIS-K-421/115/11	Prezydent Miasta Legionowo – Urząd Miasta Legionowo Legionowo, ul. Piłsudskiego 41	z urzędu	19.20.2011 decyzja DIS/DEC-1065/61961/11
115.	03-05.08.2011 DIS-K-421/116/11	Polskapresse Sp. z o.o., Warszawa, ul. Domaniewska 41	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
116.	08-12.08.2011 DIS-K-421/117/11	Powiatowy Urząd Pracy w Gryficach Gryfice, ul. Koszarowa 4	DOLiS	nie stwierdzono uchybień
117.	10-11.08.2011 DIS-K-421/118/11	Krajowe Biuro Informacji Kredytowej Sp. z o.o., Warszawa, ul. Krzywickiego 34	DOLiS	w toku
118.	09-12.08.2011 DIS-K-421/119/11	Polska Telefonía Cyfrowa Sp. z o.o. Warszawa, Al. Jerozolimskie 181	z urzędu	nie stwierdzono uchybień
119.	09-12.08.2011 DIS-K-421/120/11	Polkomtel S.A., Warszawa, ul. Postępu 3	z urzędu	nie stwierdzono uchybień
120.	16-19.08.2011 DIS-K-421/121/11	Centrum Organizacyjno - Koordynacyjne do Spraw Transplantacji "Poltransplant", Warszawa, Al. Jerozolimskie 87	DOLiS	12.03.2012 DIS/DEC-201/12/15307
121.	17-19.08.2011 DIS-K-421/122/11	Polska Telefonía Komórkowa Centertel Sp. z o.o. Warszawa, ul. Skierniewicka 10A	z urzędu	nie stwierdzono uchybień
122.	18-19.08.2011 DIS-K-421/123/11	P4 Sp. z o.o. Warszawa, ul. Taśmowa 7	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
123.	22-26.08.2011 DIS-K-421/124/11	Scanmed Multimedias S. A. - Niepubliczny Zakład Opieki Zdrowotnej Multimedias, Warszawa, ul. Armii Krajowej 5	z urzędu	nie stwierdzono uchybień
124.	29.08. - 02.09.2011 DIS-K-421/125/11	Szpital Wojewódzki im. Św. Łukasza SPZOZ w Tarnowie Tarnów, ul. Lwowska 178a	DOLiS	22.08.2011 DIS/ZAW-7/39615 06.03.2012 DIS/DEC-174/12/14274
125.	29-30.08.2011 DIS-K-421/126/11	ASTEK Polska Sp. z o.o., Warszawa, Al. Jana Pawła II 15	DOLiS	28.12.2011 decyzja DIS/DEC-1093/63919/11

126.	29.08. - 02.09.2011 DIS-K-421/127/11	Rafał Bartkowiak prowadzący działalność gospodarczą pod firmą "Agencja promocyjna Locco Event Rafał Bartkowiak", Poznań, ul. Węgorka 20	Departament Informatyki	28.11.2011 decyzja DIS/DEC-1010/57440/11
127.	29.08. - 02.09.2011 DIS-K-421/128/11	Michał Domański i Piotr Radomski wspólnicy spółki cywilnej o nazwie "Limes s.c. Michał Domański, Piotr Radomski", Gdańsk, ul. Pohulanka 2	DOLiS	10.02.2012 DIS/DEC-126/12/8986
128.	29-31.08.2011 DIS-K-421/129/11	Telekomunikacja Polska S.A. Warszawa, ul. Twarda 18	z urzędu	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
129.	05-06.09.2011 DIS-K-421/130/11	Nord Group Sp. z o.o., Warszawa, ul. Echa Leśne 27 C	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
130.	05-07.09.2011 DIS-K-421/131/11	Telepizza Poland Sp. z o.o. Warszawa, ul. Postępu 6	DOLiS	21.11.2011 decyzja DIS/DEC-987/56042/11
131.	05-08.09.2011 DIS-K-421/132/11	HDI - Gerling Życie Towarzystwo Ubezpieczeń S.A., Warszawa, Al. Jerozolimskie 133 A	Komisja Nadzoru Finansowego	nie stwierdzono uchybień
132.	06-08.09.2011 DIS-K-421/133/11	BZ WBK Faktor Sp. z o.o. Warszawa, Al. Jana Pawła II 23	Ministerstwo Finansów	w toku
133.	12-16.09.2011 DIS-K-421/134/11	Samodzielny Publiczny Zakład Opieki Zdrowotnej, Uniwersytecki Szpital Kliniczny Nr 6, Instytut Stomatologii Uniwersytetu Medycznego w Łodzi, Łódź, ul. Pomorska 251	DOLiS	nie stwierdzono uchybień
134.	12-14.09.2011 DIS-K-421/135/11	TelePolska Sp. z o.o., Warszawa, Al. Jerozolimskie 123a	Ministerstwo Infrastruktury	wysłano pismo informacyjne
135.	14-16.09.2011 DIS-K-421/136/11	Sferia S.A., Warszawa, ul. Pawia 55	z urzędu	wysłano pismo informacyjne
136.	14-21.09.2011 DIS-K-421/137/11	Biuro SIRENE -Komenda Główna Policji, Warszawa, ul. Puławska 148/150	z urzędu	13.01.2012 decyzja DIS/DEC-41/12/2283
137.	19-23.09.2011 DIS-K-421/138/11	Europejski Bank DNA Sp. z o.o. Wrocław, ul. Świdnicka 39	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
138.	19-23.09.2011 DIS-K-421/139/11	Leszek Nowicki prowadzący działalność gospodarczą pod nazwą "Piękne Narodziny", Bydgoszcz, ul. Stary Port 13	z urzędu	w toku
139.	19-23.09.2011 DIS-K-421/140/11	Centrum Systemów Informacyjnych Ochrony Zdrowia Warszawa, ul. Dubois 5A	Najwyższa Izba Kontroli	w toku
140.	19-23.09.2011 DIS-K-421/141/11	Lechia Operator Sp. z o.o. Gdańsk, ul. Szklana Huta 7	z urzędu	w toku
141.	19-23.09.2011 DIS-K-421/142/11	Lechia Gdańsk S.A., Gdańsk, ul. Szklana Huta 7	z urzędu	w toku
142.	26-30.09.2011 DIS-K-421/143/11	KKS Lech Poznań S.A. Poznań, ul. Bułgarska 17	z urzędu	nie stwierdzono uchybień
143.	27-30.09.2011 DIS-K-421/144/11	Poczta Polska S. A. Warszawa, ul. Rakowiecka 26	DOLiS	przywrócono stan zgodny z prawem
144.	27-29.09.2011 DIS-K-421/145/11	Sonata Travel Sp. z o.o. Warszawa, ul. Piękna 16	DOLiS	17.01.2012 decyzja DIS/DEC-46/12/2681
145.	26-30.09.2011 DIS-K-421/146/11	Komenda Główna Policji Warszawa, ul. Puławska 148/150	z urzędu	13.01.2012 decyzja DIS/DEC-41/12/2283
146.	29.09 - 04.10.2011 DIS-K-421/147/11	Oficjalny Klub Kibica Reprezentacji Polski Sp. z o.o. Warszawa, ul. Młynarska 7	DOLiS	nie stwierdzono uchybień
147.	03-05.10.2011 DIS-K-421/148/11	GG Warsaw Fitnes Sp. z o.o. Warszawa, ul. St. Kostki Potockiego 2	DOLiS	24.01.2012 DIS/DEC-57/12/4323
148.	03-05.10.2011	Robert Szamota i Olga Szumelda -	z urzędu	nie stwierdzono uchybień

	DIS-K-421/149/11	Szamota wspólnicy spółki cywilnej pod firmą Robbo Computer, Piaseczno, ul. Albatrosów 24 b		
149.	04-06.10.2011 DIS-K-421/150/11	Arkadiusz Hibowski prowadzący działalność gospodarczą pod firmą „Biuro Rachunkowe Agnes Arkadiusz Hibowski”, Bełchatów, Os. Słoneczne 15/34	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
150.	05-07.10.2011 DIS-K-421/151/11	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
151.	05-07.10.2011 DIS-K-421/152/11	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
152.	10.10.2011 DIS-K-421/153/11	SBB Sp. z o.o. Sp. k. Nowa Bukówka, ul. Skulska 20	DOLiS	13.01.2012 decyzja DIS/DEC-40/12/2282
153.	10-14.10.2011 DIS-K-421/154/11	Klub Sportowy Toruń Unibax S.A. Toruń, ul. Pera Jonssona 7	z urzędu	w toku
154.	06-07 i 10.10.2011 DIS-K-421/155/11	Centralny Organ Techniczny KSI (Komendant Główny Policji), Warszawa, ul. Puławska 148/150	z urzędu	11.10.2011 opinia dotycząca zmian w Krajowym Systemie Informatycznym
155.	12-14.10.2011 DIS-K-421/156/11	Exatel S.A. Warszawa, ul. Perkuna 47	z urzędu	nie stwierdzono uchybień
156.	13.10.2011 DIS-K-421/157/11	Zdzisław Tobota prowadzący działalność gospodarczą pod nazwą „Magnum 2”, Warszawa, ul. Fucika 37	w związku z kontrolą DIS-K-421/121/11	16.02.2012 DIS/DEC-137/12/10352,10354
157.	17-21.10.2011 DIS-K-421/158/11	Prezydent Miasta Gdańska – Urząd Miasta Gdańska, Gdańsk, ul. Nowe Ogrody 8/12	z urzędu	nie stwierdzono uchybień
158.	18-19.10.2011 i 07-09.11.2011 DIS-K-421/160/11	Klub Piłkarski Legia Warszawa .S.A. Warszawa, ul. Łazienkowska 3	z urzędu	06.03.2012DIS/DEC-176/12/14291
159.	19-21.10.2011 DIS-K-421/161/11	Goldman Sachs International Oddział w Polsce Warszawa, ul. Mysia 5	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
160.	24-27.10.2011 DIS-K-421/163/11	Przedszkole Nr 33 "Kraina Bajek" Warszawa, ul. Wilcza 63	z urzędu	w toku
161.	24-27.10.2011 DIS-K-421/164/11	Przedszkole Nr 165 Warszawa, ul. Ratuszowa 8 a	z urzędu	w toku
162.	24-28.10.2011 DIS-K-421/165/11	Straż Miejska Miasta Krakowa, Kraków, ul. Dobrego Pasterza 116	DRZDO	13.01.2012 decyzja DIS/DEC-39/12/2281
163.	24-28.10.2011 DIS-K-421/166/11	Szpital Powiatowy w Zawierciu Zawiercie, ul. Miodowa 14	z urzędu	06.03.2012 DIS/DEC-175/12/14285
164.	26-28.10.2011 DIS-K-421/167/11	Netia S.A. Warszawa, ul. Poleczki 13	z urzędu	nie stwierdzono uchybień
165.	19.10.2011 DIS-K-421/168/11	Agencja Bezpieczeństwa Wewnętrznego Warszawa, ul. Rakowiecka 2 A	z urzędu	wnioski przekazano do Departamentu Edukacji Społecznej i Współpracy Międzynarodowej
166.	19.10.2011 DIS-K-421/169/11	Komendant Główny Żandarmerii Wojskowej Warszawa, ul. Jana Ostroroga 25	z urzędu	wnioski przekazano do Departamentu Edukacji Społecznej i Współpracy Międzynarodowej
167.	19.10.2011 DIS-K-421/170/11	Szef Służby Celnej Warszawa, ul. Świętokrzyska 12	z urzędu	wnioski przekazano do Departamentu Edukacji Społecznej i Współpracy Międzynarodowej
168.	19.10.2011 DIS-K-421/171/11	Szef Centralnego Biura Antykorupcyjnego Warszawa, Al. Ujazdowskie 9	z urzędu	wnioski przekazano do Departamentu Edukacji Społecznej i Współpracy Międzynarodowej
169.	19.10.2011 DIS-K-421/172/11	Generalny Inspektor Kontroli Skarbowej Warszawa, ul. Świętokrzyska 12	z urzędu	wnioski przekazano do Departamentu Edukacji Społecznej i Współpracy Międzynarodowej
170.	19.10.2011 DIS-K-421/173/11	Komendant Główny Straży Granicznej Warszawa, Al. Niepodległości 100	z urzędu	wnioski przekazano do Departamentu Edukacji Społecznej i

				Współpracy Międzynarodowej
171.	07-09.11.2011 DIS-K-421/174/11	Przedszkole Nr 16 "Zaczarowany Zakątek" Warszawa, ul. Górskiego 5 A	z urzędu	w toku
172.	08-10.11.2011 DIS-K-421/175/11	Przedszkole Nr 295 Warszawa, ul. Afrykańska 9	z urzędu	w toku
173.	16.11.2011 DIS-K-421/176/11	Wspólnota Mieszkaniowa "Plac Przymierza 4" Warszawa, Plac Przymierza 4	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
174.	07-09.11.2011 DIS-K-421/177/11	Starosta Powiatu Mińskiego - Starostwo Powiatowe w Mińsku Mazowieckim, Mińsk Mazowiecki, ul. Kościuszki 3	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
175.	08-10.11.2011 DIS-K-421/178/11	Acxiom Polska Sp. z o.o. Warszawa, ul. Wołowska 3	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
176.	14-18.11.2011 DIS-K-421/179/11	Prezydent Miasta Siemianowice Śląskie, Siemianowice Śląskie ul. Jana Pawła II 10	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
177.	14-18.11.2011 DIS-K-421/180/11	Starosta Powiatu Gryfickiego - Starostwo Powiatowe w Gryficach, Gryfice, Pl. Zwycięstwa 37	w związku z kontrolą DIS-K-421/117/11	13.02.2012 DIS/DEC-128/12/9241
178.	14-16.11.2011 DIS-K-421/181/11	easyCALL.pl S.A. Warszawa, ul. Poniecka 2/16	z urzędu	nie stwierdzono uchybień
179.	14-16.11.2011 DIS-K-421/182/11	Zarząd Transportu Miejskiego, Warszawa, ul. Żelazna 61	DOLiS	w toku
180.	14-18.11.2011 DIS-K-421/183/11	Wojewoda Zachodniopomorski - Zachodniopomorski Urząd Wojewódzki, Szczecin, ul. Wały Chrobrego 4	DRZDO	nie stwierdzono uchybień
181.	21-25.11.2011 DIS-K-421/184/11	Europejski Fundusz Leasingowy S.A. Wrocław, Plac Orłat Lwowskich 1	DRZDO	nie stwierdzono uchybień
182.	21-25.11.2011 DIS-K-421/185/11	Starosta Powiatu Kłodzkiego - Starostwo Powiatu Kłodzkiego, Kłodzko, ul. Okrzei 1	DRZDO	nie stwierdzono uchybień
183.	21-23.11.2011 DIS-K-421/186/11	Przedszkole Nr 149 Warszawa, ul. Dolna 8	z urzędu	w toku
184.	28-30.11.2011 DIS-K-421/187/11	Przedszkole Pomarańczowa Ciuchcia - Bemowo I A. Sławek, J. Wawer Sp. j. Warszawa, ul. Dostępna 60	z urzędu	w toku
185.	28-30.11.2011 DIS-K-421/188/11	Przedszkole Nr 13 Warszawa, ul. Schillera 6 a	z urzędu	w toku
186.	28-30.11.2011 DIS-K-421/189/11	Publiczne Przedszkole nr 2 "Leśny Zakątek", Ząbki, ul. Prusa 3/5	z urzędu	w toku
187.	28.11-02.12.2011 DIS-K-421/190/11	Piotr Majewski prowadzący działalność gospodarczą pod nazwą „H.A.S. i P. Hurt - Detal Piotr Majewski”, Płock, ul. Tumska 4a	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
188.	05-09.12.2011 DIS-K-421/192/11	RedBelt Sp. z o.o. Łódź, ul. Łąkowa 7 b	DRZDO	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
189.	05-07.12.2011 DIS-K-421/193/11	Karol Kossut prowadzący działalność gospodarczą pod nazwą „KOSSUT PL Karol Kossut”, Skierniewice, ul. Buczka 8/19	DOLiS	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
190.	06-09.12.2011 DIS-K-421/194/11	Acxiom Polska Sp. z o.o. Warszawa, ul. Wołowska 3	w związku z kontrolą DIS-K-421/139/11	w toku
191.	12-14.12.2011 DIS-K-421/195/11	PKO Bank Polski S.A. Warszawa, ul. Puławska 15	w związku z kontrolą DIS-K-421/77/11	28.03.2012 DIS/DEC-264/12/20327
192.	12-15.12.2011	Przedsiębiorstwo Komunikacji	z urzędu	nie stwierdzono uchybień

	DIS-K-421/196/11	Samochodowej Polonus w Warszawie S.A., Warszawa, Al. Jerozolimskie 144		
193.	12-16.12.2011 DIS-K-421/197/11	PayU S.A. Poznań, ul. Marcelesińska 90	DOLiS	nie stwierdzono uchybień
194.	13-16.12.2011 DIS-K-421/198/11	Przedszkole Nr 1 Skierniewice, ul. Batorego 61/63	z urzędu	w toku
195.	19-21.12.2011 DIS-K-421/199/11	Bank Handlowy w Warszawie S.A. Warszawa, ul. Senatorska 16	w związku z kontrolą DIS- K-421/77/11	w toku
196.	19-21.12.2011 DIS-K-421/200/11	Przedszkole Nr 283 Warszawa, ul. Puszczyka 6	z urzędu	w toku
197.	19-21.12.2011 DIS-K-421/201/11	Przedszkole Miejskie Nr 11 Legionowo, ul. Zegrzyńska 9	z urzędu	w toku
198.	19-21.12.2011 DIS-K-421/202/11	Przedszkole Nr 243 Warszawa, ul. Kordiana 7/11	z urzędu	w toku
199.	20-23.12.2011 DIS-K-421/203/11	Medigen Sp. z o. o. – NZOZ „Medigen” Warszawa, ul. Morcinka 5/19	DRZDO	w toku

**Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie
i Naczelnego Sądu Administracyjnego wydanych w 2011 r.
w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych**

L.p.	Data/ sygnatura orzeczenia WSA w Warszawie lub NSA	Sygnatura rozstrzygnięcia GODO	Przedmiot sprawy	Rozstrzygnięcie WSA w Warszawie lub NSA
1.	11.01.2011 II SA/Wa 12320/10	DOLiS/DEC-640/10/21650,21651,21652	Skarga w zakresie uchylecia decyzji w części dotyczącej uzasadnienia i w zakresie tej części umorzenia postępowania	oddalenie skargi
2.	13.01.2011 I OSK 440/10	GI-DEC-DOLiS-223/07/5896,5897	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
3.	02.02.2011 II SA/Wa 796/10	DOLiS/DEC-258/10/10197,10202,10205	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
4.	10.02.2011 II SA/Wa 1560/10	DOLiS/DEC-966/10/29711,29715,29717	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji
5.	15.02.2011 II SA/Wa 1876/10	DOLiS/DEC-1119/10/37145,37146	Skarga na decyzję GODO w przedmiocie przetwarzania danych osobowych	odrzućenie skargi
6.	16.02.2011 I OSK 1084/05	GI-DEC-DIS-118/04/253	Odmowa stwierdzenia nieważności decyzji.	sprostowanie wyroku
7.	16.02.2011 II SA/Wa 2182/10	DOLiS/DEC-900/08/35916,35912	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na nieprawidłowości w procesie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
8.	24.02.2011 I OSK 653/10	DOLiS/DEC-53/08/1776,1777,1778	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi kasacyjnej
9.	01.03.2011 II SAB/Wa 304/10	DOLiS-440-481/10	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	zobowiązanie GODO do rozpoznania skargi w terminie 30 dni
10.	01.03.2011 II SA/Wa 1530/10	DOLiS/DEC-947/10/29262,29266,29271	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
11.	10.03.2011 II SA/Wa 1885/10	DOLiS/DEC-1129/10/37954,37958	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
12.	10.03.2011 II SA/Wa 41/11	DOLiS-035-1479/10/28746	Skarga na pismo GODO w przedmiocie ochrony danych osobowych	odrzućenie skargi
13.	22.03.2011 I OSK 623/10	DOLiS/DEC-285/09/12865,12867	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	uchylenie zaskarżonego wyroku i przekazanie sprawy do WSA w Warszawie w celu ponownego rozpoznania
14.	07.04.2011 I OSK 820/10	DOLiS/DEC-298/09/13168,13171,13176	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
15.	11.04.2011 I OSK 826/10	DOLiS/DEC-753/09/28118,28121,28123,28127	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	uchylenie zaskarżonego wyroku i oddalenie skargi
16.	12.04.2011 II SA/Wa 1928/10	DOLiS/DEC-1151/10/38997,38998	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	uchylenie zaskarżonej decyzji

17.	29.04.2011 II SA/Wa 385/11	DOLiS/DEC-3/11/322,324	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	oddalenie skargi
18.	06.05.2011 II SA/Wa 2167/10	DOLiS/DEC-1236/10/43133,43134,43135	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych w zakresie imienia, nazwiska oraz adresu zameldowania	odrzućcie skargi
19.	06.05.2011 II SA/Wa 2167/10	DOLiS/DEC-1236/10/43133,43134,43135	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych w zakresie imienia, nazwiska oraz adresu zameldowania	odrzućcie skargi
20.	10.05.2011 II SAB/Wa 49/11	DOLiS-440-588/10	Skarga na bezczynność w przedmiocie rozpoznania wniosku dotyczącego przetwarzania danych osobowych	odrzućcie skargi
21.	17.05.2011 II SA/Wa 1019/10	DOLiS/DEC-571/10/19486,19489,19493	Skarga w przedmiocie stwierdzenia nieważności decyzji	odrzućcie skargi kasacyjnej
22.	19.05.2011 I OSK 1086/10	DOLiS/DEC-396/09/17832,17836	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
23.	19.05.2011 I OSK 1079/10	DOLiS/DEC-109/09/4751,4752	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
24.	19.05.2011 I OSK 1162/10	DIS/DEC-1069/39458/09	Usunięcie z urzędu densytometrycznego danych osobowych skarżącego	oddalenie skargi kasacyjnej
25.	02.06.2011 II SA/Wa 720/11	DIS/DEC-43/2827/11	Niedopełnianie obowiązku informacyjnego	oddalenie skargi
26.	07.06.2011 II SA/Wa 267/11	DOLiS/DEC-1310/10/47273,47275	Skarga na decyzję w przedmiocie nakazania usunięcia uchybień powstałych w procesie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
27.	13.06.2011 II SAB/Wa 124/11	DOLiS-440-1096/10	Skarga na bezczynność w przedmiocie rozpoznania wniosku w sprawie przetwarzania danych osobowych	umorzenie postępowania
28.	17.06.2011 II SAB/Wa 143/11	DOLiS-440-180/10	Skarga na bezczynność w zakresie rozpatrzenia wniosku o ponowne rozpatrzenie sprawy dotyczącej przetwarzania danych osobowych	umorzenie postępowania
29.	20.06.2011 II SA/Wa 719/11	DIS/DEC-39/2767/11	Zbieranie danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników	oddalenie skargi
30.	22.06.2011 II SA/Wa 917/11	DOLiS/POST-31/11/6560,6561,6564	Skarga na postanowienie w przedmiocie zawieszenia postępowania w sprawie przetwarzania danych osobowych	uchylenie zaskarżonego postanowienia
31.	28.06.2011 II SAB/Wa 125/11	DOLiS-440-1095/10	Skarga na bezczynność w zakresie rozpoznania wniosku w sprawie przetwarzania danych osobowych	umorzenie postępowania
32.	28.06.2011 II SAB/Wa 194/11	GI-DS-430/997/04	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku w sprawie przetwarzania danych osobowych	odrzućcie skargi
33.	28.06.2011 II SA/Wa 1141/11	DOLiS/DEC-179/11/9834,9836,9837,9838	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych	odrzućcie skargi
34.	28.06.2011 II SA/Wa 1140/11	DOLiS/DEC-178/11/9822,9827	Skarga na decyzję w przedmiocie usunięcia danych osobowych	odrzućcie skargi
35.	28.06.2011 I OSK 1217/10	DOLiS/DEC-603/09/24307,24309	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	oddalenie skargi kasacyjnej
36.	28.06.2011 I OSK 1264/10	DOLiS/DEC-1182/09/43667,43669	Skarga na decyzję w przedmiocie nakazania usunięcia uchybień przy przetwarzaniu danych osobowych	oddalenie skargi kasacyjnej
37.	28.06.2011 II SA/Wa 1140/11	DOLiS/DEC-178/11/9822,9827	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych	odrzućcie skargi

38.	28.06.2011 I OSK 1208/10	DOLiS/DEC- 1103/09/40498,40499, 40502	Skarga na decyzję w przedmiocie umorzenia postępowania w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego wyroku i przekazanie sprawy do WSA w Warszawie w celu ponownego rozpoznania
39.	30.06.2011 II SA/Wa 1099/11	DIS/DEC- 190/10384,10387/11	Brak zapewnienia klientom możliwości złożenia oświadczenia o niewyrażeniu zgody na przetwarzanie dodatkowych danych osobowych	odmowa wstrzymania wykonania zaskarżonej decyzji
40.	07.07.2011 II SA/Wa 940/10	DOLiS/DEC- 505/10/17434,17435	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
41.	15.07.2011 I OSK 238/11	DOLiS/DEC- 835/10/26031,26035	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego wyroku i przekazania sprawy WSA w Warszawie do ponownego rozpoznania
42.	18.07.2011 II SAB/Wa 205/11	DOLiS-440-588/10	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku o ponowne rozpatrzenie sprawy zakończonej decyzją o umorzeniu postępowania w sprawie przetwarzania danych osobowych	odrzućcie skargi
43.	11.08.2011 II SAB/Wa 182/11	DOLiS-067-11/11	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku o udostępnienie informacji publicznej	odrzućcie skargi
44.	11.08.2011 II SA/Wa 1319/11	DOLiS/DEC- 358/11/21731	Skarga na decyzję w przedmiocie dostępu do informacji publicznej	Stwierdzenie nieważności decyzji
45.	11.08.2011 I SA/Wa 1152/11	DOLiS/DEC- 285/09/12865,12867	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych w zakresie adresu zamieszkania	uchylenie zaskarżonej decyzji
46.	11.08.2011 II SAB/Wa 182/11	DOLiS-067-11/11	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku o udostępnienie informacji publicznej	odrzućcie skargi
47.	11.08.2011 II SA/Wa 1319/11	DOLiS/DEC- 358/11/21731	Skarga na decyzję w przedmiocie dostępu do informacji publicznej	Stwierdzenie nieważności zaskarżonej decyzji
48.	11.08.2011 I OSK 1420/10	DOLiS/DEC-123/09- 1276/09/47685,47691	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
49.	11.08.2011 II SA/Wa 1152/11	DOLiS/DEC- 285/09/12865,12867	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych w zakresie adresu zamieszkania	uchylenie zaskarżonej decyzji
50.	17.08.2011 II SA/Wa 1675/11	DOLiS/POST- 120/11/24808	Skarga na postanowienie w przedmiocie odmowy sporządzenia i wydania uwierzytelnionych odpisów akt postępowania administracyjnego	odrzućcie skargi
51.	31.08.2011 II SAB/Wa 217/11	DOLiS-440-958/10	Skarga na bezczynność w przedmiocie sprostowania danych osobowych	odrzućcie skargi
52.	06.09.2011 I OSK 1476/10	DIS/DEC- 1172/43212/09	Zbieranie danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników, przetwarzanych w celu ewidencji czasu pracy, ich usunięcie oraz nieuwzględnienie systemu informatycznego w polityce bezpieczeństwa w opisie struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych	oddalenie skargi kasacyjnej

			i powiązań między nimi	
53.	06.09.2011 I OSK 1518/10	DOLiS/DEC- 123/09/5909	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie wniosku o wszczęcie postępowania administracyjnego	oddalenie skargi kasacyjnej
54.	07.09.2011 II SA/Wa 735/11	DOLiS/DEC- 84/11/5415,5416	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	uchylenie zaskarżonej decyzji
55.	13.09.2011 II SA/Wa 1254/11	DOLiS/POST- 75/11/14847,14849,14851	Skarga na postanowienie w przedmiocie odmowy uzupełnienia decyzji	odrzućcie skargi
56.	14.09.2011 II SA/Wa 645/11	DOLiS/DEC- 8/11/439,440,442	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku o zabezpieczenie danych osobowych	uchylenie zaskarżonej decyzji
57.	20.09.2011 I OZ 671/11	DOLiS-440-1095/10	Zażalenie na postanowienie WSA w Warszawie w zakresie rozstrzygnięcia w przedmiocie zwrotu kosztów postępowania w sprawie skargi na bezczynność w przedmiocie rozpoznania wniosku w sprawie przetwarzania danych osobowych	odrzućcie zażalenia
58.	21.09.2011 II SA/Wa 776/11	DOLiS/DEC- 60/11,4388,4390,4391	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie udostępnienia danych osobowych	oddalenie skargi
59.	22.09.2011 II SA/Wa 733/11	DOLiS/POST- 27/11/5799,5803	Skarga na postanowienie w przedmiocie stwierdzenia uchybienia terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy	odrzućcie skargi
60.	22.09.2011 II SA/Wa 733/11	DOLiS/POST- 27/11/5799,5803/11	Skarga na postanowienie w przedmiocie stwierdzenia uchybienia terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy	odrzućcie skargi
61.	28.09.2011 II SA/Wa 1141/11	DOLiS/DEC- 179/11/9834,9836,9837,9838	Skarga na decyzję w przedmiocie nakazania usunięcia danych osobowych	odrzućcie skargi
62.	29.09.2011 I OZ 728/11	DOLiS-440-1096/10	Zażalenie na postanowienie WSA w Warszawie w zakresie rozstrzygnięcia w przedmiocie zwrotu kosztów postępowania w sprawie skargi na bezczynność w przedmiocie rozpoznania wniosku w sprawie przetwarzania danych osobowych	uchylenie pkt 2 postanowienia WSA w Warszawie
63.	29.09.2011 II S.A./Wa 1330/11	DRZDO/POST-85 /11/16206 dot. DRZDO- 401/002562/09	Uchybienie terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy zakończonej decyzją o odnowie rejestracji zbioru danych osobowych	uchylenie zaskarżonego postanowienia
64.	30.09.2011 I OSK 1827/11	DIS/DEC-43/2827/11	Niedopełnianie obowiązku informacyjnego.	wstrzymanie wykonania zaskarżonej decyzji
65.	03.10.2011 I OSK 1577/10	DOLiS-440- 711/08/10775/10	Skarga kasacyjna od postanowienia WSA w Warszawie w sprawie skargi na pismo GIDO	uchylenie zaskarżonego postanowienia i przekazanie sprawy WSA w Warszawie do ponownego rozpoznania
66.	04.10.2011 I OZ 718/11	DOLiS/DEC- 189/11/10382,10386	Zażalenie na postanowienie WSA w Warszawie o odmowie wstrzymania wykonania decyzji w sprawie skargi w przedmiocie nakazu zaprzestania pozyskiwania danych osobowych odmowy uwzględnienia wniosku	oddalenie zażalenia
67.	11.10.2011 II SA/Wa 160/11	DOLiS/DEC- 1318/10/47328,47329	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi

68.	12.10.2011 II SA/Wa 1307/11	DOLiS/POST- 89/11/17187	Skarga na postanowienie w przedmiocie zwrotu wniosku	uchylenie zaskarżonego postanowienia
69.	12.10.2011 I OSK 1707/10	DOLiS/POST- 42/09/4677,4680,4683 ,4687	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na postanowienie w przedmiocie odmowy uwzględnienia wniosku o udostępnienie danych osobowych	oddalenie skargi kasacyjnej
70.	12.10.2011 II SAB/Wa 170/11	DOLiS-440-956/09	Skarga na bezczynność w przedmiocie rozpoznania wniosku dotyczącego przetwarzania danych osobowych	zobowiązanie GODO do rozpoznania wniosku w terminie 14 dni
71.	12.10.2011 II SAB/Wa 171/11	DOLiS-440-212/11	Skarga na bezczynność w przedmiocie rozpoznania wniosku dotyczącego przetwarzania danych osobowych	zobowiązanie GODO do rozpoznania wniosku w terminie 14 dni
72.	12.10.2011 II SAB/Wa 172/11	DOLiS-440-116/11	Skarga na bezczynność GODO	oddalenie skargi
73.	17.10.2011 II SA/Wa 604/11	DOLiS/DEC- 82/11/4927,4930,4931	Skarga na decyzję w przedmiocie umorzenia postępowania	oddalenie skargi
74.	18.10.2011 I OSK 1742/10	DOLiS/DEC- 1293/09/48041,48042, 48046	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	uchylenie wyroku i przekazanie sprawy do ponownego rozpoznania WSA w Warszawie
75.	20.10.2011 II SA/Wa 1055/11	DOLiS/DEC- 204/11/10954,10955	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
76.	20.10.2011 II SA/Wa 1174/11	DOLiS/DEC- 303/11/17475/17476	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	odrzućenie skargi
77.	21.10.2011 I OSK 1806/10	DOLiS/DEC- 27/10/1591,1598,1602	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
78.	24.10.2011 II SA/Wa 625/11	DOLiS/DEC- 1257/10/44416,44417, 44418,44419	Skarga na decyzję GODO w przedmiocie przetwarzania danych osobowych	oddalenie skargi
79.	26.10.2011 II SAB/Wa 294/11	dot. DRZDO/401/ 002611/11	Bezczynność GODO w przedmiocie rozpatrzenia wniosku o wpisanie zbioru danych do rejestru zbiorów danych osobowych	odrzućenie skargi
80.	27.10.2011 II SA/Wa 1691/11	DOLiS/DEC- 1103/09/40498,40499, 40502	Skarga na decyzję GODO w przedmiocie umorzenia postępowania w sprawie ochrony danych osobowych	oddalenie skargi
81.	27.10.2011 I OSK 2125/10	DOLiS/DEC- 231/10/8744,8748,875 7	Skarga kasacyjna GODO od wyroku WSA w Warszawie w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
82.	03.11.2011 II SA/Wa 1320/11	DOLiS/DEC- 311/11/17991,17992	Wniosek o dopuszczenie w charakterze uczestnika postępowania do udziału w sprawie ze skargi na decyzję GODO	odmowa uznania wniosku
83.	04.11.2011 I OSK 1934/10	DOLiS/DEC- 94/10/3315,3319	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
84.	09.11.2011 II SA/Wa 1363/11	DOLiS/DEC- 307/11/17970,17976	Skarga na decyzję GODO w przedmiocie nakazania wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych	oddalenie skargi
85.	10.11.2011 I OSK 1974/10	DOLiS/DEC-55- 10/2085,2088	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie ze skargi na decyzję GODO	oddalenie skargi kasacyjnej
86.	12.11.2011 II SAB/Wa 240/11	DOLiS-440-151/11	Zażalenie GODO na postanowienie WSA w Warszawie w zakresie rozstrzygnięcia w przedmiocie zwrotu kosztów postępowania w sprawie skargi	odrzućenie zażalenia

			na bezczynność w zakresie rozpoznania wniosku w sprawie przetwarzania danych osobowych	
87.	21.11.2011 II SAB/Wa 125/11	DOLiS-440-1095/10	Wniosek GIODO o przywrócenie terminu do wniesienia zażalenia na postanowienie WSA w Warszawie w sprawie skargi na bezczynność w zakresie rozpoznania wniosku w sprawie przetwarzania danych osobowych	przywrócenie terminu do wniesienia zażalenia
88.	21.11.2011 II SAB/Wa 240/11	DOLiS-440-151/11	Zażalenie GIODO na postanowienie WSA w Warszawie w przedmiocie zwrotu kosztów postępowania w sprawie ze skargi na bezczynność GIODO	odrzućcie zażalenia
89.	28.11.2011 II SA/Wa 978/11	DOLiS/DEC- 188/11/10381,10385	Skarga na decyzję GIODO w przedmiocie zobowiązania do usunięcia uchybień w procesie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji i decyzji poprzedzającej
90.	28.11.2011 II SA/Wa 2400/11	DOLiS/DEC- 692/11/39890	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	odrzućcie skargi
91.	06.12.2011 I OSK 11/11	DOLiS/POST-101-09- 14892,14893	Skarga kasacyjna GIODO od wyroku WSA w Warszawie w sprawie ze skargi na postanowienie GIODO w przedmiocie odmowy uwzględnienia wniosku	uchylenie zaskarżonego wyroku i przekazanie sprawy WSA w Warszawie do ponownego rozpoznania
92.	06.12.2011 I OSK 64/11	DOLiS/POST- 63/10/15823,15826,15 829	Skarga kasacyjna GIODO od wyroku WSA w Warszawie w sprawie skargi na postanowienie GIODO w przedmiocie wydania dokumentów z akt postępowania dotyczącego ochrony danych osobowych	oddalenie skargi kasacyjnej
93.	06.12.2011 I OSK 182/11	DOLiS/POST- 41/10/8991,8992,8994 ,8995,8996	Skarga kasacyjna od wyroku WSA w Warszawie w sprawie skargi na postanowienie w przedmiocie odmowy sporządzenia i przesłania uwierzytelnionych kserokopii dokumentów z akt sprawy	uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania WSA w Warszawie
94.	06.12.2011 I OSK 183/11	DOLiS/DEC- 114/10/3949,3950,395 2,3956,3958	Skarga kasacyjna od wyroku WSA w Warszawie na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania WSA w Warszawie
95.	07.12.2011 II SA/Wa 1055/11	DOLiS/DEC- 204/11/10954,10955	Skarga na decyzję w przedmiocie ochrony danych osobowych.	oddalenie skargi
96.	07.12.2011 II SA/Wa 1560/11	DOLiS/DEC- 336/11/19849,19854	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	uchylenie decyzji i poprzedzającej jej decyzji
97.	13.12.2011 I OSK 168/11	DOLiS-440-956/09	Skarga kasacyjna GIODO od wyroku WSA w Warszawie w sprawie skargi na bezczynność GIODO	oddalenie skargi kasacyjnej
98.	13.12.2011 I OSK 521/11	DOLiS/DEC- 695/10/23507,23509,2 3510,23511,23512,23 514	Skarga kasacyjna GIODO od wyroku WSA w Warszawie w sprawie skargi na decyzję GIODO w przedmiocie odmowy uwzględnienia wniosku w sprawie udostępnienia danych osobowych	uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania WSA w Warszawie
99.	13.12.2011 I OSK 834/11	DOLiS/DEC- 966/10/29715,29717	Skarga kasacyjna GIODO od wyroku WSA w Warszawie w sprawie skargi na decyzję GIODO w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania WSA w Warszawie
100.	13.12.2011 I OSK 1137/11	DOLiS/DEC- 1146/10/38752,38755, 38759	Skarga kasacyjna GIODO od wyroku WSA w Warszawie w sprawie skargi na decyzję GIODO w przedmiocie odmowy uwzględnienia wniosku o udostępnienie	uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania WSA w

			danych osobowych	Warszawie
101.	15.12.2011 II SA/Wa 2137/11	DOLiS/DEC-608/11/35364	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	odrzućcie skargi
102.	16.12.2011 I OSK 632/11	DOLiS/DEC-601/10/21236,21242,21249,21254,21256	Skarga kasacyjna GIODO od wyroku WSA w Warszawie w sprawie skargi na decyzję GIODO w przedmiocie odmowy uchylenia decyzji w sprawie przetwarzania danych osobowych	oddalenie skargi kasacyjnej
103.	29.12.2011 II SAB/Wa 240/11	DOLiS-440-151/11	Wniosek GIODO o przywróćcie terminu do wniesienia zażalenia na postanowienie WSA w Warszawie w sprawie ze skargi na bezczynność w zakresie rozpoznania wniosku w sprawie przetwarzania danych osobowych	przywróćcie terminu do wniesienia zażalenia

**Informacje przekazane przez organy ścigania
w sprawach skierowanych w 2011 r.
przez Generalnego Inspektora Ochrony Danych Osobowych
zawiadomień o popełnieniu przestępstwa**

Informacja	Rok 2009	Rok 2010	Rok 2011
Umorzenie dochodzenia	11	14	6
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	1
Odmowa wszczęcia dochodzenia	3	3	2
Wszczęcie śledztwa i jego umorzenie	-	-	
Zawieszenie dochodzenia	-	1	
Skierowanie sprawy do sądu	-	1	
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	-	1	
Brak informacji	-	1	

Wykaz szkoleń przeprowadzonych przez GIODO w 2011 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	20.01.2011	Łódź	Rada Organizacji Pozarządowych Województwa Łódzkiego
2.	31.01.2011	Warszawa	Uczniowie klas IV-V Szkoły Podstawowej Kolegium Zakonu Pijarów w Warszawie
3.	16.02.2011	Warszawa	Centrum Projektów Informatycznych Ministerstwa Spraw Wewnętrznych i Administracji
4.	24.02.2011	Warszawa	Centrum Projektów Informatycznych Ministerstwa Spraw Wewnętrznych i Administracji
5.	24.02.2011	Warszawa	Liderzy ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli.
6.	01.03.2011	Warszawa	Centrum Projektów Informatycznych Ministerstwa Spraw Wewnętrznych i Administracji
7.	05.03.2011	Warszawa	Zespół Szkół Sportowych im. Olimpijczyków Śląskich w Mysłowicach
8.	09.03.2011	Rynia	Urzędy administracji samorządowej
9.	11.03.2011	Wrocław	Państwowa Inspekcja Pracy
10.	16.03.2011	Płock	Prokuratura Okręgowa w Płocku
11.	23.03.2011	Warszawa	Centrum Rozwoju Zawodowego Ministerstwa Spraw Zagranicznych
12.	08.04.2011	Warszawa	Urząd m.st. Warszawy
13.	11.04.2011	Warszawa	Narodowy Fundusz Zdrowia
14.	11.04.2011	Warszawa	Urząd m.st. Warszawy
15.	11.04.2011	Warszawa	Krajowa Rada Radiofonii i Telewizji
16.	11.04.2011	Warszawa	Urząd m.st. Warszawy
17.	13.04.2011	Warszawa	Warszawskie Centrum Innowacji Edukacyjnych i Szkoleń
18.	09.05.2011	Warszawa	Ministerstwo Pracy i Polityki Społecznej
19.	10.05.2011	Warszawa	Ministerstwo Zdrowia
20.	11.05.2011	Płock	Prokuratura Okręgowa w Płocku
21.	12.05.2011	Warszawa	Ministerstwo Zdrowia
22.	23.05.2011	Warszawa	Ministerstwo Pracy i Polityki Społecznej
23.	16.06.2011	Warszawa	Ministerstwo Finansów, Departament Służby Celnej
24.	16.06.2011	Warszawa	Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej
25.	20.06.2011	Warszawa	Rzecznik Praw Obywatelskich, Zespół „Krajowy Mechanizm Prewencji”
26.	27.06.2011	Częstochowa	Krajowa Rada Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej w Częstochowie
27.	07-08.09.2011	Kętrzyn	Straż Graniczna
28.	20.09.2011	Łódź	Wojewódzki Urząd Pracy w Łodzi

29.	21.09.2011	Warszawa	Centrum Projektów Europejskich
30.	21.09.2011	Łańsk	Kancelaria Prezydenta RP
31.	23.09.2011	Zakopane	Polskie Towarzystwo Informacji Naukowej
32.	26.09.2011	Rzeszów	Wojewódzki Fundusz Ochrony Środowiska w Rzeszowie
33.	27.09.2011	Wrocław	Urząd Miasta Wrocław
34.	30.09.2011	Opole	Ogólnopolski Konwent Agencji Pracy
35.	04.10.2011	Warszawa	Wojewódzki Urząd Pracy w Warszawie
36.	05.10.2011	Poznań	Wojewódzki Urząd Pracy w Poznaniu
37.	14.10.2011	Warszawa	Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej
38.	14.10.2011	Warszawa	Centrum Rozwoju Zawodowego Ministerstwa Spraw Zagranicznych
39.	07.11.2011	Warszawa	Sąd Okręgowy Warszawa Praga
40.	09.11.2011	Warszawa	Sąd Okręgowy Warszawa Praga
41.	09.11.2011	Warszawa	Fundacja Dzieci Niczyje
42.	17.11.2011	Warszawa	Sąd Okręgowy Warszawa Praga
43.	17.11.2011	Warszawa	Centrum Rozwoju Zawodowego Ministerstwa Spraw Zagranicznych
44.	17.11.2011	Warszawa	Mazowiecki Zarząd Dróg Wojewódzkich w Warszawie
45.	18.11.2011	Warszawa	Sąd Okręgowy Warszawa Praga
46.	22.11.2011	Warszawa	Generalna Dyrekcja Ochrony Środowiska
47.	22.11.2011	Warszawa	Główny Inspektorat Pracy
48.	22.11.2011	Warszawa	Główny Urząd Statystyczny
49.	23.11.2011	Warszawa	Naczelna Dyrekcja Archiwów Państwowych
50.	23.11.2011	Warszawa	Warszawskie Centrum Innowacji Edukacyjnych i Szkoleń
51.	23.11.2011	Warszawa	Główny Inspektorat Pracy
52.	24.11.2011	Warszawa	Generalna Dyrekcja Ochrony Środowiska
53.	02.12.2011	Warszawa	Związek Województw RP
54.	05.12.2011	Warszawa	Urząd Ochrony Konkurencji i Konsumentów
55.	08.12.2011	Warszawa	Warszawski Uniwersytet Medyczny

**Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych
w 2011 r.**

1. III edycja konferencji „Między wolnością a bezpieczeństwem w szkole”. Organizator: Gimnazjum Nr 24 w Zabrzu. Zabrze, 24 lutego 2011 r.
2. Konferencja naukowa „Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym”. Organizator: Wydział Prawa i Administracji UW. Warszawa, 21 marca 2011 r.
3. II Zjazd Akademii Zarządzania Dyrektora Szkoły 2010/2011 „Aktualne problemy prawa oświatowego”. Organizator: miesięcznik "Dyrektor Szkoły". II Zjazd odbył się dwóch miastach - 24 marca 2011 r. w Warszawie i 7 kwietnia 2011 r. w Szczecinie.
4. Ogólnopolska konferencja naukowa Zabezpieczenie danych osobowych - aktualny stan prawny a rzeczywiste potrzeby". Organizator: Wydział Zarządzania Politechniki Warszawskiej i Stowarzyszenie Administratorów Bezpieczeństwa Informacji. Warszawa, 28 marca 2011 r.
5. Światowy Dzień Telekomunikacji i Społeczeństwa Informacyjnego 2011, który przebiegał pod hasłem "Lepsze życie w społecznościach lokalnych z Technikami Komunikacyjnymi i Informacyjnymi". Organizator: Stowarzyszenie Elektryków Polskich. Warszawa, maj 2011 r.
6. Konferencja „NIE DAJ SIĘ ZŁAPAC W SIEĆ! - prawa autorskie, bezpieczeństwo i dobra osobiste w Internecie". Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Poland, Katolicki Uniwersytet Lubelski oraz ELSA Lublin. Lublin, 16-18 maja 2011 r.
7. Obchody Światowego Dnia Społeczeństwa Informacyjnego w Polsce 2011, pod hasłem „Przeciwdziałanie wykluczeniu cyfrowemu na terenach mało zurbanizowanych". Organizator: Polskie Towarzystwo Informatyczne. Warszawa, 18 maja 2011 r.
8. VII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych, Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Spała, 25-27 maja 2011 r.
9. Trzecia edycja konferencji naukowej „Bezpieczeństwo w Internecie”. Organizator: Uniwersytet Karola Stefana Wyszyńskiego, Naukowa i Akademicka Sieć Komputerowa oraz Naukowe Centrum Prawno - Informatyczne. Warszawa, 8-9 czerwca 2011 r.
10. Konferencja "Nadzór niekontrolowany? Nowe wyzwania dla wolności". Organizator: Fundacja Panoptykon. Warszawa, 11 października 2011 r.
11. Konferencja „Cloud Computing 2011”. Organizator: tygodnik Computerworld. Warszawa, 20-21 października 2011 r.
12. Ogólnopolska konferencja „Wyzwania XXI wieku czyli nieświadomość bezpieczeństwa informacji, ochrony danych osobowych i nie tylko”. Organizator: TÜVPOL Sp. z o.o. Wrocław, 21 października 2011 r.
13. Forum IAB połączone z targami Internet Poland oraz galą konkursu kreatywnego MIXX - AWARDS. Organizator: Związek Pracodawców Branży Internetowej IAB Polska. Warszawa, 8-9 listopada 2011 r.

14. IV Międzynarodowa Konferencja „Jakość w działaniu na rzecz bezpieczeństwa państw Grupy Wyszehradzkiej z perspektywy europejskiej”. Organizator: Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi oraz Wyższa Szkoła Policyjna w Szczytnie. Józefów, 21 listopada 2011 r.
15. IV Konferencja Central European Electronic Card - Warsaw 2011. Organizator: Medien Service. Warszawa, 30 listopada - 1 grudnia 2011 r.
16. Konferencja naukowa "Bezpieczeństwo technologii biometrycznych - ochrona danych biometrycznych". Organizator: Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Warszawa, 9 grudnia 2011 r.

Wykaz konferencji, seminariów i spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2011 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty

L. p.	Data	Konferencja/Seminarium	Miejsce
1.	14.01.2011	VII edycja konferencji „Nowocześni z Urzędu”. Organizator: Serwis publiczni.pl	Warszawa
2.	20.01.2011	Seminarium nt. ochrony danych osobowych w działalności organizacji pozarządowych. Organizator: Rada Organizacji Pozarządowych Województwa Łódzkiego	Łódź
3.	31.01.2011	V Dzień Ochrony Danych Osobowych, panel dyskusyjny „Retencja danych w demokratycznym państwie prawnym”. Organizator: GIODO	Warszawa
4.	03.02.2011	Ogólnopolskie Forum Dyrektorów Urzędów Pracy	Warszawa
5.	12.02.2011	Inauguracja Studiów Podyplomowych Wyższej Szkoły Biznesu	Dąbrowa Górnicza
6.	17.02.2011	Śniadanie naukowe „Stosowanie przez pracodawcę nowoczesnych technologii nadzoru nad zatrudnionymi”. Organizator: GIODO, Kolegium Prawa Akademii Leona Koźmińskiego oraz Prawnicze Koło Naukowe <i>Summa Sapientia</i>	Warszawa
7.	22.02.2011	Seminarium naukowe nt. zagrożenia dla prywatności wynikające ze stosowania monitoringu wizyjnego. Organizator: Polskie Towarzystwo Kryminologiczne im. Prof. S. Batawii	Warszawa
8.	03-04.03.2011	Ogólnopolska konferencja Akademickich Biur Karier. Organizator: Politechnika Łódzka	Łódź
9.	06-09.03.2011	Ogólnopolskie Forum Operatorów Kablowych FORTEL 2011. Organizator: Fundacja Wspierania Nowych Technologii Telekomunikacyjnych „PROTELKO”	Wisła
10.	09.03.2011	Konwersatorium nt. ochrony informacji w urzędach administracji samorządowej. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych	Rynia
11.	11.03.2011	Spotkanie z przedstawicielami Grupy do spraw Prezydencji Amerykańskiej Izby Handlowej poświęcone reformie europejskich przepisów o ochronie prywatności w kontekście Prezydencji RP w Radzie UE	Warszawa
12.	15-16.03.2011	Ogólnopolska Konferencja Dyrektorów Szkół Katolickich. Organizator: Rada Szkół Katolickich	Częstochowa
13.	17.03.2011	Spotkanie GIODO z przedstawicielami Amerykańskiej Izby Handlowej	Warszawa
14.	17.03.2011	Konferencja 4.TeraForum Polskiej Izby Informatyki i Telekomunikacji	Warszawa
15.	21.03.2011	Konferencja „Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym”. Organizator: Wydział Prawa i Administracji Uniwersytetu Warszawskiego	Warszawa
16.	24.03.2011	II Zjazd Akademii Zarządzania Dyrektora Szkoły 2010/2011. Organizator: Miesięcznik „Dyrektor Szkoły”	Warszawa
17.	25.03.2011	Konferencja Biegłych Sądowych „Pojęcie danych osobowych i zbioru danych osobowych w świecie nowych technologii”	Spała
18.	28.03.2011	Konferencja „Zabezpieczenie danych osobowych – aktualny stan prawny a rzeczywiste potrzeby”. Organizator: Politechnika Warszawska oraz Stowarzyszenie Administratorów Bezpieczeństwa Informacji	Warszawa
19.	30.03.2011	Seminarium „Bezpieczeństwo i ochrona danych w modelu cloud computing”. Organizator: Centrum Promocji Informatyki	Warszawa

20.	04.04.2011	Konwersatorium Regionalnej Izby Gospodarczej w Katowicach nt. ochrony danych osobowych w biznesie	Katowice
21.	05-06.04.2011	XI Kongres „Programy Lojalnościowe” Organizator: Informedia i Puls Biznesu	Kraków
22.	07.04.2011	Śniadanie naukowe: „Zmiany do ustawy o ochronie danych osobowych w dobie rozwoju nowoczesnych technologii”. Organizator: Iron Mountain	Warszawa
23.	08.04.2011	Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z Dyrektorem Agencji Praw Podstawowych (APP) Panem Morten'em Kjaerum'em nt. współpracy	Warszawa
24.	14.04.2011	Konferencja pt. ochrona danych osobowych w prawie pracy i w prawie ubezpieczeń społecznych – stan obecny i perspektywy zmian”. Organizator: Kolegium Prawa Akademii Leona Koźmińskiego w Warszawie, Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie	Warszawa
25.	15.04.2011	IX edycja seminarium „Jakość danych w systemach informatycznych zakładów ubezpieczeń”. Organizator: Polska Izba Ubezpieczeń	Warszawa
26.	18-19.04.2011	Międzynarodowa konferencja naukowa „Efektywność europejskiego systemu ochrony praw człowieka”. Organizator: Instytut Ekonomii i Administracji Uniwersytetu Humanistyczno-Przyrodniczego im. J. Kochanowskiego w Kielcach oraz komisja Sprawiedliwości i praw Człowieka, Sejm RP	Warszawa
27.	11.05.2011	Spotkanie z przedstawicielami Amerykańskiej Izby Handlowej w Polsce nt. konieczności zharmonizowania przepisów dotyczących ochrony danych osobowych obowiązujących w UE i USA w celu usprawnienia działalności przedsiębiorców	Warszawa
28.	16.05.2011	Konferencja pt. „Nie daj się złapać w sieć! – prawo autorskie, bezpieczeństwo i dobra osobiste w Internecie”. Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Poland, Katolicki Uniwersytet Lubelski oraz ELSA Lublin	Lublin
29.	16.05.2011	Międzynarodowa konferencja pt. „Freedom of knowledge in the area of emerging security threats”. Organizator: Uniwersytet Łódzki	Łódź
30.	17.05.2011	Śniadanie prasowe z okazji Światowego Dnia Społeczeństwa Informacyjnego. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych i Grupa BOSSG.	Warszawa
31.	18.05.2011	Seminarium pt. „Współczesne wyzwania dla praw człowieka w kontekście zagrożeń związanych z rozwojem nowych technologii. Organizator: Rzecznik Praw Obywatelskich	Warszawa
32.	18.05.2011	Światowy Dzień Społeczeństwa Informacyjnego w Polsce w 2011 r. Organizator: Polskie Towarzystwo Informatyczne	Warszawa
33.	19-20.05.2011	Międzynarodowa konferencja szkoleniowa pt. „Miasto monitorowane – personel, aspekty prawne i technika systemów CCTV”. Organizator: Prezydent Miasta Częstochowy, Związek Miast Polskich oraz Krajowa Rada Komendantów Straży Miejskich i Gminnych RP	Częstochowa
34.	20.05.2011	Konferencja „Cyberprzestępczość i ochrona informacji”. Organizator: Wyższa Szkoła Menedżerska w Warszawie	Warszawa
35.	21.05.2011	Konferencja pt. „Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli”. Organizator: Naczelna Rada Adwokacka	Warszawa
36.	24.05.2011	Targi administracji publicznej. Organizator: Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie	Warszawa
37.	25.05.2011	Konferencja pt. „Ochrona danych osobowych na rynku finansowym”. Organizator: Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie	Warszawa
38.	25-27.05.2011	VII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych	Spała

39.	02.06.2011	Ogólnopolska konferencja nt. ochrony danych osobowych w szkołach. Organizator: GIODO	Warszawa
40.	08-09.06.2011	3. Konferencja naukowa pt. „Bezpieczeństwo w Internecie”. Organizator: Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Naukowa i Akademicka Sieć Komputerowa oraz Naukowe Centrum Prawno - Informatyczne	Warszawa
41.	09.06.2011	X Forum ADO/ABI pt. „Rosnąca rola archiwów elektronicznych i kopii bezpieczeństwa w procesie przetwarzania danych osobowych”. Organizator: Centrum Promocji Informatyki	Warszawa
42.	10.06.2011	Konferencja pt. „Standardy bezpieczeństwa dokumentów państwowych”. Organizator: Agencja Bezpieczeństwa Wewnętrznego	Warszawa
43.	14.06.2011	Międzynarodowe seminarium “Wiążące Reguły Korporacyjne – pojęcie, stosowanie, doświadczenia praktyczne”. Organizator: GIODO	Warszawa
44.	15.06.2011	Międzynarodowe warsztaty „BCR w praktyce – wymiana doświadczeń pomiędzy organami ochrony danych”	Warszawa
45.	20.06.2011	Seminarium poświęcone anonimizacji danych osobowych w działalności Zespołu „Krajowy Mechanizm Prewencji”. Organizator: Rzecznik Praw Obywatelskich	Warszawa
46.	21.06.2011	Międzynarodowe warsztaty organizowane w ramach projektu PRACTIS PRIVACY – APPRAISING CHALLENGES TO TECHNOLOGIES AND ETHICS. Organizator: Uniwersytet Łódzki	Łódź
47.	01.07.2011	Forum „Energia – Efekt – Środowisko” nt. inteligentnych sieci energetycznych. Organizator: Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej	Warszawa
48.	20.07.2011	Warsztaty podsumowujące projekt partnerski pt.: „Zwiększanie świadomości w zakresie ochrony danych osobowych wśród przedsiębiorców funkcjonujących na rynkach Unii Europejskiej”	Warszawa
49.	20.09.2011	Konferencja pt.: „Działalność agencji zatrudnienia w kontekście realizacji zadań określonych w ustawie z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy”. Organizator: Wojewódzki Urząd Pracy w Łodzi	Łódź
50.	20-23.09.2011	XI Krajowe Forum Informacji Naukowej i Technicznej „Człowiek w przestrzeni informacyjnej”. Organizator: Polskie Towarzystwo Informacji Naukowej	Zakopane
51.	21.09.2011	Międzynarodowa Konferencja o Ochronie Danych Osobowych zorganizowana w ramach Prezydencji Polski w Radzie UE przez GIODO	Warszawa
52.	23.09.2011	Kongres Kupiectwa. Organizator: Komitet Handlu przy Krajowej Izbie Gospodarczej	Warszawa
53.	26.09.2011	Seminarium „IPv6 – wydumany problem czy realne zagrożenie”. Organizator: Polska Izba Informatyki i Telekomunikacji	Warszawa
54.	04-05.10.2011	23. Warsztaty Rozpatrywania Spraw (23rd Case Handling Workshop). Organizator: GIODO	Warszawa
55.	05.10.2011	Inauguracja roku akademickiego 2011/2012 w Wyższej Szkole Biznesu w Dąbrowie Górniczej	Dąbrowa Górnicza
56.	06-07.10.2011	I Europejski Kongres Małych i Średnich Przedsiębiorstw. Organizator: Regionalna Izba Gospodarcza w Katowicach	Katowice
57.	11.10.2011	Konferencja pt. „Nadzór niekontrolowany? Nowe wyzwania dla wolności”. Organizator: Fundacja Panoptykon.	Warszawa
58.	18.10.2011	XIII Krajowa Konferencja Dyrektorów Szkół i Przedszkoli. Organizator: Wolters Kluwer	Łódź
59.	21.10.2011	Konferencja pt. „Wyzwania XX wieku, czyli nieświadomość bezpieczeństwa informacji, ochrony danych osobowych i nie tylko”. Organizator: TÜVPOL Sp. z o.o.	Wrocław
60.	17-18.11.2011	6. Europejska Konferencja Ministerialna „Transgraniczne usługi e-administracji dla Europejczyków”. Organizator: Ministerstwo	Poznań

		Spraw Wewnętrznych i Administracji	
61.	21.11.2011	IV Międzynarodowa Konferencja „Jakość w działaniu na rzecz bezpieczeństwa państw Grupy Wyszehradzkiej z perspektywy europejskiej”. Organizator: Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi	Józefów
62.	23.11.2011	Spotkanie GIODO z przedstawicielami Stowarzyszenia Marketingu Bezpośredniego	Warszawa
63.	24.11.2011	Śniadanie naukowe dotyczące zasad profilowania klientów przez instytucje finansowe. Organizator: Iron Mountain	Warszawa
64.	24.11.2011	V Ogólnopolskie Forum Komunikacji Publicznej. Organizator: Mennica Polska. S.A.	Bydgoszcz
65.	28-29.11.2011	Konferencja „E-zdrowie – bezpieczeństwo i jakość informacji medycznej oraz szerokie zastosowanie technologii telemedycznych dla Unii Europejskiej w ramach Europy Cyfrowej”. Organizator: Centrum Systemów Informatycznych Ochrony Zdrowia	Warszawa
66.	30.11.2011	Konferencja naukowo-branżowa pt. „Bezpieczny hotel – oczekiwania i wyzwania wobec Euro 2012”. Organizator: Wyższa Szkoła Hotelarstwa, Gastronomii i Turystyki w Warszawie oraz Instytut Wiedzy i Umiejętności	Warszawa
67.	30.11.2011	IV Konferencja Central European Electronic Card - Warsaw 2011. Organizator: Medien Service	Warszawa
68.	02.12.2011	Konferencja naukowa „Medycyna personalizowana. Genom – etyka – prawo”. Organizator: Zakład Genetyki Klinicznej oraz Zakład Etyki i Filozofii Człowieka Uniwersytetu Medycznego w Lublinie	Lublin
69.	06-07.12.2011	Konferencja „Wyzwania w zakresie badań nad bezpieczeństwem wewnętrznym – nowa perspektywa finansowa UE 2013-2020”. Organizator: Polska Platforma Bezpieczeństwa Wewnętrznego	Będlewo k/Poznań
70.	08.12.2011	Wykład dla studentów Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego z zakresu bezpieczeństwa baz danych w praktyce aptecznej. Organizator: Warszawski Uniwersytet Medyczny, Zakład Opieki Farmaceutycznej	Warszawa
71.	09.12.2011	Konferencja naukowa pt. „Bezpieczeństwo technologii biometrycznych – ochrona danych biometrycznych”. Organizator: Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego	Warszawa
72.	15.12.2011	Seminarium „Zasady prawne monitoringu wizyjnego – co można, a co jest nielegalne”. Organizator: Centrum Promocji Informatyki.	Warszawa

**Wykaz konferencji, seminariów i spotkań międzynarodowych z udziałem GIODO
lub jego przedstawicieli, które odbyły się w 2011 r. za granicą**

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	16-17.01.2011	Posiedzenie Grupy Roboczej ds. wymiany informacji i ochrony danych	Bruksela
2.	16-18.01.2011	Posiedzenie Podgrupy ds. istotnych przepisów dyrektywy 95/46/WE	Bruksela
3.	24.01.2011	Konferencja „Data Breach Notification In Europe – The way forward” zorganizowana przez Europejską Agencję Bezpieczeństwa Sieci i Informacji (ENISA)	Bruksela
4.	25.01.2011	Spotkanie Podgrupy Technologicznej Grupy Roboczej Art. 29	Bruksela
5.	26.01.2011	Spotkanie GIODO z polskimi europosłami w Brukseli nt. reformy ochrony prywatności	Bruksela
6.	27.01.2011	Konferencja z okazji obchodów V Dnia Ochrony Danych Osobowych pt. „Portale społecznościowe” zorganizowana przez Urząd Węgierskiego Parlamentarnego Rzecznika Ochrony Danych i Wolności Informacji.	Budapeszt
7.	28.01.2011	Konferencja z okazji obchodów V Europejskiego Dnia Ochrony Danych Osobowych pt. „Data protection 30 years later: from European to international standards” zorganizowana przez Radę Europy i Komisję Europejską	Bruksela
8.	01-02.02.2011	Posiedzenie Wspólnych Organów Nadzorczych	Lublana
9.	09-11.02.2011	79. posiedzenie Grupy Roboczej Art. 29	Bruksela
10.	20-21.02.2011	Agencja Praw Podstawowych UE - spotkanie konsultacyjne	Wiedeń
11.	24.02.2011	Posiedzenie Podgrupy Grupy Roboczej Art. 29 Future in Privacy	Bruksela
12.	01-03.03.2011	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
13.	10-11.03.2011	Spotkanie organizacyjne w ramach projektu programu UE Prawa Podstawowe i Obywatelstwo	Budapeszt
14.	11.03.2011	Obrady Okrągłego Stołu „Ochrona danych osobowych: normy europejskie i ustawodawstwo ukraińskie” zorganizowane przez Dyрекcję Generalną ds. Praw Człowieka i Spraw Prawnych	Kijów
15.	14.03.2011	Posiedzenie Podgrupy ds. istotnych przepisów dyrektywy 95/46/WE	Bruksela
16.	17.03.2011	Spotkanie Podgrupy Technologicznej Grupy Roboczej Art. 29	Bruksela
17.	21.03.2011	Warsztaty ochrony danych osobowych w kontekście współpracy w dziedzinie konsumentów	Bruksela
18.	22-23.03.2011	Warsztaty eksperckie dotyczące wpływu technologii informacyjno-komunikacyjnych na administrację publiczną	Londyn
19.	02-04.04.2011	49. Spotkanie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji	Montreal
20.	04-05.04.2011	80. posiedzenie Grupy Roboczej Artykułu 29 ds. Ochrony Danych	Bruksela
21.	05.04.2011	Wiosenna Konferencja Europejskich Rzeczników Ochrony Danych	Bruksela
22.	28-29.04.2011	13. Spotkanie Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA)	Budapeszt
23.	10.05.2011	Spotkanie Podgrupy Grupy Roboczej Art. 29 ds. Zdrowia – systemu wymiany informacji o osobach uprawnionych do korzystania z usług medycznych	Bruksela
24.	11.05.2011	Spotkanie grupy ekspertów ENISA – Data Breach Notification – zgłaszanie naruszeń danych osobowych	Bruksela
25.	11-13.05.2011	Symposium APP	Wiedeń
26.	13.05.2011	Posiedzenie Podgrupy Grupy Roboczej Art. 29 ds. Key Provisions	Bruksela
27.	19.05.2011	Spotkanie Podgrupy Technologicznej Grupy Roboczej Art. 29 ds. Biometrii i eGovernment	Bruksela
28.	23-24.05.2011	Wizyta studyjna w sprawie PNR	Londyn

29.	26-27.05.2011	Spotkanie w Węgierskim Urzędzie Ochrony Danych Osobowych w ramach projektu partnerskiego Leonardo da Vinci	Budapeszt
30.	31.05.2011	81. posiedzenie Grupy Roboczej Artykułu 29 ds. Ochrony Danych	Bruksela
31.	06.06.2011	Posiedzenie Podgrupy Roboczej ds. BCR	Bruksela
32.	06-08.06.2011	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
33.	16-17.06.2011	Międzynarodowa Konferencja o Ochronie Danych Osobowych, zorganizowana w ramach współpracy Prezydencji Węgierskiej i Polskiej	Budapeszt
34.	22.06.2011	Warsztaty robocze dotyczące retencji danych	Bruksela
35.	28.06.2011	Spotkanie Podgrupy Technologicznej Grupy Roboczej Art. 29	Bruksela
36.	03-04.07.2011	Spotkanie grupy ekspertów ENISA – Data Breach Notification	Bruksela
37.	11-13.07.2011	24. Coroczna Międzynarodowa Konferencja Privacy Laws & Business	Cambridge
38.	11-13.09.2011	50. Spotkanie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji	Berlin
39.	13.07.2011	Spotkanie Podgrupy Grupy Roboczej Art. 29 Future in Privacy	Bruksela
40.	10-23.09.2011	Wizyta studyjna w Departamencie Stanu USA	Waszyngton
41.	11-13.09.2011	50. Posiedzenie Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (tzw. Grupa Berlińska)	Berlin
42.	13-15.09.2011	1. Spotkanie Europejskiego Forum ds. e-fakturowania	Bruksela
43.	16.09.2011	Posiedzenie Podgrupy Roboczej ds. BCR	Bruksela
44.	19-20.09.2011	Posiedzenie Podgrupy Technologicznej i Podgrupy ds. Implementacji Dyrektywy o prywatności i łączności elektronicznej Grupy Roboczej Art. 29	Bruksela
45.	27.09.2011	Spotkanie GIODO z przedstawicielami TechAmerica	Bruksela
46.	28.09.2011	Posiedzenie European Privacy Officers Forum, EPOF	Bruksela
47.	28-30.09.2011	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
48.	02-12.10.2011	Spotkanie w sprawie ewaluacji Schengen państw skandynawskich	Kopenhaga
49.	09-14.10.2011	Wizyta w Chorwackim Urzędzie Ochrony Danych Osobowych	Zadar
50.	12-13.10.2011	Spotkanie GIODO z Posłami do Parlamentu Europejskiego w ramach konsultacji nad reformą ram ochrony danych osobowych w UE	Bruksela
51.	12-13.10.2011	Posiedzenie Podgrupy Grupy Roboczej Art. 29 Future in Privacy	Bruksela
52.	13-14.10.2011	82. posiedzenie Grupy Roboczej Artykułu 29 ds. Ochrony Danych	Bruksela
53.	21.10.2011	Posiedzenie Grupy Roboczej EURODAC	Bruksela
54.	25-26.10.2011	II Międzynarodowa Konferencja „Ochrona danych osobowych” zorganizowana z inicjatywy Federalnej Służby Nadzoru w sektorze Łączności, Technologii Informacyjnych i Masowej Komunikacji Federacji Rosyjskiej	Moskwa
55.	31.10.2011	Udział GIODO w Spotkaniu Global Privacy Enforcement Network - GPEN	Meksyk
56.	01-03.11.2011	33. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności – Prywatność: Era Globalna	Meksyk
57.	11.11.2011	Konferencja na Uniwersytecie w Bocconi pt. „Ochrona danych osobowych 15 lat po uchwaleniu włoskiej ustawy o ochronie prywatności”	Mediolan
58.	29-30.11.2011	Kongres zorganizowany przez międzynarodową organizację International Association of Privacy Professional (IAPP).	Paryż
59.	29.11-02.12.2011	27. plenarne zebranie Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD)	Strasburg
60.	30.11-01.12.2011	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
61.	06.12.2011	2. Europejska Konferencja o Ochronie Danych i Prywatności	Bruksela
62.	07-08.12.2011	83. posiedzenie Grupy Roboczej Artykułu 29 ds. Ochrony Danych	Bruksela
63.	18-19.12.2011	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela

**Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych
wydanych w 2011 roku w sprawach o wyrażenie zgody
na przekazanie danych osobowych za granicę**

Lp.	Data wydania decyzji/postanowienia	Nazwa podmiotu	Sygnatura decyzji/postanowienia
1.	24.03.2011	Misys International Banking Systems Sp. z o.o., Warszawa (obecna nazwa Misys Poland Sp. z o.o., Warszawa)	DESiWM/DEC-237/13279/11 (decyzja wyrażająca zgodę na przekazanie danych)
2.	24.03.2011	Misys International Banking Systems Sp. z o.o., Warszawa (obecna nazwa Misys Poland Sp. z o.o., Warszawa)	DESiWM/DEC-238/13281/11 (decyzja częściowo umarzająca postępowanie ze względu na przekazywanie danych do Kanady; w pozostałym zakresie zgoda na przekazanie danych)
3.	28.03.2011	Turner Broadcasting System Poland Sp. z o.o., Warszawa	DESiWM/DEC-244/11/13775 (niewyrażenie zgody na przekazanie danych w zakresie danych ujawniających pochodzenie etniczne pracownika; w pozostałym zakresie zgoda na przekazanie danych)
4.	29.03.2011	Lenovo Technology B.V. Sp. z o.o., Oddział w Polsce	DESiWM/DEC-247/13947/11 (decyzja wyrażająca zgodę na przekazanie danych)
5.	29.03.2011	Staples Polska Sp. z o.o., Gdańsk	DESiWM/DEC-248/13965/11 (decyzja częściowo umarzająca postępowanie ze względu na przekazywanie danych do odbiorcy uczestniczącego w amerykańskim programie 'bezpiecznej przystani'; w pozostałym zakresie zgoda na przekazanie danych)
6.	06.04.2011	HSBC Bank Polska S.A., Warszawa	DESiWM/POST-81/15802/11 (postanowienie o podjęciu zawieszonego postępowania)
7.	18.04.2011	HJ Heinz Polska S.A., Krobia	DESiWM/DEC-308/17935/11 (decyzja wyrażająca zgodę na przekazanie danych)
8.	27.05.2011	Polska Telefonía Cyfrowa Sp. z o.o., Warszawa	DESiWM/DEC-414/24799/11 (decyzja wyrażająca zgodę na przekazanie danych)
9.	16.06.2011	HSBC Bank Polska S.A., Warszawa	DESiWM/DEC-493/28749/11 (decyzja wyrażająca zgodę na przekazanie danych)
10.	16.06.2011	Linde Gaz Polska Sp. z o.o., Kraków	DESiWM/DEC-494/28764/11 (decyzja wyrażająca zgodę na przekazanie danych)
11.	16.06.2011	Linde Gaz Polska Sp. z o.o., Kraków	DESiWM/DEC-495/28776/11 (decyzja wyrażająca zgodę na przekazanie danych)
12.	26.07.2011	J.P. Morgan Poland Limited Sp. z o.o., Bydgoszcz	DESiWM/DEC-611/35415/11 (decyzja wyrażająca zgodę na przekazanie danych)
13.	26.07.2011	JPMorgan Chase Bank National Association Przedstawicielstwo w Polsce, Nowy Jork, Warszawa	DESiWM/DEC-612/35422/11 (decyzja wyrażająca zgodę na przekazanie danych)
14.	27.07.2011	Brand Connection Sp. z o.o., Warszawa	DESiWM/DEC-614/35581/11

			(decyzja wyrażająca zgodę na przekazanie danych)
15.	27.07.2011	Initiative Media Warszawa Sp. z o.o., Warszawa	DESiWM/DEC-615/35586/11 (decyzja wyrażająca zgodę na przekazanie danych)
16.	27.07.2011	U2 Media Sp. z o.o., Warszawa	DESiWM/DEC-616/35591/11 (decyzja wyrażająca zgodę na przekazanie danych)
17.	27.07.2011	Universal McCann Sp. z o.o., Warszawa	DESiWM/DEC-617/35595/11 (decyzja wyrażająca zgodę na przekazanie danych)
18.	27.07.2011	McCann Erickson Polska Sp. z o.o., Warszawa	DESiWM/DEC-618/35598/11 (decyzja wyrażająca zgodę na przekazanie danych)
19.	27.07.2011	Momentum Worldwide Sp. z o.o., Warszawa	DESiWM/DEC-619/35605/11 (decyzja wyrażająca zgodę na przekazanie danych)
20.	27.07.2011	Weber Shandwick Sp. z o.o., Warszawa	DESiWM/DEC-620/35612/11 (decyzja wyrażająca zgodę na przekazanie danych)
21.	27.07.2011	MMR Worldwide Sp. z o.o., Warszawa	DESiWM/DEC-621/35614/11 (decyzja wyrażająca zgodę na przekazanie danych)
22.	27.07.2011	Bard Poland Sp. z o.o., Warszawa	DESiWM/DEC-613/35567/11 (decyzja wyrażająca zgodę na przekazanie danych)
23.	20.09.2011	AmeriGas Polska Sp. z o.o., Warszawa	DESiWM/DEC-809/44847/11 (decyzja wyrażająca zgodę na przekazanie danych)
24.	20.09.2011	Gaz Centrum Sp. z o.o., Warszawa	DESiWM/DEC-810/44858/11 decyzja wyrażająca zgodę na przekazanie danych)
25.	20.09.2011	Flaga Terminal Polska Sp. z o.o., Wółka Dobryńska	DESiWM/DEC-811/44859/11 (decyzja wyrażająca zgodę na przekazanie danych)
26.	20.09.2011	Flaga Gas Polska Sp. z o.o., Warszawa	DESiWM/DEC-812/44884/11 (decyzja wyrażająca zgodę na przekazanie danych)
27.	18.10.2011	Toshiba Television Central Europe Sp. z o.o., Biskupice Podgórne	DESiWM/DEC-866/49641/11 (decyzja wyrażająca zgodę na przekazanie danych)
28.	18.10.2011	Toshiba Logistics Central Europe Sp. z o.o., Biskupice Podgórne	DESiWM/DEC-867/49646/11 (decyzja wyrażająca zgodę na przekazanie danych)
29.	21.10.2011	Przedsiębiorstwo Usług Kolejowych Kolprem Sp. z o.o., Dąbrowa Górnicza	DESiWM/DEC-879/50661/11 (decyzja wyrażająca zgodę na przekazanie danych)
30.	21.10.2011	ArcelorMittal Poland S.A., Dąbrowa Górnicza	DESiWM/DEC-880/50668/11 (decyzja wyrażająca zgodę na przekazanie danych)
31.	21.10.2011	ArcelorMittal Shared Service Centre Europe Sp. z o.o., Dąbrowa Górnicza	DESiWM/DEC-881/50671/11 (decyzja wyrażająca zgodę na przekazanie danych)
32.	21.10.2011	ArcelorMittal Service Group Sp. z o.o., Dąbrowa Górnicza	DESiWM/DEC-882/50675/11 (decyzja wyrażająca zgodę na przekazanie danych)
33.	28.10.2011	Invensys Eurotherm Sp. z o.o., Warszawa	DESiWM/DEC-911/52273/11 (decyzja o umorzeniu postępowania na wniosek strony)
34.	28.10.2011	Invensys Systems Sp. z o.o., Warszawa	DESiWM/DEC-910/52265/11 (decyzja o umorzeniu postępowania na wniosek strony)

35.	17.11.2011	ADP Polska Sp. z o.o., Warszawa	DESiWM/DEC-976/55516/11 (decyzja wyrażająca zgodę na przekazanie danych)
36.	17.11.2011	ADP Polska Sp. z o.o., Warszawa	DESiWM/DEC-977/55554/11 (decyzja wyrażająca zgodę na przekazanie danych)
37.	17.11.2011	Invensys Systems Sp. z o.o., Warszawa	DESiWM/DEC-978/55581/11 (decyzja wyrażająca zgodę na przekazanie danych)
38.	17.11.2011	Invensys Eurotherm Sp. z o.o., Warszawa	DESiWM/DEC-979/55590/11 (decyzja wyrażająca zgodę na przekazanie danych)
39.	17.11.2011	Bank Handlowy w Warszawie S.A., Warszawa	DESiWM/DEC-980/55599/11 (decyzja wyrażająca zgodę na przekazanie danych)
40.	17.11.2011	Eurogaz-Gdynia Sp. z o.o., Gdynia	DESiWM/DEC-981/55601/11 (decyzja wyrażająca zgodę na przekazanie danych)
41.	17.11.2011	Eurogaz-Gdynia Sp. z o.o., Gdynia	DESiWM/DEC-982/55618/11 (decyzja wyrażająca zgodę na przekazanie danych)
42.	23.11.2011	Bristol-Myers Squibb Services Sp. z o.o., Warszawa	DESiWM/DEC-999/56694/11 (decyzja wyrażająca zgodę na przekazanie danych)
43.	23.11.2011	Bristol-Myers Squibb Polska Sp. z o.o., Warszawa	DESiWM/DEC-1000/56707/1111 (decyzja wyrażająca zgodę na przekazanie danych)
44.	23.11.2011	TI Poland Sp. z o.o., Bielsko-Biała	DESiWM/DEC-1001/56715/11 (decyzja wyrażająca zgodę na przekazanie danych)
45.	28.12.2011	Daimler Fleet Management Polska Sp. z o.o., Warszawa	DESiWM/DEC-1098/11/64024 (decyzja wyrażająca zgodę na przekazanie danych)
46.	28.12.2011	Mercedes-Benz Polska Sp. z o.o., Warszawa	DESiWM/DEC-1097/11/64000 (decyzja wyrażająca zgodę na przekazanie danych)
47.	28.12.2011	Mercedes-Benz Warszawa Sp. z o.o., Warszawa	DESiWM/DEC-1096/11/63994 (decyzja wyrażająca zgodę na przekazanie danych)
48.	28.12.2011	Mercedes-Benz Sosnowiec Sp. z o.o., Warszawa	DESiWM/DEC-1095/11/63986 (decyzja wyrażająca zgodę na przekazanie danych)
49.	28.12.2011	Mercedes-Benz Leasing Polska Sp. z o.o., Warszawa	DESiWM/DEC-1094/11/63955 (decyzja wyrażająca zgodę na przekazanie danych)
50.	28.12.2011	Mercedes-Benz Bank Polska S.A., Warszawa	DESiWM/DEC-1099/11/64025 (decyzja wyrażająca zgodę na przekazanie danych)
51.	28.12.2011	BP Polska Services Sp. z o.o., Kraków oraz BP Europa S.E. Oddział w Polsce, Kraków	DESiWM/POST-281/11/64035 (postanowienie o łącznym rozpatrzeniu spraw)
52.	30.12.2011	Nestlé Polska S.A., Warszawa	DESiWM/DEC-1109/64632/11 (decyzja wyrażająca zgodę na przekazanie danych)